LOS ARCHIVOS PREDATOR: EMBOSCADA EN LA RED

LA AMENAZA GLOBAL DEL SOFTWARE ESPÍA "REGULADO POR LA UE"

AMNISTÍA INTERNACIONAL

Amnistía Internacional es un movimiento integrado por 10 millones de personas que activa el sentido de humanidad dentro de cada una de ellas y que hace campaña en favor de cambios que permitan que todo el mundo disfrute de sus derechos humanos. Nuestra visión es la de un mundo donde quienes están en el poder cumplen sus promesas, respetan el derecho internacional y rinden cuentas. Somos independientes de todo gobierno, ideología política, interés económico y credo religioso, y nuestro trabajo se financia principalmente con las contribuciones de nuestra membresía y con donativos. Creemos que actuar movidos por la solidaridad y la compasión hacia nuestros semejantes en todo el mundo puede hacer mejorar nuestras sociedades.

© Amnesty International 2023

Salvo cuando se indique lo contrario, el contenido de este documento está protegido por una licencia 4.0 de Creative Commons (atribución, no comercial, sin obra derivada, internacional). https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.es

Para más información, visiten la página Permisos de nuestro sitio web: https://www.amnesty.org/es/permissions/.
El material atribuido a titulares de derechos de autor distintos de Amnistía Internacional no está protegido por la licencia Creative Commons.

Publicado por primera vez en 2023
por Amnesty International Ltd
Peter Benenson House, 1 Easton Street
London WC1X 0DW, Rino Unido

Índice: ACT 10/7245/2023 Spanish
Idioma original: Inglés

amnesty.org

Imagen de portada: © Colin Foo

AMNISTÍA INTERNACIONAL

ÍNDICE

GLOSARIO **5**

TÉRMINO 5

DEFINICIÓN 5

TABLA 1: RESUMEN DE EMPRESAS 8

1. RESUMEN EJECUTIVO **10**

2. METODOLOGÍA **15**

3. INTRODUCCIÓN **17**

4. LA ALIANZA INTELLEXA Y EL PROGRAMA ESPÍA PREDATOR **20**

4.1 UNA HISTORIA DE USOS ABUSIVOS DE LA VIGILANCIA 20

4.2 EL SOFTWARE ESPÍA PREDATOR DE INTELLEXA 23

4.3 CASO PRÁCTICO DE PREDATOR: @JOSEPH_GORDON16 25

4.4 OBJETIVOS DE @JOSEPH_GORDON16 27

4.4.1 ATAQUES CONTRA THOIBAO. DE 27

KHOA LÊ TRUNG, REDACTOR JEFE DE THOIBAO.DE 29

4.4.2 INTERESES EN EL SECTOR PESQUERO: ATAQUES CONTRA EL FUNCIONARIADO DE LA UNIÓN EUROPEA Y DE LA ONU 30

4.4.3 ATAQUES CONTRA OTRAS INSTITUCIONES Y ALTOS CARGOS 32

ATAQUES CONTRA AUTORIDADES ESTATALES DE ESTADOS UNIDOS Y TAIWÁN 35

4.4.4 OTROS INTENTOS DE ATAQUE CON SOFTWARE ESPÍA PREDATOR LIGADOS A ESTE OPERADOR 37

4.5 VENTAS A VIETNAM DE LA ALIANZA INTELLEXA 38

4.6 ATRIBUCIÓN DE LA RESPONSABILIDAD 40

4.7 DE LOS ATAQUES 40

5. IMPLICACIONES PARA LOS DERECHOS HUMANOS RELACIONADAS CON EL USO DE SOFTWARE ESPÍA **42**

5.1 PROHIBICIÓN DEL SOFTWARE ESPÍA ALTAMENTE INVASIVO 42

5.2 INEXISTENCIA DE SALVAGUARDIAS DE DERECHOS HUMANOS 43

5.3 LAS OBLIGACIONES EN MATERIA DE DERECHOS HUMANOS DE LOS ESTADOS 45
5.4 LA RESPONSABILIDAD DE LAS EMPRESAS DE RESPETAR LOS DERECHOS HUMANOS 46

6. "REGULADA Y RADICADA EN LA UE" 48

6.1 INACCIÓN DE LA UNIÓN EUROPEA Y DE LOS ESTADOS MIEMBROS PARA ACABAR CON EL USO INDEBIDO DE SOFTWARE ESPÍA 48
6.1.1 MEDIDAS REGULADORAS DE LA UE 49
6.2 DILIGENCIA DEBIDA OBLIGATORIA DE LAS EMPRESAS EN MATERIA DE DERECHOS HUMANOS 50

7. RECOMENDACIONES 51

A LA UNIÓN EUROPEA Y SUS ESTADOS MIEMBROS: 51
RECOMENDACIONES DE ACCIÓN DENTRO DE LA UNIÓN EUROPEA 51
RECOMENDACIONES DE ACCIONES DE LA UNIÓN EUROPEA Y SUS ESTADOS MIEMBROS A TRAVÉS DE SUS 52
INSTRUMENTOS DE POLÍTICA EXTERIOR 52
EL GOBIERNO DE VIETNAM DEBE: 53
TODOS LOS ESTADOS DEBEN: 54
LA ALIANZA INTELLEXA DEBE, COMO MÍNIMO: 55

8. ANEXOS 56

ANEXO I: INDICADORES DE RIESGO 56
DOMINIOS DE PREDATOR DE INTELLEXA LIGADOS A ESTA CAMPAÑA 56
CUENTAS DE X (TWITTER) LIGADAS A ESTA CAMPAÑA 56
CUENTAS DE FACEBOOK LIGADAS A ESTA CAMPAÑA 56
ANEXO II: TUITS 57
ANEXO III: OTROS ENLACES DE PREDATOR COMPARTIDOS EN REDES SOCIALES 60
ANEXO IV: ANÁLISIS DE CUENTAS DE REDES SOCIALES PRESUNTAMENTE RELACIONADAS CON EL ATACANTE 60

GLOSARIO

TÉRMINO	DEFINICIÓN
PROGRAMA ESPÍA	Los *programas espía* (*spyware* o software espía) son aquellos que permiten que un operador obtenga acceso encubierto a información de un sistema o dispositivo informático objetivo.
PROGRAMA ESPÍA COMERCIAL	Los *programas espía comerciales o mercenarios* son productos de vigilancia desarrollados y vendidos por actores empresariales a gobiernos que los emplean para llevar a cabo operaciones de vigilancia. El software espía comercial "de extremo a extremo" proporciona un sistema completo para la infección de dispositivos y la recopilación de datos. Entre los componentes de estos sistemas figuran los *exploits* empleados para instalar el programa espía: agentes del programa espía que se ejecuta en el dispositivo objetivo tras la infección y sistemas de *backend* para reunir y analizar los datos de vigilancia recopilados.
AGENTE DEL PROGRAMA ESPÍA	Un *agente del programa espía* (o implante) es el código de software final instalado en el ordenador o en el teléfono una vez que ha sido infectado. El agente es el responsable de recoger datos del dispositivo, activar sensores como micrófonos y cámaras, y subir estos datos al operador del programa espía.
VULNERABILIDAD DE SOFTWARE	Una *vulnerabilidad de software* es un defecto técnico o debilidad de un componente de software o de un fragmento de código que puede ser explotado por un atacante para burlar las defensas de seguridad.
EXPLOIT	Un *exploit* es un fragmento de software o de código que aprovecha (*explota*) una o más vulnerabilidades de software para obtener acceso a un dispositivo. En los dispositivos móviles modernos, los *exploits* deben eludir numerosas capas de defensas de seguridad y pueden ser sumamente complejos. Una cadena de *exploits* completa dirigida a las últimas versiones de dispositivos puede venderse por millones de euros.
BANDA BASE	La *banda base* del móvil son los componentes de hardware y software de un teléfono móvil responsables de comunicarse a través de una interfaz de radio con una torre o estación base de telefonía móvil.
DÍA CERO	Una *vulnerabilidad de día cero* es un defecto del software que no conoce el desarrollador original de éste y para el que no hay una corrección de software. Un *exploit* de día cero que aproveche este defecto puede atacar incluso dispositivos totalmente parcheados y actualizados.
VECTOR	*Vector* es un término empleado por el sector de la vigilancia para designar las diferentes vías o técnicas que se pueden usar para enviar un *exploit* a un dispositivo objetivo. Entre ellos figuran los que se conocen con el nombre de vectores de 1 clic o de 0 clics.

TÉRMINO	DEFINICIÓN
1 CLIC	Un ataque de *1 clic* necesita una acción del objetivo que permita la infección de su dispositivo, normalmente al abrir un enlace malicioso. Para engañar al objetivo y que éste abra el enlace, se usan diversas técnicas de ingeniería social, como la suplantación de sitios web o artículos de noticias legítimos. Si se clica en el enlace atacante, éste carga una cadena de *exploits* para, primero, afectar al navegador y, en último término, instalar el agente espía en el dispositivo objetivo.
0 CLICS	Ataque de *0 clics* es un término comercial del sector de la vigilancia que se aplica a cualquier vector que puede infectar un dispositivo sin necesidad de que el usuario o usuaria ejecute ninguna acción, como hacer clic en un enlace. Los ataques de 0 clics *totalmente remotos* permiten la infección por Internet, a menudo aprovechando fallos de aplicaciones de mensajería populares como iMessage o WhatsApp. Los ataques de 0 clics *tácticos* o no remotos pueden infectar dispositivos silenciosamente cuando el atacante tiene acceso privilegiado a la red o está cerca físicamente del objetivo.
INYECCIÓN DE RED	La *inyección de red* es una técnica en la que se inyectan paquetes de datos de Internet en el tráfico de Internet de un objetivo para bloquear, interceptar o manipular dicho tráfico.
HOMBRE EN EL MEDIO (*MAN-IN-THE-MIDDLE*, MITM)	Un *hombre en el medio* (o intermediario) es un atacante que puede leer, modificar y bloquear el tráfico de red de un objetivo. Se puede usar una función MitM para censurar al objetivo o perpetrar ataques de inyección de red.
HOMBRE A UN LADO (*MAN-ON-THE-SIDE*, MOTS)	Un *hombre a un lado* es un atacante que puede leer y monitorear el tráfico de la red, pero no puede bloquearlo ni modificarlo directamente. Esta situación es habitual cuando el atacante tiene acceso a una copia o un espejo del tráfico que se envía a través de un enlace de fibra óptica. Los ataques de inyección de red pueden llevarse a cabo también desde esta posición en la red.
INFECCIÓN TÁCTICA	Un *vector de infección táctica* permite al atacante atacar dispositivos situados en estrecha proximidad física. Se pueden usar redes de wifi maliciosas y estaciones base de telefonía móvil para redirigir silenciosamente un objetivo cercano a un enlace de *exploit*. Los atacantes también pueden aprovechar vulnerabilidades del software de la banda base del móvil y de las interfaces de wifi para infectar dispositivos próximos usando paquetes de radio enviados por aire.
INFECCIÓN ESTRATÉGICA	*Infección estratégica* es un término comercial que se refiere a sistemas de inyección de red desplegados en un proveedor de servicio de Internet (ISP, por sus siglas en inglés) o pasarela nacional de Internet que se pueden usar para enviar programas espía. Estos sistemas pueden interceptar peticiones no encriptadas enviadas por un objetivo y redirigir silenciosamente el dispositivo de éste a un enlace de *exploit*.
SS7	*Signaling System Number 7* es un conjunto de protocolos y estándares de señalización que se usan en las redes de telefonía para llevar a cabo funciones como el establecimiento de llamada, el enrutamiento y la itinerancia entre proveedores de telefonía móvil nacionales e internacionales. El protocolo se diseñó sin defensas de seguridad modernas y ha sido aprovechado por proveedores de vigilancia comercial para permitir diversos ataques, como el seguimiento de la localización y la interceptación de comunicaciones.
DENEGACIÓN DE SERVICIO	Una *denegación de servicio distribuido* es un ataque encaminado a interrumpir el funcionamiento de un sitio web o de una red sobrecargando el sistema con

TÉRMINO	DEFINICIÓN
DISTRIBUIDO (DDOS)	demasiado tráfico o demasiadas peticiones. Este tipo de ataque puede hacer que un sitio web no esté disponible para visitantes legítimos.
AVATAR	Un *avatar* es una identidad o cuenta en Internet falsa que se usa para recoger información de plataformas online o para interactuar con un usuario o usuaria objetivo. Estos perfiles aparentemente reales pueden usarse para enviar enlaces de ataque selectivos o difundir información online a través de redes sociales o servicios de mensajería.

TABLA 1: RESUMEN DE EMPRESAS

La alianza Intellexa, sus filiales y asociaciones han evolucionado desde su nacimiento hasta convertirse en una compleja estructura empresarial de ámbito mundial. Para facilitar la lectura, tanto la asociación de organizaciones europeas de medios de comunicación EIC (European Investigative Collaborations) como Amnistía Internacional usan el siguiente desglose:

Grupo Nexa: Nexa Technologies (Francia),[1] Nexa Technologies CZ s.r.o (República Checa), Advanced Middle East Systems (Emiratos Árabes Unidos), Trovicor fz (Emiratos Árabes Unidos).[2]

Grupo Intellexa: Wispear/Passitora (Chipre),[3] Cytrox (Macedonia del Norte),[4] Cytrox Holdings Zrt (Hungría), Intellexa S. A (Grecia),[5], Intellexa ltd (Irlanda),[6] Thalestris ltd (Irlanda).[7]

Alianza Intellexa[8]: es una alianza tecnológica y comercial que establecieron en 2019 el grupo Intellexa y el grupo Nexa. Ambos grupos mantuvieron accionariados separados. En el comunicado de prensa en el que se anunciaba el nacimiento de la alianza, las empresas miembros eran Nexa Technologies, Advanced Middle East Systems, Cytrox, WiSpear y Senpai Technologies.[9] No está claro si la alianza entre el grupo Nexa y el Grupo Intellexa sigue activa hoy.

El grupo empresarial Intellexa fue fundado en 2018 por el exoficial del ejército israelí Tal Dillan y varios de sus asociados, y vende el software espía Predator. Desde 2020, está controlado por el grupo empresarial Thalestris, con sede en Irlanda. Las principales empresas del grupo Intellexa son Cytrox (Macedonia del Norte), que desarrolla el sistema del programa espía Predator; WiSpear (Chipre), especialista en interceptación wifi; y Senpai Technologies (Israel), especialista en información de fuentes abiertas y la creación de avatares virtuales.

El grupo empresarial Nexa, que operaba principalmente desde Francia, estaba especializado en interceptación de tráfico y sistemas de vigilancia masiva (IP, voz, satélite, captadores IMSI, análisis de macrodatos). Fue creado en 2012 para hacerse cargo del negocio de la vigilancia de la empresa francesa Amesys. Incluyó desde el principio a Nexa Technologies (Francia) y a Advanced Middle East Systems (Dubái), empresa asociada que Nexa usaba como oficina de ventas. Entre 2019 y 2022, las empresas de este grupo estuvieron controladas por el grupo empresarial Boss Industries (Francia).[10] En 2019, Boss Industries compró la empresa Trovicor (Dubai),[11] especializada en "interceptación legítima" (sistemas de vigilancia telefónica). En 2020, el grupo Nexa decidió abandonar Nexa Technologies como marca y empezó a operar bajo el nombre comercial de Trovicor Intelligence.[12]

---

[1] Data INPI, "Présentation de l'entreprise RB 42", 26 de septiembre de 2023, https://data.inpi.fr/entreprises/751230681?q=751230681#751230681.
[2] Trovicor Intelligence, Aviso legal, https://trovicor.com/legal-disclosure/ (consultado por última vez el 26 de septiembre de 2023).
[3] Departamento de Registro de Sociedades y Propiedad Intelectual, 26 de septiembre de 2023, https://efiling.drcor.mcit.gov.cy/DrcorPublic/SearchResults.aspx?name=%25&number=318328&searchtype=optStartMatch&index=1&lang=EN&tname=%25&sc=1.
[4] Depositario Central de Valores, Известувања за корпоративни настани, https://www.cdhv.mk/известувања_за_корпоративни_настани.aspx (consultado por última vez el 26 de septiembre de 2023).
[5] Cámara de Comercio e Industria de Atenas, Intellexa ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ, 26 de septiembre de 2023, https://directory.acci.gr/companies/details/140944573.
[6] Oficina de Registro de Sociedades, Intellexa Limited, https://core.cro.ie/e-commerce/company/697890 (consultado por última vez el 26 de septiembre de 2023).
[7] Oficina de Registro de Sociedades, Thalestris Limited, https://core.cro.ie/e-commerce/company/693992 (consultado por última vez
el 26 de septiembre de 2023).
[8] Release Wire, "The Intellexa Intelligence Alliance Expands with the Addition of New Members and the Enhancement of Its End-to-End Offering", 20 de junio de 2019, http://www.releasewire.com/press-releases/the-intellexa-intelligence-alliance-expands-with-the-addition-of-new-members-and-the-enhancement-of-its-end-to-end-offering-1234811.htm.
[9] Release Wire, "The Intellexa Intelligence Alliance Expands with the Addition of New Members and the Enhancement of Its End-to-End Offering" (antes citado), http://www.releasewire.com/press-releases/the-intellexa-intelligence-alliance-expands-with-the-addition-of-new-members-and-the-enhancement-of-its-end-to-end-offering-1234811.htm.
[10] Data INPI, "Présentation de l'entreprise BOSS INDUSTRIES", 26 de septiembre de 2023, https://data.inpi.fr/entreprises/853120541?q=Boss%20Industries%20#853120541.
[11] Clairfield, "Clairfield advises Boss Industries on the acquisition of Dubai-based company Trovicor", 17 de diciembre de 2019, https://www.clairfield.com/clairfield-advises-boss-industries-on-the-acquisition-of-dubai-based-company-trovicor/.
[12] Intelligence Online, "France: Nexa renamed RB 42 with new cybersecurity focus", 3 de abril de 2023, https://www.intelligenceonline.com/surveillance--interception/2023/04/03/nexa-renamed-rb-42-with-new-cybersecurity-focus,109930650-art.

En 2022, Nexa Technologies vendió sus activos a la empresa francesa ChapsVision,[13] y en 2023 cambió su nombre a RB 42 y anunció que había cesado en sus actividades en el sector de la vigilancia.[14] Boss Industries sigue siendo propietaria de Trovicor, según documentos públicos.[15]

Cytrox es una empresa de Macedonia del Norte; establecida en 2017,[16] es la creadora original del programa espía Predator. Fue adquirida por WiSpear en 2018.[17]

Amesys, radicada en Francia, era una empresa de telecomunicaciones y defensa que creó un sistema de vigilancia masiva llamado Eagle capaz de llevar a cabo una vigilancia masiva del tráfico de Internet (IP) a escala de todo un país.[18] Amesys cesó en sus actividades en el sector de la cibervigilancia en 2012, tras la transferencia de sus activos a Nexa Technologies, que rebautizó Eagle como Cerebro.

[13] Intelligence Online, "France: ChapsVision takes up strong position in interceptions thanks to Elektron takeover", 24 de enero de 2022, https://www.intelligenceonline.com/surveillance--interception/2022/01/24/chapsvision-takes-up-strong-position-in-interceptions-thanks-to-elektron-takeover,109718567-art.
[14] Nexa Technologies, "Nexa Technologies: Une page se tourne", 2023, https://www.nexatech.fr/fr/about.
[15] Boss Industries, *Comptes sociaux,* 2021, p. 18.
[16] Depositario Central de Valores, Известувања за корпоративни настани (antes citado), https://www.cdhv.mk/известувања_за_корпоративни_настани.aspx.
[17] Atooro, 25 de mayo de 2020, http://web.archive.org/web/20200525234222/http://www.atooro.com/.
[18] Privacy International, "Amesys Brochure Eagle", febrero de 2009, https://www.documentcloud.org/documents/409206-95-amesys-critical-system-architect.html.

1. RESUMEN EJECUTIVO

Durante la última década, organizaciones de la sociedad civil, personal de investigación y periodistas han expuesto el modo en que gobiernos de todo el mundo vigilaban ilegítimamente a activistas, periodistas y representantes políticos mediante herramientas desarrolladas por empresas privadas de cibervigilancia. Tanto Amnistía Internacional como numerosas organizaciones de la sociedad civil han advertido en repetidas ocasiones de que el comercio y despliegue opacos de tecnologías de vigilancia de fabricación privada —en especial, software espía— por parte de los Estados ha provocado una crisis en materia de vigilancia digital, la cual ha repercutido negativa y gravemente en los derechos humanos, las libertades de los medios de comunicación y los movimientos sociales de todo el mundo. Las revelaciones del Proyecto Pegasus de 2021 —que destaparon la escala y amplitud global de la vigilancia ilegítima facilitada por el software espía Pegasus, de NSO Group— y las posteriores indagaciones de la sociedad civil han obligado a los gobiernos de todo el mundo a tomar nota de la escala y amplitud ingentes del abuso del software espía, lo que ha llevado a adoptar medidas iniciales para frenar a algunos de los distribuidores de software espía más conocidos. Sin embargo, las últimas revelaciones de Amnistía Internacional y las conclusiones de la nueva investigación denominada Archivos Predator, coordinada por la red de medios de comunicación European Investigative Collaborations (EIC), han evidenciado que la acción gubernamental no ha sido ni adecuada ni eficaz para acabar con el abuso del software espía. El presente informe detalla estas conclusiones.

En primer lugar, como parte de la investigación Archivos Predator, el Laboratorio sobre Seguridad de Amnistía Internacional colaboró con EIC —asociación de organizaciones europeas de medios de comunicación— en calidad de socio técnico. Amnistía Internacional analizó documentos a los que había tenido acceso EIC para determinar las especificaciones técnicas de un conjunto de productos de vigilancia desarrollados, operados y comercializados por la alianza Intellexa —formada por empresas de tecnología de vigilancia— entre 2007 y 2022 y descubrió que dicho conjunto incluía infinidad de tecnologías de vigilancia selectiva y masiva.

Las tecnologías de vigilancia selectiva comprenden software espía para móviles altamente invasivo, como Predator, que puede enviarse a los dispositivos mediante ataques de 1 clic o de 0 clics. La alianza Intellexa también ofrece varias técnicas para instalar el software espía mediante “ataques tácticos”, que permiten seleccionar como objetivo dispositivos que se hallan en estrecha proximidad física. Además, Intellexa ha desarrollado, operado y comercializado métodos de infección estratégica, los cuales permiten a un agente estatal dirigir intentos de infección silenciosos a personas usuarias de proveedores de servicios de Internet que cooperen o incluso a todo un país si el operador del software espía tiene acceso directo al tráfico de Internet. Los sistemas de infección estratégica se asemejan a las herramientas de vigilancia masiva, puesto que, para seleccionar como objetivo a una persona e infectarla, precisan tener acceso al tráfico de Internet a gran escala. En los productos de vigilancia masiva ofrecidos por la alianza Intellexa se presupone una evolución de las tecnologías de vigilancia previas, desde sistemas de interceptación legítimos que permitían vigilar el tráfico de forma selectiva e individualizada —lo que en teoría admitía más controles y limitaciones— hasta métodos más amplios e indiscriminados.

Amnistía Internacional cree que ambos tipos de tecnología —software espía altamente invasivo y herramientas de vigilancia masiva indiscriminada— son fundamentalmente incompatibles con los derechos humanos. El software espía Predator y sus variantes bajo denominaciones alternativas son programas espía altamente invasivos que pueden acceder a cantidades ilimitadas de datos de un dispositivo y que, en la actualidad, no pueden auditarse de forma independiente. Por lo tanto, Amnistía Internacional considera que todo despliegue de Predator y de otras formas de software espía altamente invasivo es incompatible con los derechos humanos y debe prohibirse con carácter permanente (véase el capítulo 5).

En segundo lugar, en este informe Amnistía Internacional expone una operación de vigilancia selectiva no revelada hasta la fecha que llevó a cabo un cliente del software espía Predator de Intellexa relacionado con Vietnam. El cliente parece ser afín a los intereses del gobierno de Vietnam y, entre febrero y junio de 2023, seleccionó como objetivo un mínimo de 50 cuentas en redes sociales titularidad de 27 personas y 23 instituciones utilizando para ello herramientas de software espía desarrolladas y comercializadas por la alianza Intellexa. El proceso consistió en enviar ataques de 1 clic a las cuentas de estas personas e instituciones en las redes sociales desde una cuenta en X (antes Twitter) con el nombre @Joseph_Gordon16. Entre los objetivos de esta operación con software espía se cuentan una web de noticias independiente con sede en Berlín, varias personalidades políticas del Parlamento Europeo, la Comisión Europea, personal académico de investigación y grupos consultivos. Además, entre los objetivos fallidos se halla personal de las Naciones Unidas, la presidenta de Taiwán; miembros del Senado y representantes de Estados Unidos, y otras autoridades diplomáticas.

El Grupo de Análisis de Amenazas de Google confirmó a Amnistía Internacional los hallazgos de la propia investigación de Google: los dominios y las URL que Amnistía Internacional había descubierto como parte de la operación de software espía estaban vinculados al sistema de software espía Predator de la alianza Intellexa. Junto con las pruebas aportadas por las entidades asociadas de EIC, en nuestros hallazgos se aprecian indicios de ventas de productos de vigilancia de la alianza Intellexa al Ministerio de Seguridad Pública de Vietnam y se sugiere que detrás de la campaña de software espía podría haber agentes de las autoridades vietnamitas o personas que actúan en su nombre. Además, Google confirmó a entidades asociadas de EIC que "asocian" la campaña de Predator de Intellexa y los indicadores descritos en este informe a "un agente gubernamental de Vietnam" (véase el capítulo 4).

Estas revelaciones se basan en la investigación técnica que lleva a cabo el Laboratorio sobre Seguridad de Amnistía Internacional para vigilar el desarrollo y despliegue de tecnologías de vigilancia ofrecidas por empresas de software espía mercenario, incluidas aquéllas propuestas por la alianza Intellexa. Como parte de estos esfuerzos, el análisis de Amnistía Internacional sobre la infraestructura técnica reciente ligada al sistema del software espía Predator señala también probables clientes activos o personas objetivo en lugares como, entre otros, Sudán, Madagascar, Kazajistán, Mongolia, Egipto, Indonesia, Vietnam y Angola (véase el capítulo 3).

Las conclusiones de este informe se basan también en una entrevista con un periodista de Vietnam seleccionado como objetivo, registros de envíos, datos comerciales y otras investigaciones e informes de EIC sobre las ventas de programas de vigilancia e infección de la alianza Intellexa. Amnistía Internacional revisó informes, declaraciones, leyes y estudios de organismos y especialistas de la ONU, autoridades regionales y nacionales a distintos niveles, informes de investigación y sobre políticas de organizaciones de la sociedad civil, así como informes de los medios de comunicación (véase el capítulo 2).

En tercer lugar, este informe analiza las implicaciones para los derechos humanos de lo revelado en los Archivos Predator, que muestra cómo se vende y transfiere impunemente en todo el mundo un conjunto de tecnologías de vigilancia altamente invasivas suministradas por la alianza Intellexa. La alianza Intellexa está compuesta por varios proveedores de sistemas de vigilancia que cuentan con presencia empresarial en Estados miembros de la Unión Europea (UE), así como en otros países de todo el mundo. Las revelaciones muestran la escala y amplitud globales de las ventas de tecnologías de vigilancia de una sola alianza de proveedores, que suministró sus productos a Egipto, Libia, Madagascar, Arabia Saudí, Vietnam y Francia —entre muchos otros países— entre 2007 y 2022. Estas transferencias generan una alta probabilidad de violación de los derechos humanos, dados los casos anteriores de vigilancia ilegítima en estos países o la ausencia de salvaguardias nacionales respecto a la vigilancia para impedir que estas tecnologías se usen ilegítimamente contra la sociedad civil, periodistas o figuras de la oposición política (véase el capítulo 3).

En cuarto lugar, este informe detalla un historial de abusos contra los derechos humanos que se han vinculado con la alianza Intellexa en Grecia, Libia y Egipto. Intellexa se publicita como una "empresa regulada y radicada en la UE". Según informes, la alianza Intellexa se compone de Nexa Technologies y Advanced Middle East Systems (que integran el grupo Nexa), así como de WiSpear, Cytrox y Senpai Technologies (que conforman el grupo Intellexa). Los grupos de empresas Nexa e Intellexa controlan múltiples entidades corporativas, algunas de las cuales han cambiado de denominación. Las entidades operan en varias jurisdicciones, tanto dentro como fuera de la UE. La naturaleza exacta de los vínculos entre estas empresas está inmersa en el secretismo, ya que las entidades corporativas y las estructuras entre ellas se transforman, se rebautizan, cambian de marca y evolucionan constantemente. Estas estructuras corporativas opacas y complejas parecen facilitar que las empresas eludan la rendición de cuentas, la transparencia y la normativa gubernamental, incluidos los controles de exportación regionales y nacionales, así como los mecanismos de diligencia debida corporativa. En el caso de la alianza Intellexa, el panorama es aún más complejo, debido a las estructuras corporativas no sólo de una empresa principal, sino de los distribuidores de productos de

vigilancia aliados, sus empresas matrices y sus inversores. La naturaleza enrevesada de esta entidad corporativa podría dificultar aún más la rendición de cuentas y la transparencia en lo que respecta a la vigilancia selectiva ilegítima que se practica con herramientas de esta alianza (véase la tabla 1 y el capítulo 4).

Tal como se establece en los Principios Rectores de la ONU sobre las Empresas y los Derechos Humanos (Principios Rectores de la ONU), las empresas tienen también la responsabilidad de respetar los derechos humanos con independencia del lugar del mundo en el que operen. Para hacer frente a esa responsabilidad, las empresas deben ejercer la diligencia debida en materia de derechos humanos. Las propias empresas de la alianza Intellexa no han revelado con carácter proactivo ninguna información sobre sus prácticas de diligencia debida en materia de derechos humanos. Cualquier evaluación —si es que existe— sobre el impacto de sus tecnologías de vigilancia en los derechos humanos es un misterio. En virtud del derecho internacional de los derechos humanos, los Estados están también obligados a proteger los derechos humanos de abusos perpetrados por terceros. Esto incluye la obligación de regular la conducta de las empresas que están domiciliadas en su territorio o bajo su control efectivo para impedir que cometan o contribuyan a cometer abusos contra los derechos humanos, incluso en el caso de que éstos se produzcan en otros países. La incapacidad de los Estados para ejercer un control significativo sobre la alianza Intellexa —por ejemplo, los Estados donde tienen su sede las entidades corporativas de la alianza, entre ellos Grecia, Irlanda, Francia, Alemania, República Checa, Chipre, Hungría, Suiza, Israel, Macedonia del Norte y Emiratos Árabes Unidos— ha dado paso a violaciones de los derechos humanos. En conjunto, las conclusiones ya mencionadas muestran que sociedad civil y periodistas siguen afrontando las devastadoras consecuencias del uso ilegítimo e incontrolado de tecnologías de vigilancia, que continúan amenazando los derechos a la privacidad y a la libertad de expresión, de asociación y de reunión pacífica de las personas afectadas. Además, como se detalla en este informe, la selección de autoridades oficiales regionales, nacionales e internacionales como objetivo demuestra una vez más que el software espía comercial tiene graves consecuencias tanto para los derechos humanos como para la seguridad del ecosistema digital. En ausencia de normativa, estas tecnologías de vigilancia pueden volverse contra terceros gobiernos y autoridades, como ya ha sucedido.

Estos hallazgos son sólo la punta del iceberg. Dado que las empresas de vigilancia y sus clientes estatales siguen ocultándose tras la retórica de la seguridad nacional y la confidencialidad para eludir la transparencia y la rendición de cuentas, es probable que la escala y el alcance reales de la vigilancia ilegítima mediante herramientas suministradas por la alianza Intellexa sean mucho mayores. Las advertencias de la sociedad civil y las lecciones aprendidas del Proyecto Pegasus significan que, en cada uno de los países en los que las revelaciones muestran que la alianza Intellexa ha vendido sus tecnologías, la sociedad civil podría estar sometida a una vigilancia clandestina generalizada. Estas nuevas revelaciones dejan patente, una vez más, que la venta y transferencia descontrolada de tecnologías de vigilancia podría seguir facilitando abusos contra los derechos humanos a escala global y masiva, puesto que se sigue permitiendo a las empresas vender y transferir libremente sus productos en el más absoluto secreto. Nuestros hallazgos demuestran una vez más que cualquier afirmación por parte de las empresas de que la vigilancia ilegítima es esporádica es rotundamente falsa. Los abusos contra los derechos humanos son la norma del sector, no una excepción.

Tras las revelaciones del Proyecto Pegasus, los Estados han dado algunos pasos con vistas a regular el sector y el uso estatal de estas tecnologías. Algunos avances son significativos y van en la dirección correcta. Sin embargo, las declaraciones públicas, las recomendaciones y los compromisos voluntarios no siempre se han convertido en acciones, y aún no se han rendido cuentas ni se ha ofrecido resarcimiento a las personas que, en todo el mundo, han sido seleccionadas ilegítimamente como objetivo de software espía. Si bien algunos Estados han emprendido iniciativas voluntarias, otros han obstruido las investigaciones y no han proporcionado una transparencia significativa. Es necesario que los Estados lleven a cabo más esfuerzos concertados para establecer salvaguardias de derechos humanos que sean vinculantes y aplicables a nivel nacional, regional e internacional. En 2019, el anterior relator especial de las Naciones Unidas sobre la libertad de opinión y de expresión indicó: “Decir que todo un sistema completo de control y utilización de tecnologías de vigilancia selectiva ha dejado de funcionar ni siquiera se acerca a la realidad. La realidad es que apenas existe”. Amnistía Internacional cree que, a pesar de los progresos iniciales, la situación no ha variado (véase el capítulo 5).

En particular, las últimas revelaciones plasman un panorama desolador en lo que respecta a la inacción de la UE y sus Estados miembros a la hora de frenar a las empresas que no rinden cuentas y a los Estados miembros díscolos, que siguen aprovechándose de las grietas, visiblemente grandes, de los sistemas normativos a nivel regional y nacional. La descarada campaña de vigilancia que se detalla en este informe, efectuada con las herramientas de la alianza Intellexa, muestra los riesgos muy directos de la proliferación y transferencia sin control de herramientas de cibervigilancia desde países de la UE. No sólo conducen a

abusos contra los derechos humanos fuera de la Unión, sino que también suponen una amenaza para la seguridad y los derechos humanos dentro de ella.

Las exportaciones de software espía desde la UE están sujetas a la concesión de licencias en virtud del Reglamento relativo a las exportaciones de productos de doble uso, para la cual, en teoría, deberían tenerse en cuenta los riesgos para los derechos humanos que plantean dichas exportaciones. Sin embargo, las revelaciones de los Archivos Predator demuestran que los Estados miembros concedieron licencias de exportación para tecnologías de vigilancia cuando existía un riesgo sustancial de que los usuarios finales cometieran violaciones de derechos humanos. Las revelaciones muestran también que la normativa europea de control de las exportaciones se eludió a través de estructuras corporativas opacas y entidades en terceros países. Queda claro que el Reglamento europeo relativo a las exportaciones de productos de doble uso presenta carencias importantes. Dos años después de publicarse el Reglamento refundido relativo a las exportaciones de productos de doble uso, éste no se ha aplicado de forma sólida y transparente. La Comisión de Investigación Encargada de Examinar el Uso del Programa Espía de Vigilancia Pegasus y Otros Programas Equivalentes (Comisión PEGA) del Parlamento Europeo ha señalado también la falta de voluntad política de la UE y los Estados miembros. Aunque los esfuerzos legislativos en curso, como la Propuesta de directiva sobre la diligencia debida de las empresas en materia de sostenibilidad, ofrecen una acertada oportunidad para empezar a abordar los daños del sector de la vigilancia selectiva, las lagunas de las propuestas presentadas por las entidades colegisladoras de la UE podrían significar que dicha directiva no se aplique correctamente a las empresas que comercializan tecnología de vigilancia (véase el capítulo 6).

RECOMENDACIONES CLAVE A LOS ESTADOS

Vista la ineficacia de la normativa actual, así como la naturaleza intrínsecamente abusiva de Predator, todos los Estados deberían:

- (especialmente los Estados que han concedido licencias de exportación) revocar inmediatamente todas las licencias de comercialización y exportación concedidas a la alianza Intellexa y llevar a cabo una investigación independiente, imparcial y transparente para determinar el alcance de la selección ilegítima de objetivos, que culmine con una declaración pública sobre los resultados de los esfuerzos realizados y las medidas tomadas para prevenir futuros daños.
- Hacer cumplir la prohibición del uso de software espía altamente invasivo. En la actualidad, dicho software espía no puede ser auditado de forma independiente y su funcionamiento no puede limitarse sólo a las funciones necesarias y proporcionadas a un uso y un objetivo específicos.
- Implantar un marco normativo de derechos humanos que regule la vigilancia y que sea conforme a las normas internacionales de derechos humanos. Hasta que exista un marco de este tipo, debería dictarse una moratoria sobre la compra, venta, transferencia y uso de todos los programas espía.
- Aplicar una legislación nacional que imponga salvaguardias contra las violaciones de derechos humanos y los abusos cometidos a través de la vigilancia digital y establecer mecanismos de rendición de cuentas que proporcionen a las víctimas de abusos de vigilancia una vía de recurso.
- Exigir legalmente a las empresas de vigilancia que ejerzan la diligencia debida en materia de derechos humanos en relación con sus operaciones globales, incluido el uso de sus productos y servicios.

RECOMENDACIONES CLAVE A LA UNIÓN EUROPEA Y SUS ESTADOS MIEMBROS

- Los Estados miembros de la UE y a la Comisión Europea deberían garantizar una aplicación firme del Reglamento de la UE de control de las exportaciones de 2021. Esto incluye tomar medidas inmediatas para subrayar la obligación de ejercer la diligencia debida en materia de derechos humanos derivada del Reglamento sobre exportaciones de doble uso y crear un mercado transparente de tecnologías de cibervigilancia sujeto a salvaguardias efectivas de derechos humanos.
- Los Estados miembros de la UE deben adoptar y hacer cumplir una legislación que exija a todos los actores empresariales el respeto de los derechos humanos y la aplicación de medidas de diligencia debida en materia de derechos humanos acordes con los Principios Rectores de la ONU. Como parte de las deliberaciones en curso en torno a la Propuesta de directiva sobre la diligencia debida de las empresas en materia de sostenibilidad, la UE debe exigir a las empresas que ejerzan la diligencia debida en materia de derechos humanos con respecto a toda la cadena de valor, incluidos la compra, la venta, la

transferencia, la exportación y el uso de los productos. Las empresas que operan en cualquier sector —incluidas las que producen software espía, así como las instituciones financieras— deberían aplicar los requisitos de la citada propuesta de directiva.

RECOMENDACIONES CLAVE AL GOBIERNO DE VIETNAM

El gobierno de Vietnam debe llevar a cabo una investigación independiente, imparcial y transparente sobre la vigilancia selectiva ilegítima mencionada en este informe, incluidas averiguaciones para determinar si existen vínculos entre esta campaña de software espía y alguna agencia gubernamental específica.

RECOMENDACIONES CLAVE A LA ALIANZA INTELLEXA

La alianza Intellexa debe poner fin a la producción y venta de Predator y de cualquier otro software espía altamente invasivo similar que no incluya salvaguardias técnicas que permitan su uso legítimo en virtud de un marco normativo que respete los derechos humanos. También debería proporcionar una indemnización adecuada u otras formas de resarcimiento efectivo a las víctimas de vigilancia ilegítima.

2. METODOLOGÍA

El informe se basa en las investigaciones técnicas en curso que lleva a cabo Amnistía Internacional para seguir el desarrollo y despliegue de tecnologías de vigilancia —programas espía selectivos para móviles incluidos— que representan una amenaza para quienes defienden los derechos humanos y la sociedad civil en todo el mundo.[19] Este trabajo incluye identificar y seguir la evolución de los productos de vigilancia que ofrecen empresas de programas espía mercenarios como NSO Group, la alianza Intellexa y otras.[20] El Laboratorio sobre Seguridad viene siguiendo muy de cerca el programa espía Predator de Intellexa desde septiembre de 2021, lo que ha permitido la identificación de víctimas de Predator de la sociedad civil en múltiples países. Esta investigación técnica llevó a Amnistía Internacional a identificar, en abril de 2023, una cuenta pública de X (antes Twitter) que compartía enlaces de infección del programa espía de Intellexa, dato totalmente documentado como caso práctico en el informe.

Amnistía Internacional entrevistó a un periodista originario de Vietnam que vive actualmente en Alemania y cuya plataforma de medios de comunicación fue atacada como parte de la campaña de ataques de este programa espía en febrero de 2023. La organización también identificó registros de envíos y datos comerciales, y estudió un análisis de otros registros empresariales de la alianza Intellexa obtenidos por EIC que documentan ventas de las soluciones de vigilancia e infección de la alianza. Amnistía revisó asimismo informes, declaraciones, leyes y estudios de organismos y especialistas de la ONU, autoridades regionales y nacionales a distintos niveles; informes de investigación y sobre políticas elaborados por organizaciones de la sociedad civil, así como informes de los medios de comunicación.

Además, como parte de la investigación Archivos Predator, el Laboratorio sobre Seguridad de Amnistía Internacional colaboró con la asociación de organizaciones europeas de medios de comunicación EIC (European Investigative Collaborations) en calidad de socio técnico. Este informe contiene conclusiones del análisis de Amnistía de las especificaciones técnicas de un conjunto de productos de vigilancia que ofrecía la alianza Intellexa de empresas de tecnología de vigilancia. Para ello, la organización analizó folletos promocionales y documentos técnicos a los que había tenido acceso EIC a fin de determinar las especificaciones técnicas y analizar las implicaciones para los derechos humanos del conjunto de productos de vigilancia desarrollados, operados y comercializados por la alianza Intellexa entre 2007 y 2022.

Amnistía Internacional envió el 19 de septiembre de 2023 una carta al Ministerio de Seguridad Pública de Vietnam solicitando sus comentarios a las conclusiones de este informe, pero no había obtenido respuesta en el momento de la publicación. La organización envió asimismo cartas solicitando una respuesta a estas conclusiones a representantes del grupo Intellexa y del grupo Nexa el 20 de septiembre de 2023. Las estructuras cambiantes y a menudo deliberadamente opacas de muchas de estas empresas —que se exponen *infra*— dificultaron llegar a ellas. Amnistía Internacional contactó con las entidades corporativas más recientes para algunas de estas empresas basándose en información disponible públicamente contenida en diversos registros mercantiles o en sus sitios web (véase en la tabla 1 una explicación de las entidades corporativas). La organización pidió a las entidades información sobre sus prácticas de diligencia debida en

[19] Amnistía Internacional, *Forensic Methodology Report: How to catch NSO Group's Pegasus*, 18 de julio de 2021, https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/.
[20] Véase, por ejemplo: Amnistía Internacional, *Amnistía Internacional denuncia nueva campaña de hackeo ligada a empresa de software espía mercenario*, 29 de marzo de 2023, https://www.amnesty.org/es/latest/news/2023/03/new-android-hacking-campaign-linked-to-mercenary-spyware-company/.

materia de derechos humanos. También preguntó a las empresas por las medidas que habían adoptado para proporcionar una reparación a las personas afectadas por el uso de sus tecnologías reveladas en anteriores informes de investigación, pero no había recibido respuesta en el momento de la publicación. El 26 de septiembre de 2023, Amnistía Internacional escribió también a Delsons Hong Kong Limited sobre nuestras conclusiones acerca de los envíos de tecnologías de vigilancia a Vietnam expuestas en el apartado 4.5 *infra*. En el momento de la publicación no había recibido respuesta.

Aunque Amnistía Internacional no recibió ninguna respuesta directa ni del grupo Intellexa ni del grupo Nexa, ex personal directivo y accionistas principales del segundo sí respondieron a entidades asociadas de EIC en nombre de sus empresas, incluidas Nexa Technologies y Advanced Middle East Systems. Parte de su respuesta se refería a su implicación en las ventas a Vietnam y se ha incorporado al apartado 4.5 *infra*.

Amnistía Internacional hace extensivo su más profundo agradecimiento a todas las personas que han participado en esta investigación, en concreto a nuestras entidades asociadas en EIC y a Khoa Lê Trung. Por su parte, el Laboratorio sobre Seguridad de Amnistía Internacional agradece al Digital Security Lab de Reporteros sin Fronteras su asistencia para recabar información forense durante esta investigación. Amnistía Internacional da las gracias al Citizen Lab por su verificación independiente de nuestros hallazgos sobre la conexión entre dominios de ataque identificados y el programa espía Predator de Intellexa, y al Grupo de Análisis de Amenazas de Google[21] por compartir su investigación sobre la infraestructura de vigilancia de la alianza Intellexa.

CONSEJOS SOBRE SEGURIDAD DIGITAL

Los sofisticados programas espía y ataques digitales que se exponen en este informe se usan contra personas que, por su actividad profesional, su trabajo en la sociedad civil o la información que poseen revierten un interés especial para operadores gubernamentales de programas espía. Si cree que corre un mayor riesgo de sufrir este tipo de ataques, encontrará a continuación una serie de medidas prácticas que puede adoptar para dificultar esta clase de ataques digitales avanzados:

- Actualice su navegador y el sistema operativo móvil tan pronto como se disponga de actualizaciones de seguridad para sus dispositivos.
- Si usa un dispositivo Apple, habilite el "Modo Bloqueo" de alta seguridad. Esto puede dificultar el éxito del ataque a su dispositivo.
- Cuidado con hacer clic en enlaces de desconocidos. No se fíe únicamente de la vista previa de la URL que se muestra en aplicaciones de mensajería o plataformas de redes sociales, pues podría ser engañosa.
- Preste atención a cualquier cambio en el funcionamiento del dispositivo (por ejemplo, una duración menor de la batería), pero tenga en cuenta que, esto en sí mismo no es un indicador claro de actividad sospechosa.
- Deshabilite la opción para permitir las solicitudes de mensajes directos de todas las personas en X (antes Twitter).
- En cuentas personales de Facebook, gestione la configuración de la privacidad para limitar la visibilidad de su perfil a los amigos y evalúe las solicitudes de amistad o de Messenger antes de aceptarlas.
- Si recibe un aviso de atacante patrocinado por un Estado, pida ayuda experta para comprender los riesgos que corren sus cuentas o dispositivos.

Si se dedica a la defensa de los derechos humanos, es periodista o miembro de la sociedad civil y cree que ha sido un objetivo de esta campaña o ha recibido enlaces de ataque similares a través de redes sociales, le aconsejamos que contacte con https://securitylab.amnesty.org/contact-us/.

[21] El Grupo de Análisis de Amenazas de Google afirma que está creado para "contrarrestar ataques respaldados por un gobierno". Grupo de Análisis de Amenazas de Google, https://blog.google/threat-analysis-group/ (consultado por última vez el 28 de septiembre de 2023).

3. INTRODUCCIÓN

Durante el último decenio, organizaciones de la sociedad civil, personal de investigación y periodistas han expuesto, a través de un flujo constante de revelaciones, el modo en que gobiernos de todo el mundo vigilaban ilegítimamente a activistas, periodistas y funcionarios y funcionarias de gobiernos mediante herramientas desarrolladas por empresas privadas de cibervigilancia. Tanto Amnistía Internacional como numerosas organizaciones de la sociedad civil han advertido en repetidas ocasiones de que el comercio y despliegue opacos de tecnologías de vigilancia de fabricación privada —en especial, software espía— por parte de los Estados ha provocado una crisis en materia de vigilancia digital[22] que ha repercutido de forma negativa y grave en los derechos humanos, las libertades de los medios de comunicación y los movimientos sociales de todo el mundo. Las revelaciones del Proyecto Pegasus de 2021[23] —que destaparon la escala y amplitud globales de la vigilancia ilegítima facilitada por el software espía Pegasus de NSO Group— y las posteriores indagaciones de la sociedad civil[24] han obligado a los gobiernos de todo el mundo a tomar nota de la escala y amplitud ingentes del uso indebido del software espía, lo que ha llevado a adoptar medidas iniciales para frenar a algunos de los proveedores de software espía más conocidos y a exigir rendición de cuentas por las víctimas de vigilancia ilegítima.

Ahora, una nueva investigación, coordinada por la red de medios de comunicación EIC con el apoyo técnico del Laboratorio sobre Seguridad de Amnistía Internacional, ha evidenciado que la acción gubernamental ha sido insuficiente e ineficaz para acabar con el uso indebido del software espía.[25] Las nuevas revelaciones de los Archivos Predator han dejado al descubierto que el uso por los Estados de software espía y herramientas de vigilancia de fabricación privada sigue estando fuera de control y constituye una amenaza para los derechos humanos de las personas mientras Estados y proveedores de vigilancia continúan la venta, transferencia y uso sin control de tecnologías de vigilancia en todo el mundo.[26]

Lo revelado en los Archivos Predator muestra la venta y transferencia con impunidad en todo el mundo de tecnologías de vigilancia altamente invasivas suministradas por la alianza Intellexa, integrada por proveedores de vigilancia con presencia empresarial en Estados miembros de la Unión Europea, así como en otros países del mundo. Las revelaciones muestran la escala y amplitud globales de las ventas de tecnologías de vigilancia de esta sola alianza de proveedores, que ha suministrado sus productos a Egipto, Libia, Madagascar, Arabia Saudí, Vietnam y Francia —entre muchos otros países— entre 2007 y 2022.[27] Estas transferencias generan una alta probabilidad de que se cometan abusos contra los derechos humanos dados los casos anteriores de

[22] Amnistía Internacional, *Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector* (Índice: DOC 10/4491/2021), 23 de julio de 2021, https://www.amnesty.org/es/documents/doc10/4491/2021/en/; Amnistía Internacional, *Carta abierta conjunta de organizaciones de la sociedad civil y expertos/as independientes en la que se insta a los Estados a que apliquen una moratoria inmediata sobre la venta, la transferencia y el uso de tecnología de vigilancia* (Índice: DOC 10/4516/2021), 27 de julio de 2021, https://www.amnesty.org/es/documents/doc10/4516/2021/es/.

[23] El Proyecto Pegasus fue una colaboración pionera de más de 80 periodistas de 17 medios de comunicación en 10 países coordinados por Forbidden Stories (organización sin ánimo de lucro de medios de comunicación con sede en París) con el apoyo técnico de Amnistía Internacional.

[24] Véanse, por ejemplo: Access Now, "Spyware in warfare: Access Now documents first-time use of Pegasus tech in Azerbaijan-Armenia conflict", 25 de mayo de 2023, https://www.accessnow.org/press-release/spyware-warfare-pegasus-in-azerbaijan-armenia-conflict/; Citizen Lab, "Proyecto Torogoz: Hackeo extensivo de los medios de comunicación y la sociedad civil en El Salvador con el programa espía Pegasus", 12 de enero de 2022, https://citizenlab.ca/2022/01/proyecto-torogoz-hackeo-extensivo-de-los-medios-de-comunicacion-y-la-sociedad-civil-en-el-salvador-con-el-programa-espia-pegasus/.

[25] Todos los informes de EIC sobre los Archivos Predator se publican simultáneamente a este informe. Pueden encontrar los enlaces a los informes en https://eic.network/#projects.

[26] EIC, Projects, https://eic.network/#projects.

[27] EIC, Projects, https://eic.network/#projects.

vigilancia ilegítima en estos países o la ausencia de salvaguardias nacionales respecto a la vigilancia para impedir que estas tecnologías se usen ilegítimamente contra la sociedad civil, periodistas o figuras de la oposición política.

En este informe, el Laboratorio sobre Seguridad de Amnistía Internacional ha revelado también una operación de software espía selectivo que no se había dado a conocer hasta ahora en la que se usó el producto de software espía Predator de Intellexa contra objetivos alineados con los intereses del gobierno de Vietnam. La campaña de vigilancia dirigió como mínimo a 50 cuentas en redes sociales pertenecientes a 27 personas y 23 instituciones de todo el mundo enlaces de infección de software espía de 1 clic conectados con la infraestructura de ataque del programa espía Predator de Intellexa. Entre los objetivos se cuentan varias personalidades políticas del Parlamento Europeo, la Comisión Europea, periodistas de la UE, personal académico de investigación y grupos consultivos. Además de éstos, hubo objetivos fallidos como personal de las Naciones Unidas, la presidenta de Taiwán, miembros del Senado y la Cámara de Representantes de Estados Unidos, y otras autoridades diplomáticas. Los ataques contra estas personas se produjeron en fechas tan recientes como junio de 2023. Amnistía Internacional también identificó registros de envíos y datos comerciales, y, para este informe, se basa en investigaciones de entidades asociadas de EIC sobre ventas de las soluciones de vigilancia e infección de la alianza Intellexa. Esta investigación revela que las herramientas se vendieron a través de diversas empresas intermediarias vietnamitas a un usuario final del gobierno: el Ministerio de Seguridad Pública de Vietnam. Amnistía Internacional no ha identificado pericialmente ninguna infección derivada de esta campaña; sin embargo, las capacidades conocidas del sistema del software espía Predator —además del descaro y, a veces, falta de cuidado de esta operación de vigilancia— ponen de manifiesto los enormes riesgos que plantean la proliferación y las transferencias sin control de estas herramientas.

El análisis de Amnistía Internacional sobre la infraestructura técnica reciente ligada al sistema del software espía Predator indica también probables clientes activos o ataques a personas en Sudán, Madagascar, Kazajistán, Mongolia, Egipto, Indonesia, Vietnam y Angola, entre otros países. Esto se basa en la investigación de 2021 de Citizen Lab y Meta, que documentó posibles clientes de Predator activos en Arabia Saudí, Omán, Grecia, Serbia, Trinidad y Tobago, Armenia, Egipto, Colombia, Costa de Marfil, Vietnam, Filipinas, Alemania, Indonesia y Madagascar.[28]

El análisis de folletos promocionales a los que había tenido acceso EIC ha permitido que Amnistía Internacional confirme las especificaciones técnicas de un conjunto de productos de vigilancia desarrollados, operados y comercializados entre 2007 y 2022 por las empresas que formaron parte de lo que se convirtió en la alianza Intellexa.[29] Dicho conjunto incluía infinidad de tecnologías de vigilancia selectiva y masiva. Las tecnologías de vigilancia selectiva comprenden software espía para móviles altamente invasivo, como Predator, que puede enviarse a los dispositivos mediante ataques de 1 clic o de 0 clics. El programa espía Predator fue desarrollado originalmente por la empresa de vigilancia Cytrox, radicada en Macedonia del Norte, que forma parte del grupo empresarial Intellexa (véase la tabla 1, Resumen de empresas).

Las revelaciones de la investigación de los Archivos Predator también documentan diversos "vectores" o técnicas que ofrece la alianza Intellexa para instalar el software espía mediante "ataques tácticos" que permiten infectar dispositivos que se hallan en estrecha proximidad física mediante el uso de múltiples tipos de métodos de inyección de red y ataques contra bandas base de teléfonos móviles. Además, la alianza Intellexa también ha desarrollado, operado y comercializado métodos de infección estratégica que permiten que un actor estatal dirija intentos de infección silenciosos a personas usuarias de proveedores de servicios de Internet que cooperen o incluso a todo un país si el operador del software espía tiene acceso directo al tráfico de Internet. Los sistemas de infección estratégica se asemejan a las herramientas de vigilancia masiva puesto que, para atacar e infectar a una persona, precisan tener acceso al tráfico de Internet a gran escala. En los productos de vigilancia masiva que ofrece la alianza Intellexa se presupone una evolución de las tecnologías de vigilancia previas, desde sistemas de interceptación legítimos que permitían vigilar el tráfico de forma selectiva e individualizada —lo que en teoría admitía más controles y limitaciones— hasta métodos más amplios e indiscriminados.[30] Ambos tipos de vigilancia —es decir, software espía altamente invasivo y

[28] Meta, *Threat Report on the Surveillance-for-Hire Industry,* 16 de diciembre de 2021, https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf; Citizen Lab, "Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware", 16 de diciembre de 2021, https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/.
[29] Amnistía Internacional, 6 de octubre de 2023, https://securitylab.amnesty.org/latest/2023/10/technical-deep-dive-into-intellexa-alliance-surveillance-products/.
[30] Wiki Leaks, Amesys product descriptions document for the Prague ISS World Europe 2008 Conference, https://wikileaks.org/spyfiles/files/0/21_200810-ISS-PRG-AMESYS.pdf (consultado por última vez el 26 de septiembre de 2023).

herramientas de vigilancia masiva indiscriminada— son fundamentalmente incompatibles con los derechos humanos.

Estos hallazgos son sólo la punta del iceberg. Dado que las empresas de vigilancia y sus clientes estatales siguen parapetándose en la retórica de la seguridad nacional y la confidencialidad para eludir la transparencia y la rendición de cuentas, es probable que la escala y el alcance reales de los ataques ilegítimos mediante herramientas suministradas por la alianza Intellexa sean mucho mayores. Las advertencias de la sociedad civil y las lecciones aprendidas del Proyecto Pegasus significan que, en cada uno de los países donde las revelaciones muestran que la alianza Intellexa ha vendido sus tecnologías, se podría estar atacando masivamente a la sociedad civil de forma incontrolada y con impunidad. Estas nuevas revelaciones dejan patente, una vez más, que la venta y transferencia incontrolada de tecnologías de vigilancia podría seguir facilitando abusos contra los derechos humanos a escala global, puesto que se sigue permitiendo a las empresas vender y transferir libremente sus productos en secreto. Los nuevos datos sobre ataques ilegítimos demuestran, una vez más, que cualquier afirmación por parte de las empresas de que la vigilancia ilegítima es esporádica es rotundamente falsa.[31] Los abusos contra los derechos humanos son la norma del sector, no una excepción.[32]

La sociedad civil lleva tiempo advirtiendo de que se ha desarrollado una cultura de impunidad específica de la vigilancia digital selectiva contra la que se debe luchar con urgencia. El flujo constante de revelaciones de la sociedad civil debería haber dado pie a actuaciones más contundentes de los gobiernos en los ámbitos nacional, regional y multilateral. Aunque no cabe duda de que se han dado algunos pasos en la dirección correcta, sociedad civil, periodistas y personal investigador siguen liderando las revelaciones sobre esta industria clandestina y esfera de práctica estatal que no rinde cuentas mediante conocimientos ganados a pulso.[33]

Amnistía Internacional ha advertido en ocasiones anteriores de que las revelaciones de la sociedad civil no deberían ser la única forma de controlar a los Estados y a las empresas de vigilancia.[34] El comercio continuo de tecnologías de vigilancia y su uso indebido, denunciado en estas revelaciones más recientes, debe impulsar una acción urgente y concertada de los Estados, que deben mostrar liderazgo a la hora de acabar con los abusos contra los derechos humanos derivados del uso ilegítimo de tecnologías de vigilancia selectiva y garantizar que sus víctimas cuentan con vías significativas para la rendición de cuentas.

[31] Amnistía Internacional, *Carta abierta conjunta de organizaciones de la sociedad civil y expertos/as independientes en la que se insta a los Estados a que apliquen una moratoria inmediata sobre la venta, la transferencia y el uso de tecnología de vigilancia* (antes citada), https://www.amnesty.org/es/documents/doc10/4516/2021/es/.
[32] Amnistía Internacional, *Operating in the shadows*: *Investor risk from the private surveillance industry* (Índice: DOC 10/4359/2021), 21 de octubre de 2021, https://www.amnesty.org/es/documents/doc10/4359/2021/en/.
[33] Amnistía Internacional, *Carta abierta conjunta de organizaciones de la sociedad civil y expertos/as independientes en la que se insta a los Estados a que apliquen una moratoria inmediata sobre la venta, la transferencia y el uso de tecnología de vigilancia* (antes citada), https://www.amnesty.org/es/documents/doc10/4516/2021/es/.
[34] Amnistía Internacional, *Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector* (antes citado) https://www.amnesty.org/es/documents/doc10/4491/2021/en/.

4. LA ALIANZA INTELLEXA Y EL PROGRAMA ESPÍA PREDATOR

Este capítulo resume el historial de venta mundial de tecnologías de vigilancia de la alianza Intellexa. Pese a las reiteradas informaciones sobre casos de uso indebido de sus herramientas para vigilar ilegítimamente a personas y organizaciones, nuestras conclusiones muestran, una vez más, la insuficiencia de las salvaguardias diseñadas para prevenir este tipo de usos abusivos, incluso dentro de la UE. A continuación se expone la forma en que se puede usar el programa espía Predator de Intellexa para infectar dispositivos —sobre la base de folletos y documentos técnicos obtenidos por EIC—, lo que demuestra que esta tecnología es intrínsecamente causante de abusos contra los derechos humanos.

La mayor parte del capítulo está dedicada a un caso descubierto por el Laboratorio sobre Seguridad de Amnistía Internacional en el que se usó el programa espía Predator de Intellexa contra diversos sujetos. Este caso práctico muestra cómo un operador del programa espía de Intellexa puede atacar cuentas de personas e instituciones para tratar de infectar sus dispositivos, como ilustra una reciente campaña dirigida contra un periodista de Vietnam y la sociedad civil, así como contra personalidades políticas de la UE, Estados Unidos y otros países que trabajan en temas de interés para el gobierno de Vietnam. El Laboratorio sobre Seguridad de Amnistía Internacional no ha confirmado ningún caso de infección relacionado con este caso práctico que, sin embargo, sí demuestra que un operador podría atacar a personas y organizaciones de todo el mundo con una forma de programa espía altamente invasivo. El capítulo concluye con la valoración de Amnistía Internacional sobre la responsabilidad de este uso del programa espía Predator.

4.1 UNA HISTORIA DE USOS ABUSIVOS DE LA VIGILANCIA

El grupo Intellexa se publicita como una "empresa regulada y radicada en la UE".[35] Según la documentación financiera anual de la empresa matriz de Intellexa, Thalestris Ltd., la actividad principal de Intellexa es "proporcionar productos de inteligencia a organismos encargados de hacer cumplir la ley".[36] Según informes, la alianza Intellexa está integrada por Nexa Technologies y Advanced Middle East Systems (grupo Nexa), así como por WiSpear, Cytrox y Senpai Technologies (grupo Intellexa).[37] Los grupos de empresas Nexa e Intellexa controlan múltiples entidades corporativas, algunas de las cuales han cambiado de denominación. Estas

[35] Intellexa, https://web.archive.org/web/20230719063910/https://intellexa.com/ (consultado por última vez el 19 de julio de 2023).
[36] Thalestris Limited, "Annual report and consolidated financial statements for December 2021", p. 29 (consultado por última vez en agosto de 2023).
[37] Nexa Technologies, "Intellexa Alliance: Intellexa, The Intelligence Alliance, to Provide Unmatched End-To-End Intelligence Solutions for Law Enforcement and Intelligence Agencies", 16 de febrero de 2019, https://web.archive.org/web/20200109072024/https://www.nexatech.fr/intellexa-alliance-press-news; Fast Company, "Inside the shadowy world of spyware makers that target activists and dissidents", 26 de junio de 2019, https://www.fastcompany.com/90369108/inside-the-shadowy-world-of-spyware-makers-that-target-activists-and-dissidents.

entidades operan en varias jurisdicciones, tanto dentro como fuera de la UE, entre otras en las de Grecia, Irlanda, Francia, Alemania, República Checa, Chipre, Hungría, Macedonia del Norte, Suiza, Israel y Emiratos Árabes Unidos (EAU).[38]

Las entidades y los países que se enumeran aquí son una relación no exhaustiva de la presencia corporativa de la alianza Intellexa. La naturaleza exacta de los vínculos entre estas empresas está envuelta en secretismo, ya que las entidades corporativas y las estructuras entre ellas se transforman, se rebautizan, cambian de marca y evolucionan constantemente. Como en el caso de otros proveedores de programas espía como el conocido NSO Group, estas estructuras corporativas opacas e incesantemente complejas facilitan que las empresas eludan la rendición de cuentas, la transparencia y la normativa gubernamental, incluidos los controles de exportación regionales y nacionales, así como los mecanismos de diligencia debida corporativa.[39] En el caso de la alianza Intellexa, el panorama es aún más complejo debido a las estructuras corporativas no sólo de una empresa principal, sino de los proveedores de productos de vigilancia aliados, las empresas matrices y sus inversores. Todo esto hace que el panorama completo sea aún más complejo y opaco, lo que dificulta más todavía la rendición de cuentas y la transparencia en lo que se refiere a la vigilancia ilegítima con herramientas de esta alianza.

Estas revelaciones distan de ser la primera vez que se relaciona a las empresas de la alianza Intellexa con abusos contra los derechos humanos en el mundo. En 2011, la Federación Internacional de los Derechos Humanos (FIDH) y la Liga de Derechos Humanos (LDH) presentaron una denuncia penal contra Amesys por complicidad en actos de tortura por ventas de tecnología de vigilancia a Libia realizadas en 2007.[40]

La FIDH y la LDH presentaron una segunda denuncia en 2017 en relación con la venta de la misma tecnología a Egipto por Nexa Technologies en 2014, lo que hizo que la justicia francesa abriera una segunda investigación penal por complicidad en tortura y desaparición forzada contra Nexa.[41] Nexa Technologies y varios miembros de su personal directivo fueron acusados formalmente en relación con esta segunda investigación en 2021, pero el tribunal de apelación de París anuló la acusación formal un año después.[42] Nexa es una de las empresas que forma parte de la alianza Intellexa.

En 2021, Citizen Lab halló que una figura política exiliada y una persona profesional del periodismo de Egipto habían sido hackeadas por el programa espía Predator.[43] En 2022, una serie de investigaciones y revelaciones dieron a conocer que el periodista griego Thanasis Koukakis y el líder de un partido de la oposición en Grecia y miembro del Parlamento Europeo Nikos Androulakis habían sido atacados con Predator, y que el Servicio Nacional de Inteligencia (NIS) griego había intervenido sus teléfonos.[44] También se publicó en un periódico una lista de personas muy conocidas que al parecer estaban sometidas a vigilancia

[38] Departamento de Estado de Estados Unidos, "The United States Adds Foreign Companies to Entity List for Malicious Cyber Activities", 18 de julio de 2023, https://www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities-2/; Parlamento Europeo, Recomendación del Parlamento Europeo, de 15 de junio de 2023, al Consejo y a la Comisión a raíz del examen de las alegaciones de infracción y de mala administración en la aplicación del Derecho de la Unión en relación con el uso del programa espía de vigilancia Pegasus y otros programas equivalentes, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_ES.html; Citizen Lab, "Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware" (antes citado), https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/; https://www.business-humanrights.org/de/unternehmen/nexa-technologies/CRFS, Nexa Technologies https://www.crfs.com/partner/nexa-technologies/ (consultado por última vez el 26 de septiembre de 2023); Intelligence Online, *France's Nexa acquires European interception specialist Trovicor*, 3 de diciembre de 2019, https://www.intelligenceonline.com/surveillance--interception/2019/12/03/france-s-nexa-acquires-european-interception-specialist-trovicor,108384645-art, 3 diciembre de 2019, https://www.intelligenceonline.com/surveillance--interception/2019/12/03/france-s-nexa-acquires-european-interception-specialist-trovicor,108384645-art.

[39] Amnistía Internacional, *Operating in the shadows*: *Inside NSO Group's Corporate Structure* (Índice: DOC 10/4182/2021), 31 de mayo de 2021, https://www.amnesty.org/es/documents/doc10/4182/2021/en/.

[40] Federación Internacional de los Derechos Humanos, "FIDH and LDH file a complaint concerning the responsibility of the company AMESYS in relation to acts of torture", 19 de octubre de 2011, https://www.fidh.org/en/region/north-africa-middle-east/libya/FIDH-and-LDH-file-a-complaint.

[41] Federación Internacional de los Derechos Humanos, "Vigilancia y tortura en Egipto y Libia: varios dirigentes de Amesys y Nexa Technologies imputados", 22 de junio de 2021, https://www.fidh.org/es/region/magreb-y-medio-oriente/egipto/vigilancia-y-tortura-en-egipto-y-libia-varios-dirigentes-de-amesys-y.

[42] Tech Xplore, "Charges dropped against French company over Egypt spyware", 14 de diciembre de 2022, https://techxplore.com/news/2022-12-french-company-egypt-spyware.html.

[43] Citizen Lab, "Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware" (antes citado), https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/.

[44] Inside Story, " Από τον Κουκάκη στον Ανδρουλάκη: Νέα τροπή στην υπόθεση του spyware Predator", 27 de julio de 2022, https://insidestory.gr/article/apo-koykaki-androylaki-nea-tropi-ypothesi-predator; Parlamento Europeo, *INFORME sobre el examen de las alegaciones de infracción y de mala administración en la aplicación del Derecho de la Unión en relación con el uso del programa espía de vigilancia Pegasus y otros programas equivalentes* (2022/2077(INI)), 22 de mayo de 2023, https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_ES.html; Amnistía Internacional, *Greece's surveillance scandal must shake us out of complacency*, 26 de enero de 2023, https://www.amnesty.org/en/latest/news/2023/01/greeces-surveillance-scandal-must-shake-us-out-of-complacency/.

estatal o habían sido atacadas con Predator.[45] En 2023, se reveló que un miembro de la dirección de Meta de nacionalidad estadounidense-griega había sido atacado con Predator y que, según informes, el NIS había intervenido su teléfono.[46] Una investigación sobre el uso de Predator llevada a cabo por la entidad griega encargada de la vigilancia de la privacidad (la Autoridad Helénica de Protección de Datos) localizó 350 SMS que trataban de instalar software de vigilancia y encontró 92 objetivos.[47]

En septiembre de 2023, Citizen Lab reveló que entre un ex parlamentario egipcio había sido atacado con el programa espía Predator.[48]

En julio de 2023, la Oficina de Industria y Seguridad del gobierno estadounidense incluyó cuatro entidades corporativas que formaban parte de la alianza Intellexa en su lista de entidades que llevaban a cabo actividades informáticas maliciosas afirmando que "participaban en el tráfico de *exploits* informáticos utilizados para obtener acceso a sistemas de información, lo que representa[ba] una amenaza para la privacidad y la seguridad de personas y organizaciones de todo el mundo."[49] Estas entidades corporativas son Intellexa S. A. en Grecia, Intellexa Limited en Irlanda, Cytrox AD en Macedonia del Norte, y Cytrox Holdings Crt en Hungría.

Dado que empresas de las propias entidades corporativas del grupo Nexa y el grupo Intellexa son sospechosas de abusos contra los derechos humanos cometidos en Grecia, Egipto y Libia, Amnistía Internacional les escribió preguntándoles qué medidas habían adoptado tras la publicación de estas primeras revelaciones para garantizar que operan de una forma respetuosa con los derechos humanos y con arreglo a los Principios Rectores de la ONU, y qué pasos habían dado para proporcionar una reparación a las personas afectadas. En el momento de la publicación, la organización no había recibido respuesta. Sin embargo, exmiembros del personal directivo del grupo Nexa respondieron a entidades asociadas de EIC en nombre de sus empresas, incluidas Nexa Technologies y Advanced Middle East Systems, afirmando que (traducción de Amnistía Internacional):

> "Nunca hemos subestimado el dilema ético que plantea nuestro trabajo. Sabíamos que algunos de los países con los que pudimos entablar relaciones comerciales distaban mucho de ser perfectos en lo que se refiere al Estado de derecho. No obstante, también éramos conscientes del hecho de que nuestro planteamiento era, la mayoría de las veces, parte de un esfuerzo de la comunidad internacional para ayudar a estos países a ir hacia la democracia."
>
> "Al exponer los dilemas morales muy concretos que hemos tenido que afrontar durante nuestra vida profesional, acabamos de mencionar el papel de las autoridades y, en concreto, de las autoridades francesas en lo que se refiere a la exportación de una solución francesa. En varios de los países controvertidos que mencionan, no sólo hemos obtenido autorización de exportación, sino que, además, no hemos hecho más que seguir la vía de estrecha colaboración iniciada por Francia con estos mismos países."

Su respuesta proseguía:

> "Las empresas francesas deben poder actuar dentro de un marco normativo claro."
>
> "Confiábamos en que las autoridades nos dieran luz verde. Desde entonces, a partir de 2021, venimos tratando de avanzar con asesoramiento externo para comprender mejor la realidad en el terreno de diferentes países y poder evaluar los riesgos de violaciones de derechos fundamentales. Por eso hemos establecido un proceso que recurre a personas ajenas a la empresa especializadas en derechos humanos."

---

[45] Documento, "Αποκάλυψη: Αυτούς παρακολουθούσε – Αυτή την Κυριακή στο Documento", 5 de noviembre de 2022, https://www.documentonews.gr/article/apokalypsi-aytoys-parakoloythoyse-ayti-tin-kyriaki-sto-documento/; *The Economist*, "Fresh allegations in a Greek phone-hacking scandal", 10 de noviembre de 2022, https://www.economist.com/europe/2022/11/10/fresh-allegations-in-a-greek-phone-hacking-scandal.

[46] *The New York Times*, "Meta Manager Was Hacked With Spyware and Wiretapped in Greece", 20 de marzo de 2023, https://www.nytimes.com/2023/03/20/world/europe/greece-spyware-hacking-meta.html; Parlamento Europeo, *INFORME sobre el examen de las alegaciones de infracción y de mala administración en la aplicación del Derecho de la Unión en relación con el uso del programa espía de vigilancia Pegasus y otros programas equivalentes* (antes citado), https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_ES.html.

[47] Euroactiv, "Privacy watchdog finds 92 'targets' in Greek wiretapping scandal", 21 de julio de 2023, https://www.euractiv.com/section/politics/news/privacy-watchdog-finds-92-targets-in-greek-wiretapping-scandal/.

[48] Citizen Lab, "Predator in the Wires: Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions", 22 de septiembre de 2023, https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-presidential-ambitions/.

[49] Departamento de Estado de Estados Unidos, "The United States Adds Foreign Companies to Entity List for Malicious Cyber Activities" (antes citado), https://www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities-2/.

> "Siguiendo su opinión, tomamos la decisión de cesar en todas las relaciones comerciales con un Estado. En los últimos dos años, también nos hemos negado a entablar relaciones comerciales con varios Estados más."

En cuanto al cumplimiento de la normativa sobre control de exportaciones, afirmaron:

> "Como hemos explicado antes, todos los contratos comerciales de las empresas que nombran ustedes cumplieron escrupulosamente la normativa sobre exportación."
>
> "Como hemos explicado en la introducción, cuando obteníamos autorización del SBDU, considerábamos de buena fe que nuestro producto podía exportarse legalmente, y más aún en el caso de un país como Egipto, con el que las autoridades francesas mantenían una intensa cooperación que exaltaban y en cuyo territorio nuestra propia seguridad [la de Francia] estaba también en juego. Esta es precisamente una de las razones por las que el Tribunal de Apelación de París anuló las acusaciones formales formuladas en contra nuestra en diciembre de 2022, como informó la prensa."
>
> "Contrariamente a lo que piensan ustedes, el lugar de inscripción en registro de nuestras empresas nunca tuvo como intención eludir la normativa, sino que se basaba en una lógica empresarial porque nuestros clientes requerían a menudo una presencia local."

En respuesta a EIC sobre ventas de Predator, su contestación también dice que:

> "Denunciamos estos contratos [incluido el suscrito con Vietnam] después de la investigación judicial de 2021, que nos hizo ser conscientes de los riesgos relacionados con estos acuerdos. Nos dimos cuenta de que las autorizaciones concedidas no nos protegían lo suficiente y no constituían ninguna garantía frente a violaciones de derechos humanos."

Dada la naturaleza del sector de los programas espías y su capacidad para facilitar abusos contra los derechos humanos, junto con el propio conocimiento de la alianza Intellexa de casos anteriores de abusos, la alianza de empresas de vigilancia sabía, o debía haber sabido razonablemente, que podían cometerse abusos contra los derechos humanos. Además, habida cuenta del historial de abusos contra los derechos humanos que se detalla en este apartado, las autoridades de exportación y otras autoridades estatales tenían avisos de sobra de la probabilidad de que las ventas de productos de la alianza Intellexa planteasen graves riesgos para los derechos humanos.

4.2 EL SOFTWARE ESPÍA PREDATOR DE INTELLEXA

El sistema de software espía Predator de Intellexa es una forma de software espía altamente invasivo que obtiene por defecto acceso total a todos los datos almacenados o transmitidos desde el dispositivo infectado y que está diseñado para no dejar rastro en dicho dispositivo y hacer imposible cualquier auditoría independiente de posibles abusos. En este sentido, Predator es fundamentalmente incompatible con los derechos humanos y debería ser prohibido.

El análisis del Laboratorio sobre Seguridad de Amnistía Internacional de folletos y documentación técnica facilitada por EIC proporciona nuevos conocimientos sobre el funcionamiento de este programa espía a nivel técnico y los métodos con los que infecta los dispositivos objetivo.

Según estos documentos, las infecciones del programa espía Predator se gestionan a través de un sistema basado en la web que Intellexa denomina "Plataforma de Operaciones Cibernéticas". La interfaz de Predator permite que el operador del programa espía inicie intentos de infección contra un teléfono objetivo y, si tiene éxito, recupere y acceda a información sensible como fotos, datos de ubicación, mensajes de chat y grabaciones del dispositivo infectado.

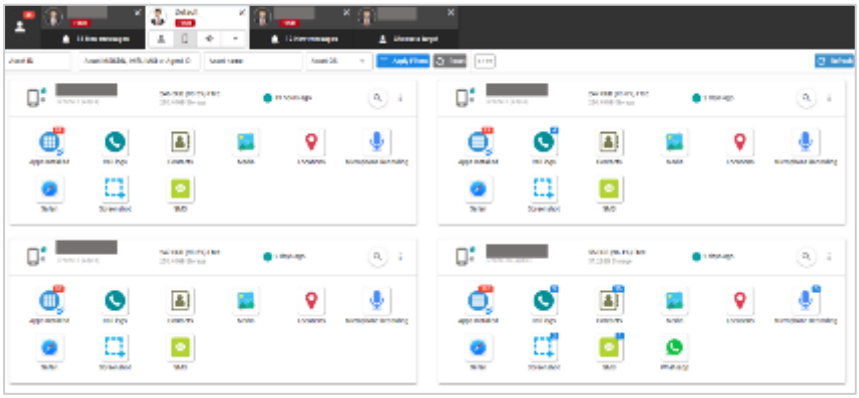

Figura 1: Interfaz del software espía Predator de Intellexa (fuente: documentos de EIC)

El sistema Predator completo incluye varios programas y componentes de infraestructura, a saber: el agente del programa espía en sí que se instala en el dispositivo objetivo y los *exploits* de software y vectores de ataque necesarios para instalar subrepticiamente el programa espía en el teléfono objetivo. La empresa ha usado varios nombres comerciales para sus productos de software espía para dispositivos móviles: Green Arrow para su agente de programa espía para Android; Red Arrow para su agente de programa espía para iOS; y Predator, Helios y NOVA, entre otros. En este informe nos referimos a este producto de software espía para dispositivos móviles en general como Predator, pues creemos que todos estos nombres de productos se refieren al mismo conjunto de tecnologías de software espía relacionadas desarrolladas originalmente por Cytrox y que sigue desarrollando, comercializando y vendiendo la alianza Intellexa.

El código *exploit* y las cargas del programa espía se envían al dispositivo objetivo desde lo que Intellexa denomina su "servidor de instalación". Una vez infectado el teléfono con el agente Predator, el dispositivo se conecta a una red de mando y control (CNC) donde los operadores pueden emitir órdenes al agente, por ejemplo, para recuperar ciertos archivos o activar el micrófono. Las órdenes se envían al dispositivo a través de una red de anonimización que tiene como fin ocultar la ubicación y la identidad del operador del programa espía y hacer más difícil que el personal de investigación identifique la fuente y la naturaleza de los ataques. El "servidor de instalación" y los servidores CNC deben ser accesibles públicamente en Internet para permitir las conexiones desde los dispositivos objetivo. Otros servidores, como la red de anonimización y el "Núcleo de Operaciones Cibernéticas" pueden ubicarse tras un cortafuegos o estar aislados dentro de la red del cliente Predator.

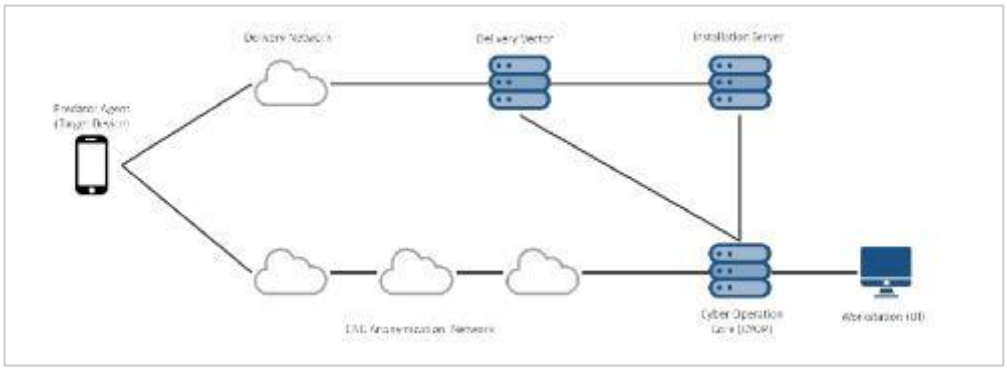

Figura 2: Arquitectura de servidor de alto nivel (fuente: documentos de EIC)

Se pueden usar diversos vectores de infección de 1 clic y 0 clics para infectar un dispositivo determinado. Algunos ataques documentados públicamente con anterioridad ligados a Predator se lanzaron a través de mensajes de ingeniería social que contenían una URL maliciosa, lo que se conoce como ataques de 1 clic.[50] El éxito de los ataques de programa espía de 1 clic depende de la capacidad del operador del programa espía para generar confianza en el objetivo y personalizar la URL de ataque y el mensaje de manera que incite al

[50] Citizen Lab, "Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware" (antes citado), https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/; Inside Story, "Predatorgate: Τι έγραφαν τα SMS-παγίδα που έλαβαν επιχειρηματίες, υπουργοί και δημοσιογράφοι", 27 de julio de 2023, https://insidestory.gr/article/predatorgate-ti-egrafan-ta-sms-pagida-poy-elavan-epiheirimaties-ypoyrgoi-kai-dimosiografoi.

objetivo a abrir el enlace. En este informe nos centraremos en los ataques de 1 clic que también identificamos que fueron usados en los ataques que se describen en el siguiente apartado.[51]

Si el teléfono seleccionado está ejecutando un navegador y una versión del sistema operativo compatibles, se enviará una cadena de *exploit* que primero infectará el navegador y después intentará aumentar sus privilegios e instalar el agente de programa espía completo en el dispositivo. Estos ataques de 1 clic son especialmente potentes, pues pueden usarse para infectar un dispositivo vulnerable en cualquier lugar del mundo simplemente abriendo un enlace.

4.3 CASO PRÁCTICO DE PREDATOR: @JOSEPH_GORDON16

En abril de 2023, el Laboratorio sobre Seguridad de Amnistía Internacional identificó una cuenta de Twitter (actualmente X) que, con el nombre de usuario @Joseph_Gordon16, compartía públicamente enlaces que contenían enlaces de infección de Predator de Intellexa. La cuenta fue identificada por primera vez en búsquedas en Internet de dominios activos de Intellexa que el Laboratorio sobre Seguridad había identificado gracias a su labor en curso de rastreo de infraestructura de software espía de Intellexa.

Después de identificar la cuenta del atacante, el Laboratorio sobre Seguridad de Amnistía Internacional observó, durante un periodo de dos meses, decenas de casos en los que la cuenta @Joseph_Gordon16 envió tuits públicos y respuestas a tuits de otros usuarios que contenían enlaces a URL maliciosas acortadas y de sitios web de noticias suplantados. Amnistía Internacional pudo relacionar estos enlaces con dominios de Predator de Intellexa conocidos descubiertos durante una investigación anterior. En concreto, los dominios lnktonews[.]co y witteridea[.]co, tuiteados ambos por la cuenta @Joseph_Gordon16, habían sido identificados con anterioridad en la investigación del Laboratorio sobre Seguridad como dominios de Predator activos de URL acortadas. Los dominios de ataques espía de 1 clic y de URL acortadas suelen ser registrados con nombres engañosos para hacer creer al objetivo que el enlace es legítimo. Uno de los dominios, lnktonews[.]co, sugiere que el enlace lleva a una noticia. El segundo, witteridea[.]co, imita un enlace relacionado con la plataforma Twitter/X.

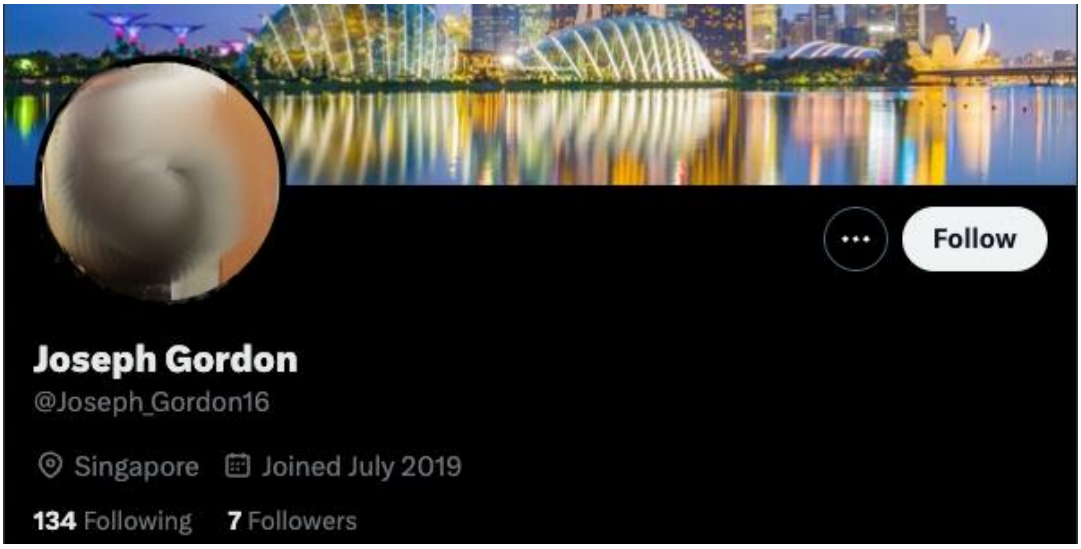

Figura 3: Captura de pantalla de la cuenta @Joseph_Gordon16

Tras el descubrimiento por Amnistía Internacional de los tuits de ataque iniciales, la cuenta @Joseph_Gordon16 siguió tuiteando enlaces sospechosos de dominios recién creados como asean-news[.]net, southchinapost[.]net y caavn[.]org. Tanto asean-news[.]net como southchinapost[.]net coincidían con patrones asociados a servidores conocidos de Predator.

[51] Estas URL de infección suelen tener también un límite de tiempo y restricciones geográficas para que al personal de investigación le resulte más difícil analizar la totalidad de los enlaces de ataque o capturar las tan valiosas muestras del *exploit* de día cero usado para infectar dispositivos totalmente actualizados.

Amnistía Internacional compartió un subconjunto de esta actividad con otros equipos de investigación sobre seguridad, como el Grupo de Análisis de Amenazas de Google, que tiene un historial de rastreo de campañas de ataques y *exploits* llevadas a cabo por la alianza Intellexa y otros proveedores de vigilancia comercial.[52] El Grupo de Análisis de Amenazas de Google confirmó a Amnistía Internacional que la propia investigación de Google había determinado que los dominios y las URL compartidos por la cuenta @Joseph_Gordon16, incluidos southchinapost[.]net, Inktonews[.]co y witteridea[.]co, son parte del sistema de software espía Predator de Intellexa.

El equipo de investigación del Grupo de Análisis de Amenazas de Google también logró acceder a las URL de infección de Predator tuiteadas por la cuenta @Joseph_Gorden16 mientras estuvo activa. El enlace acortado a la URL maliciosa original alojado en southchinapost[.]net redirigía a un servidor de instalación de Predator en scanningandinfo[.]online. En este caso, el servidor de instalación no intentó enviar un *exploit* ni infectar al dispositivo de prueba.

OBJETIVO	URL
Página de aterrizaje de la URL acortada	https://southchinapost[.]net/eNISDKnI
Servidor de instalación de Predator	https://scanningandinfo[.]online/jbz7xv9xox0bn2ya3gat39i64/xfer-ovc?sip=2d2c3a697858f315177940709c236a69
Servidor de instalación de Predator	https://scanningandinfo[.]online/jbz7xv9xox0bn2ya3gat39i64/xfer-ovc?r=true&sip=2d2c3a697858f315177940709c236a69

Tabla 2: Ejemplo de cadena de redirección desde el enlace de Predator compartido por @Joseph_Gordon16

Un tercer dominio, caavn[.]org, compartido por la cuenta de X @Joseph_Gordon16 ya no estaba online cuando se hizo el análisis, lo que nos impidió determinar si tenía la huella digital de los servidores de Intellexa. El dominio caavn[.]org estaba alojado anteriormente en la dirección IP 212.90.121.247, que también alojaba otros dos dominios que imitaban sitios web vietnamitas legítimos, xuatnhapcanhvn[.]info y tokhaiytehanoi[.]org.[53] La aparición de múltiples nombres de dominio relacionados con Vietnam en el mismo servidor de Internet en torno al mismo periodo y registrados en el mismo registrador de nombres de dominio indica que los tres dominios fueron registrados por el mismo operador.

Figura 4: Dominio caavn[.]org controlado por un atacante que imita un artículo de prensa del South China Morning Post

A diferencia de las URL acortadas antes referidas, el tuit caavn[.]org contenía una URL completa similar a la de una noticia publicada por el diario *South China Morning Post*. La imitación de una noticia o una página web legítimas podría ser otra técnica de ataque usada por los atacantes para incitar al objetivo a abrir el enlace. La vista previa del enlace que mostraba X se corresponde con el dominio auténtico del diario *South*

[52] Grupo de Análisis de Amenazas de Google, "Protecting Android users from 0-Day attacks", 19 de mayo de 2022, https://blog.google/threat-analysis-group/protecting-android-users-from-0-day-attacks/.
[53] Los nombres de dominio son visualmente similares al del departamento oficial de inmigración del Ministerio de la Policía de Vietnam (xuatnhapcanh.gov.vn) y al de un sitio web usado en Vietnam para registrar declaraciones de salud durante la pandemia de COVID-19 (tokhaiyte.vn).

China Morning Post en scmp.com, lo que sugiere que los atacantes habían configurado su enlace malicioso para que redirigiera al *South China Morning Post* como sitio web reclamo mostrado cuando accediera a él el generador de vistas previas de enlaces de X (véase la figura 4).

El hecho de que algunos de los dominios de Intellexa usados en los ataques estuvieran diseñados para imitar sitios web vietnamitas legítimos sugiere una relación con actores ligados a Vietnam que está respaldada por indicios circunstanciales significativos basados en un análisis de la cuenta en X del atacante y de los antecedentes de los objetivos. El primer tuit de la cuenta, de 2020, está en vietnamita. La cuenta envió después otros tuits que contenían un nombre de dominio controlado por el atacante a Thời Báo, sitio de noticias vietnamita radicado en Alemania, como se expone con más detalle en el apartado 4.4.1 *infra*.

Figura 5: Uno de los primeros tuits de @Joseph_Gordon16, escrito en vietnamita

4.4 OBJETIVOS DE @JOSEPH_GORDON16

Los intentos de ataque, de gran alcance y públicos, con software espía por la cuenta de X @Joseph_Gordon16 permitieron que el Laboratorio sobre Seguridad de Amnistía Internacional conociera las metas del operador de Predator de Intellexa que estaba detrás de esta campaña de ataques. Entre los objetivos seleccionados por esta cuenta había periodistas, personal de investigación del ámbito académico que trabajaba sobre cuestiones de seguridad en el Mar de China Meridional y Vietnam, así como altos cargos políticos de la UE, Estados Unidos y otros países relacionados con la regulación de la pesca internacional, cuestión de interés para las autoridades vietnamitas (véase el apartado 4.4.2).

En el siguiente apartado se exponen varios de los principales casos de intentos de ataque contra periodistas, miembros de la sociedad civil y otras figuras públicas. Aunque el perfil y la ubicación de los objetivos es diverso, en muchos casos éstos son relevantes para los intereses políticos, militares y de inteligencia de Vietnam.

En el anexo II de este informe figura una lista completa de tuits.

CATEGORÍA	NÚMERO DE INTENTOS DE ATAQUE CON SOFTWARE ESPÍA
Medios de comunicación	16
Instituciones académicas	2
Figuras políticas/instituciones	27
Grupos consultivos	6
Otros	7

Tabla 3: Ejemplo de cadena de redirección desde el enlace de Predator compartido por @Joseph_Gordon16

4.4.1 ATAQUES CONTRA THOIBAO. DE

Uno de los primeros tuits de ataque enviados por la cuenta de X @Joseph_Gordon16 estaba dirigido a un sitio web de noticias independiente radicado en Berlín: Thời Báo, que publica noticias sobre Vietnam. El tuit se envió en respuesta a un artículo publicado por Thời Báo relativo a una investigación sobre corrupción en la que estaba implicado el Ministerio de Defensa de Vietnam. En la respuesta, escrita en vietnamita, el operador de la cuenta sugiere que la investigación sobre corrupción tiene relación con luchas internas o una lucha por el poder entre el Ministerio de Seguridad Pública y las fuerzas armadas de Vietnam (figura 6).

Figura 6: Texto del tuit de ataque a Thoibao.de: Công an đấu đá nội bộ, Bộ Công an bắt công an Hải Dương

Puede parecer que el enlace incluido, Inktonews[.]co pertenece a un sitio web de noticias, pero en realidad es un enlace a la infraestructura de infección de Predator que al parecer trató de infectar con el software espía Predator a personas relacionadas con esta organización de medios de comunicación.

FECHA	PARA	URL	PLATAFORMA
09/02/2023	thoibao_de	https://Inktonews[.]co/MEmK	X

Tabla 4: Enlace de infección de Predator enviado a Thoibao.de en X

Este intento de atacar e infectar con software espía a una organización de medios de comunicación radicada en la UE y a quienes trabajan en ella es una amenaza clara para la capacidad de las personas que se dedican al periodismo de informar y publicar abiertamente sobre temas relevantes para su audiencia incluso en comunidades de la diáspora. El riesgo también puede ser extremadamente grave para las fuentes periodísticas que se comunican con periodistas que después son objeto de hackeo.[54]

Khoa Lê Trung en su oficina. © Amnesty International.

[54] Véase, por ejemplo, Amnistía Internacional, *Uzbekistan: Tentacles of mass surveillance spread across borders*, 31 de marzo de 2017, https://www.amnesty.org/en/latest/news/2017/03/uzbekistan-tentacles-of-mass-surveillance-spread-across-borders/.

KHOA LÊ TRUNG, REDACTOR JEFE DE THOIBAO.DE

Khoa Lê Trung es un periodista de Vietnam que vive en Berlín (Alemania) y es redactor jefe de Thoibao.de. La cuenta de Thoibao.de fue atacada con software espía Predator de Intellexa, enviado en X como ataque de 1 clic.

Thoi Bao informa sobre temas políticos, económicos y medioambientales de Vietnam y del mundo. El derecho a recibir y difundir información dentro de Vietnam está indebidamente restringido debido al panorama represivo para los medios de comunicación imperante en el país, donde quienes expresan opiniones críticas online se exponen a ser objeto de intensa represión.[55] Khoa Lê Trung intenta contrarrestar esto con reportajes en Thoi Bao, para garantizar a la ciudadanía vietnamita el acceso a información precisa. El sitio web recibe 20 millones de visitas al mes y es una de las plataformas de medios de comunicación vietnamitas que funcionan desde el exilio más visitada.

La vigilancia selectiva de la clase que se expone en este informe es una de las numerosas formas de represalia que afronta la profesión periodística por su trabajo en Vietnam y en el mundo. Esta vigilancia suele ir acompañada de intimidación, hostigamiento y censura online. El ataque contra Thoi Bao con el software espía Predator de Intellexa es sólo una muestra de una serie de ejemplos de represión dentro y fuera de Internet que Khoa Lê Trung ha afrontado a lo largo de los años.

“No se pueden vender [tecnologías de vigilancia] sin más a países como Vietnam [...] este software occidental, hardware occidental se vuelve contra Alemania o [los países] europeos. Esto también daña la libertad de prensa y la libertad de expresión de la ciudadanía aquí, en Alemania”.
Khoa Lê Trung

Debido a su trabajo en Thoi Bao, Khoa Lê Trung ha recibido amenazas de muerte y ha sido objeto de intimidación por el mero hecho de ejercer su derecho a la libertad de expresión. Dijo a Amnistía Internacional: “También recibo amenazas, especialmente de vietnamitas en Alemania, también hay gente que me llama o me envía mensajes de texto y me amenaza [...] con cortarme la cabeza si sigo así. También hay personas que vienen directamente a mi despacho y me dicen: ‘No sigas con tus informes porque no es bueno para ti’.”. A causa de estas amenazas, Khoa Lê Trung está bajo protección policial en Berlín desde 2018.

Aunque la protección le hace sentir relativamente a salvo, también representa cierto grado de restricción en sus actividades cotidianas. “Cada vez que voy a un acto tengo que considerar si tiene sentido o no, y si vale la pena, porque siempre tengo que informar a la policía antes de ir. Por si ocurre algo en ese acto”, explicó a Amnistía Internacional.

La represión que sufre se extiende al ámbito de Internet. Khoa Lê Trung ha recibido amenazas, ha sido objeto de campañas de desprestigio online y ha sido calificado a menudo de “traidor”. Dijo a Amnistía Internacional que, desde 2017, cuando informó sobre un tema políticamente sensible relativo al secuestro de un hombre de negocios vietnamita en Berlín y sufrió presiones de la embajada vietnamita para que retirase la historia, el sitio web de Thoi Bao está bloqueado en Vietnam. Además, contó a Amnistía Internacional que también han bloqueado en el país su cuenta personal en Facebook y señaló que a menudo censuran sus vídeos en las redes sociales. Cuando las empresas de redes sociales retiran vídeos de noticias a petición de las autoridades, recuperarlos requiere tiempo y trabajo. Aun así, algunos se han perdido para siempre. “Tenemos que hacer muchas gestiones para que los devuelvan”, dijo a Amnistía Internacional. “Hay vídeos que puedo recuperar, pero también hay vídeos que no se pueden recuperar”, añadió.

El ataque más reciente con software espía Predator de Intellexa que se detalla en este informe no es el primer ciberataque que recibe. Explicó a Amnistía Internacional que el sitio web de Thoi Bao recibió ataques de denegación de servicio distribuido (DDoS) (véase el glosario) que provocaron la caída de la web. La práctica de los ataques con enlaces maliciosos en las redes sociales, como se

detalla en este informe, es peligrosa no sólo para él, sino también para otros y otras periodistas que trabajan para Thoi Bao. Khoa Lê Trung dijo a Amnistía Internacional: "[...] también hay muchos comentarios allí [en Thoibao.de] en los que sería peligroso hacer clic, pues es probable que el ordenador sea infectado y se averíe o que se puedan robar los datos. Es muy peligroso. Por eso tengo que tener mucho cuidado, incluso para las personas empleadas en mi sitio web." Como consecuencia de estos ataques, Khoa Lê Trung ha dedicado tiempo y recursos significativos para garantizar la seguridad digital de su sitio web y su propia seguridad y la de las personas que trabajan allí; tiempo y recursos que se podrían dedicar al trabajo y a reportajes periodísticos.

Khoa Lê Trung dijo a Amnistía Internacional que los ataques de vigilancia selectiva tienen un impacto sumamente perjudicial en quienes ejercen el periodismo o tienen blogs en Vietnam. Cree que detrás de estos ataques están las autoridades vietnamitas, que, según dice, invierten mucho para llevar a cabo ataques digitales contra disidentes online, incluida su plataforma de noticias.

Khoa Lê Trung explicó a Amnistía Internacional que los gobiernos europeos tienen la responsabilidad de controlar la venta y transferencia de tecnologías de vigilancia. "No se pueden vender [tecnologías de vigilancia] sin más a países como Vietnam [...] de forma que este software occidental, hardware occidental se vuelve contra Alemania o [los países] europeos. Esto también daña la libertad de prensa y la libertad de expresión de la ciudadanía aquí, en Alemania", dijo a Amnistía Internacional.

La investigación de Amnistía Internacional ha identificado con anterioridad otras presuntas campañas de software espía afines al Estado dirigidas contra activistas y blogueros vietnamitas radicados en Alemania. Una investigación de febrero de 2021 halló que el bloguero y activista en favor de la democracia Bui Thanh Hieu había sido atacado con software espía de Windows al menos cuatro veces entre febrero de 2018 y diciembre de 2019.[56] El destacado activista había sido hostigado reiteradamente por las autoridades vietnamitas antes de buscar refugio en Alemania, donde vive desde 2013. Otra persona que publicaba un blog en Vietnam, cuyo nombre no se dio a conocer por razones de seguridad, fue atacada tres veces entre julio y noviembre de 2020. Estos atacantes con software espía anteriores que tenían como objetivo activistas vietnamitas en Alemania están vinculados a un grupo de ataque conocido en el sector de la ciberseguridad como Ocean Lotus. Ocean Lotus también ha sido identificado en reiteradas ocasiones por empresas de ciberseguridad como atacante de disidentes políticos vietnamitas, gobiernos extranjeros y empresas.[57]

4.4.2 INTERESES EN EL SECTOR PESQUERO: ATAQUES CONTRA EL FUNCIONARIADO DE LA UNIÓN EUROPEA Y DE LA ONU

Una segunda categoría de personas atacadas por la cuenta en X @Joseph_Gordon16 abarca a múltiples personas del sector académico e institucional que trabajaban en asuntos marítimos, especialmente personal académico investigador y responsables de las políticas de la UE y de la ONU sobre pesca ilegal o indocumentada.

Los esfuerzos de la UE para combatir la pesca ilegal están recogidos en el reglamento sobre la eliminación de la pesca ilegal, no declarada y no reglamentada. En octubre de 2017, la Comisión Europea emitió una "tarjeta amarilla" por la que advertía a Vietnam de que no estaba tomando medidas suficientes para combatir la pesca ilegal. En la advertencia, se invitaba a las autoridades vietnamitas a "iniciar un procedimiento formal de diálogo para resolver los problemas detectados y aplicar el Plan de Acción".[58] Sin embargo, esta advertencia no detuvo la importación de productos de pescado y marisco de Vietnam a la UE, sino que indicaba que Vietnam estaba en riesgo de ser identificado como país no cooperador.

---

[55] Amnistía Internacional, *Viet Nam: Let Us breathe! Censorship and Criminalization of Online Expression in Viet Nam* (Índice: ASA 41/3243/2020), 30 de noviembre de 2020, https://www.amnesty.org/es/documents/asa41/3243/2020/en/.
[56] Amnistía Internacional, *Click and Bait: Vietnamese Human Rights Defenders Targeted with Spyware Attacks*, 24 de febrero de 2021, https://www.amnesty.org/en/latest/research/2021/02/click-and-bait-vietnamese-human-rights-defenders-targeted-with-spyware-attacks/.
[57] Amnistía Internacional, *Vietnamese activists targeted by notorious hacking group*, 24 de febrero de 2021, https://www.amnesty.org/en/latest/press-release/2021/02/viet-nam-hacking-group-targets-activist/; Reuters, "Facebook tracks 'OceanLotus' hackers to IT firm in Vietnam", 11 de diciembre de 2020, https://www.reuters.com/article/facebook-vietnam-cyber-idCAKBN28L03Y.
[58] Comisión Europea, "Commission warns Vietnam over insufficient action to fight illegal fishing", 23 de octubre de 2017, https://ec.europa.eu/commission/presscorner/detail/en/IP_17_4064.

El 16 de mayo de 2023, la cuenta @Joseph_Gordon16 respondió públicamente a una persona del ámbito académico español cuyo trabajo está dedicado a la política sobre pesca ilegal y caza furtiva (aunque no trabaja en cuestiones relacionadas con Vietnam). Este tuit contenía otro enlace de infección de Predator, esta vez alojado en asean-news[.]net (véase la figura 7). El tuit estaba escrito en español y se refiere directamente al procedimiento de la "tarjeta amarilla" de la UE. Dice: "¿Cuál es su solución para deshacerse de la tarjeta amarilla?"

Figura 7: Tuit de ataque enviado a una persona del ámbito académico español que investigaba la política de pesca

El 8 de febrero de 2023, la cuenta envió dos tuits con un enlace de ataque a Charlina Vitcheva (@vitcheva_eu), directora general de Asuntos Marítimos y Pesca de la Comisión Europea. Ambos tuits incluían un enlace de infección idéntico con el dominio de Predator witteridea[.]co y el mensaje: "How will this issue be resolved?" ("¿Cómo se va a resolver esta cuestión?"). La Dirección General de Asuntos Marítimos y Pesca de la Comisión Europea es la responsable de administrar los mecanismos sobre pesca ilegal, no declarada y no reglamentada, como el mecanismo de la "tarjeta amarilla". Uno de los tuits de ataque fue enviado en respuesta a un tuit público (véase la figura 8) de Charlina Vitcheva que mencionaba múltiples cuentas institucionales y públicas, como la de Pierre Karleskind (@Pierre_Ka), europarlamentario francés que preside la Comisión de Pesca del Parlamento Europeo (véase la figura 9). Las respuestas a un tuit en X, como el mensaje enviado por el atacante, se envían a todas las cuentas mencionadas en el tuit original. En la tabla 5 figura la lista completa de cuentas atacadas. La cuenta en X de la Misión Agua y Océanos de la UE también fue atacada dos veces con dos enlaces diferentes, el 9 de febrero de 2023 y, de nuevo, el 1 de junio de 2023 (véase la figura 10). El ataque contra esta cuenta académica y la referencia directa a la "tarjeta amarilla" de la UE en el mensaje de ataque, más el resto del personal y figuras políticas de la UE que se dedican a esta cuestión, sugiere que el tema es de interés directo para el operador que se halla detrás de esta campaña de infección con Predator.

Figura 8:
Atacante respondió a tuit de @vitcheva_eu sobre pesca mencionando otras cuentas

Figura 9: Cuenta @Pierre_Ka mencionada en el tuit original de @vitcheva_eu e incluida en la respuesta de ataque

Figura 10: Enlace de ataque de Predator enviado el 1 de junio de 2023

4.4.3 ATAQUES CONTRA OTRAS INSTITUCIONES Y ALTOS CARGOS

Esta investigación también identificó ataques de @Joseph_Gordon16 contra otros altos cargos de la UE y 11 instituciones ligadas a la Unión (incluidos los dirigidos contra la Misión Agua y Océanos mencionada en el apartado 4.4.2).

Cabe destacar que @Joseph_Gordon16 atacó la cuenta pública en X de la presidenta del Parlamento Europeo, Roberta Metsola, el 1 de junio de 2023 con el dominio de infección de Predator southchinapost[.]net.

Figura 11: Enlace de ataque enviado a Roberta Metsola, presidenta del Parlamento Europeo

En torno a esas fechas, @Joseph_Gordon16 atacó la cuenta institucional oficial en X de la Comisión Europea usando el mismo enlace de Predator enviado a Roberta Metsola.

Figura 12: Enlace de ataque enviado a una cuenta oficial de la Comisión Europea en X

La cuenta @Joseph_Gordon16 también atacó la cuenta en X de la embajadora alemana en Estados Unidos el 8 de marzo de 2023.

Figura 13: Enlace de ataque enviado a Emily Haber, embajadora de Alemania en Estados Unidos en aquel momento

FECHA	PARA	URL	PLATAFORMA
08/02/2023	@vitcheva_eu @EMODnet @cinea_eu @Pierre_Ka @EUgreenresearch @CMEMS_EU @FSUMDC @UNDPOceanInnov @REA_research @EU_ENV @EUClimateAction @eumissionocean	https://witteridea[.]co/LFJeZQu	X (antes Twitter)
08/02/2023	vitcheva_eu	https://witteridea[.]co/LFJeZQu	X
08/03/2023	GermanAmbUSA	https://Inktonews[.]co/CVgp	X
01/06/2023	EP_President	https://southchinapost[.]net/VuAfn	X
01/06/2023	EU_Commission	https://southchinapost[.]net/VuAfn	X
01/06/2023	EU_Commission	https://southchinapost[.]net/VuAfn	X
01/06/2023	eumissionocean	https://southchinapost[.]net/VuAfn	X

Tabla 5: Enlaces de ataque enviados a figuras políticas e instituciones de la UE

ATAQUES CONTRA AUTORIDADES ESTATALES DE ESTADOS UNIDOS Y TAIWÁN

El operador que actuaba tras la cuenta @Joseph_Gordon16 tuiteó un enlace de ataque dirigido a Tsai Ing-Wen, presidenta de Taiwán, el 14 de abril de 2023. Dado que el senador estadounidense por Dakota del Norte John Hoeven (@SenJohnHoeven) estaba etiquetado también en el tuit original de Tsai Ing-Wen, el tuit de respuesta y el enlace de ataque fueron enviados también, indirectamente, a la cuenta en X del senador (figura 14).

Figura 14: Enlace de ataque enviado a Tsai Ing-wen (@iingwen) y al senador estadounidense John Hoeven

El sitio web controlado por el atacante en caavn[.]org fue configurado, probablemente, para redirigir las peticiones de vista previa del enlace realizadas desde X al sitio web legítimo del *South China Morning Post*, a fin de crear una vista previa realista del enlace. Esta es una táctica habitual empleada para infectar dispositivos con software espía. En este caso, la vista previa contiene información de un artículo legítimo publicado en el sitio web del *South China Morning Post* sobre cooperación en materia de seguridad entre Estados Unidos y Taiwán.

En la misma fecha, @Joseph_Gordon16 dirigió también un enlace de ataque a la cuenta en X del Ministerio de Relaciones Exteriores de Taiwán. Dado que @Joseph_Gordon16 estaba respondiendo a un tuit que etiquetaba originalmente a un representante estadounidense —Michael McCaul, representante del 10º distrito de Texas—, éste habría recibido también automáticamente el mensaje de ataque. McCaul había sido

mencionado en el tuit original en su calidad de presidente de la Comisión de Asuntos Exteriores de la Cámara de Representantes del Congreso de Estados Unidos.

Figura 15: Enlace de ataque enviado al Ministerio de Relaciones Exteriores de Taiwán y al congresista estadounidense Michael McCaul

Figura 16: Enlace de ataque enviado a Tsai Ing-wen (@iingwen) con el nuevo dominio de infección de Predator southchinapost[.]net

El operador de @Joseph_Gordon16 regresó para atacar a Tsai Ing-Wen una vez más el 21 de mayo de 2023. En este intento de ataque se usó el dominio de infección de Predator southchinapost[.]net (figura 16).

ALTOS CARGOS E INSTITUCIONES DE ESTADOS UNIDOS Y DE TAIWÁN ATACADOS CON SOFTWARE ESPÍA DE PREDATOR

FECHA	PARA	URL	PLATAFORMA
14/04/23	@iingwen @SenJohnHoeven	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
14/04/23	@MofaTaiwan	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X
22/05/23	@iingwen	https://southchinapost[.]net/RtQBG	X

Tabla 6: Enlaces de ataque enviados a altos cargos e instituciones estadounidenses y taiwanesas

4.4.4 OTROS INTENTOS DE ATAQUE CON SOFTWARE ESPÍA PREDATOR LIGADOS A ESTE OPERADOR

Además de la cuenta en X @Joseph_Gordon16, Amnistía Internacional ha identificado otra cuenta de redes sociales que también envió enlaces que contenían los mismos dominios de software espía. La cuenta de Facebook Anh Tran compartió enlaces de Predator adicionales que contenían el dominio caavn[.]org. El uso del mismo nombre de dominio personalizado en enlaces enviados desde las dos cuentas confirma que ambas cuentas en redes sociales están probablemente relacionadas con el mismo operador de Predator.

Figura 18: Perfil de Facebook de la cuenta Anh Tran

Amnistía Internacional observó que esta cuenta posteaba dos comentarios públicos en marzo de 2023 en la página pública en Facebook de un grupo de la oposición política vietnamita, Liên Minh Dân Tộc Việt Nam, que está radicado en Estados Unidos.[59] Los enlaces de ataque se postearon públicamente en comentarios en Facebook y, en este caso, imitaban artículos publicados en el sitio web de noticias en lengua vietnamita Tiếng Dân (véase la figura 19).[60] El sitio web Tieng Dan ha sufrido con anterioridad ataques de denegación de servicio distribuido (DDoS) y ha sido objetivo del grupo Ocean Lotus.[61]

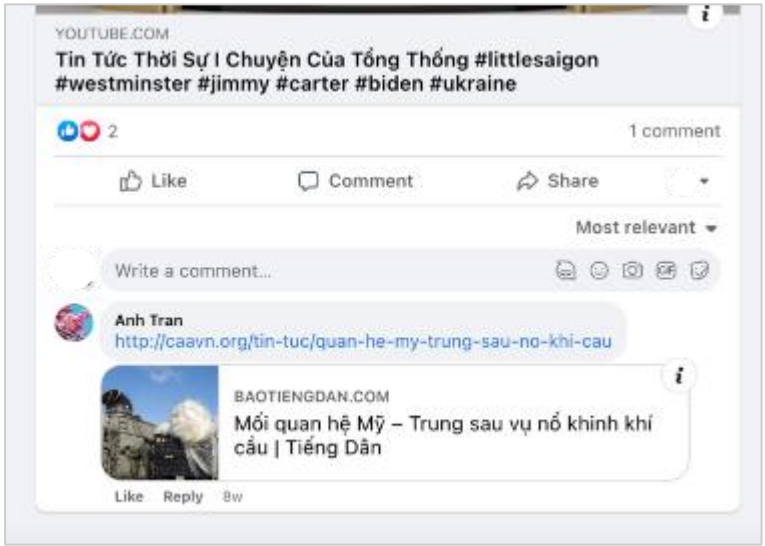

Figura 19: Enlace de ataque que imita a baotiengdan.com

El ataque adicional dirigido a un grupo político de la diáspora vietnamita en Facebook muestra el enfoque en curso del operador de Predator que está detrás de estos ataques. Estos enlaces de ataque compartidos en público representan probablemente sólo un subconjunto de los ataques generales ligados a esta campaña de vigilancia. Los intentos de ataque adicionales enviados a través de aplicaciones de mensajería instantánea o en mensajes directos son más difíciles de identificar para el personal de investigación.

[59] Facebook, Liên Minh Dân Tộc Việt Nam, https://www.facebook.com/LMDTVN/ (consultado por última vez el 26 de septiembre de 2023).
[60] Tiếng Dân, https://baotiengdan.com/ (consultado por última vez el 26 de septiembre de 2023).
[61] Deflect, "News From Deflect Labs: DDoS attacks against Vietnamese Civil Society", 7 de septiembre de 2018, https://deflect.ca/ddos-attacks-vietnamese-civil-society/.

4.5 VENTAS A VIETNAM DE LA ALIANZA INTELLEXA

Amnistía Internacional ha examinado adicionalmente informes y análisis elaborados por medios de comunicación asociados en EIC que se basaron en registros empresariales confidenciales de los que las organizaciones de medios de comunicación disponían como parte de la investigación sobre los Archivos Predator. Estos informes, compartidos con Amnistía Internacional antes de su publicación, exponen ventas de tecnologías de vigilancia de entidades de la alianza Intellexa a las autoridades vietnamitas. Tomados junto con los datos forenses y técnicos expuestos en el apartado 4.4, estos hallazgos de socios de EIC, como Mediapart y *Der Spiegel*, refuerzan las pruebas técnicas sobre el origen de los ataques.

Según la información de EIC, Nexa Technologies firmó un acuerdo de "soluciones de infección" con el Ministerio de Seguridad Pública de Vietnam a principios de 2020 a través de Advanced Middle East Systems, filial de ventas del grupo Nexa radicada en EAU. Su análisis muestra también que el proyecto, con el nombre en código "Angler Fish", se ofreció con una licencia de dos años y tenía un valor de 5,6 millones de euros. Un segundo documento de Nexa Technologies que ha visto EIC, fechado en enero de 2021, dice que los ingresos previstos en relación con este contrato eran de 3,36 millones de euros en 2021 y de 2,44 millones de euros en 2022.

El informe también identificó otro registro de previsión de ventas de 26 de enero de 2021 que mostraba que Advanced Middle East Systems intentaba obtener una "ampliación" del contrato con el Ministerio de Seguridad Pública vietnamita valorado en 800.000 euros por Blue Arrow. Las entidades de la alianza Intellexa usan la marca Arrow, incluidas Green Arrow y Red Arrow, como nombres comerciales de sus soluciones de software espía Predator. Los documentos de que disponía EIC no confirman si se firmó esta ampliación del contrato.

Según otros registros a los que tuvo acceso EIC, un mes después, el 19 de febrero de 2021, Advanced Middle East Systems vendió el software espía Arrow a la empresa Delsons Hong Kong Limited, registrada en Hong Kong. Registros públicos del registro de sociedades de Hong Kong[62] muestran que Delsons Hong Kong es propiedad de Alexis Delevaux, empresario suizo que vive en Asia y que también ejerce de cónsul honorario de Mónaco en Hanoi. Una filtración pública de correos electrónicos del proveedor de software espía Hacking Team incluye correos de Delevaux de 2011 en los que éste expresa interés en adquirir productos de software espía de Hacking Team[63] en nombre de clientes del Ministerio de Seguridad Pública de Vietnam (véase la figura 20).[64]

Dear Mr Marco Bettini,

Thank you for your prompt answer by email and for your information.

Our main target is Ministry of Public Security of Vietnam , in your particular field , they have several projects in the process. Customer will also be attending tomorrow some exhibition on the

If you are already in touch with end users in Vietnam I do understand and do not want to trouble you overlapping on the same customers. If you can disclose the name of your partner I can

If it is possible to cooperate on some projects, I have no issue to sign any NDA,

Best Regards

Alexis Delevaux

Figura 20: Correo electrónico filtrado sobre la compra de herramientas de programa espía de Hacking Team en nombre del Ministerio de la Seguridad Pública de Vietnam en 2011

Registros de exportación[65] obtenidos por Amnistía Internacional y EIC revelan que el 1 de noviembre de 2021 se enviaron por avión desde Delsons Hong Kong Ltd. a Vietnam 30 artículos de hardware informático por valor de 8,5 millones de dólares estadounidenses. El destinatario de los bienes era BCA - Thang Long Co., Ltd, una empresa de propiedad estatal establecida en Vietnam en 1993 por decreto del Ministerio de

[62] Integrated Companies Registry, https://www.icris.cr.gov.hk/csci/ (consultado por última vez el 2 de octubre de 2023).
[63] Hacking Team era un fabricante italiano de software espía que produjo el programa espía Galileo, vendido a numerosos países del mundo.
[64] WikiLeaks, "Hacking Team: [BULK] RE: demand information Vietnam following Milipol", 8 de julio de 2015, https://wikileaks.org/hackingteam/emails/emailid/571541.
[65] El registro de exportación, conocido también como registro de embarque o conocimiento de embarque (B/L, por sus siglas en inglés), es un documento mediante el cual el transportista acusa recibo del cargamento. En él figuran el método de transporte, el valor declarado, el número de unidades, el transportista, el destinatario, el tipo de bienes y la descripción de éstos, entre otros datos.

Seguridad Pública entre cuyas actividades figura la importación y exportación de productos para el Ministerio, como se afirma en su sitio web. [66]

Este envío incluía un "módulo de vigilancia de PC", un "centro de control" y un "módulo de vigilancia de teléfonos móviles inteligentes" relacionados con un "sistema de software profesional" (véase la figura 21). Los tres artículos, que valían 8,4 millones de dólares, fueron fabricados por "AS". Medios de comunicación asociados a EIC que analizaron las conclusiones de Amnistía Internacional confirmaron a ésta que "AS" se usa como abreviatura de Advanced Middle East Systems en la documentación interna del grupo Nexa. Entre los otros 27 artículos incluidos en el envío, cuyo valor total era de 167.600 dólares estadounidenses, había servidores y ordenadores de sobremesa Dell, equipo de red y un ordenador portátil.

Amnistía y EIC obtuvieron información sobre este envío de tres bases de datos de registros de exportación diferentes. Los datos son exactamente los mismos en todos los aspectos del envío (precios, cantidad y descripción de productos, fecha de entrega, nombres de empresas exportadora e importadora) salvo el país de origen. Según dos de las bases de datos, los productos fueron enviados desde EAU, mientras que la tercera indica que se remitieron desde Israel. El Servicio de Aduanas israelí se negó a responder a las preguntas de EIC sobre este envío, y el gobierno de EAU no contestó.

Amnistía Internacional cree que este envío de Delsons Hong Kong Ltd. está ligado a la venta del sistema de software espía Predator a Vietnam. La organización pidió por carta a Delsons una respuesta sobre estos datos, pero, en el momento de la publicación, no había recibido respuesta. EIC también solicitó una respuesta a Delsons Hong Kong Ltd.

< 10/13 >

Transaction date	2021/11/01
B/L No.	--
Buyers	Bca Thang Long One Member Limited Company
Supplier	Delsons Hong Kong Ltd.
Import area	Vietnam
Export area	Israel
Product description	MOBILE SMART PHONE MONITORING MODULE BELONGING TO PROFESSIONAL SOFTWARE SYSTEM, MANUFACTURER: AS ® Translate
HS code	84714190
Quantity	1.0 OTHER
Weight	--
Total price	2800000.0
Unit price	2800000.0
POL	--
POD	--
Shipping methods	Air Transport
Contact person	--

Figura 21: Transferencia de "módulo de vigilancia de teléfonos móviles" a BCA.-Thang Long Co con un valor declarado de 2,8 millones de dólares.[67]

Registros de embarque adicionales obtenidos por Amnistía Internacional revelan que Advanced Middle East Systems envió directamente componentes de redes informáticas durante el mismo periodo, en octubre de 2021, a una empresa vietnamita llamada I-Globe. Según su sitio web, I-Globe se dedica a "seguridad, encriptación, tecnologías de la información y soluciones especializadas, dedicadas a organizaciones

[66] BCA – Thang Long Co., Ltd, https://bca-thanglong.vn/ (consultado por última vez el 26 de septiembre de 2023).
[67] 52wmb.com, registro de exportación, https://www.52wmb.com/ (consultado por última vez el 26 e septiembre de 2023).

gubernamentales especiales, empresas [...]".[68] En su cuenta en Facebook, I-Globe afirma que trabaja con el Ministerio de Seguridad Pública de Vietnam.[69]

Figura 22: Captura de pantalla del sitio web de i-Globe

Basándose en el análisis de EIC de los documentos internos de que disponía y en la información adicional sobre envíos expuesta *supra*, Amnistía Internacional cree que el grupo Nexa y su filial de ventas Advanced Middle East Systems vendió el software espía Predator de Intellexa a un cliente vietnamita en el Ministerio de Seguridad Pública de Vietnam a través de varias empresas intermediarias internacionales y locales. En una carta de respuesta enviada a EIC, representantes del grupo Nexa dijeron:

> "Advanced Middle East Systems trabajó después brevemente con Intellexa para ayudarla a comercializar sus soluciones. Advanced Middle East Systems actuó como revendedor/intermediario y no era responsable del control de exportaciones. Correspondía al fabricante de la solución solicitar las autorizaciones de exportación en función de los países en los que se podía instalar la solución".
>
> "Sobre este tema, su información es incorrecta. Aunque es cierto que se firmaron algunos contratos de intermediación, en cumplimiento pleno de las normas sobre exportación, en relación con las tecnologías que ustedes califican de 'ofensivas', no se cumplió ninguno de nuestros contratos. En 2021, los rescindimos todos antes de que fueran operativos porque consideramos que estas tecnologías eran demasiado controvertidas."

En una respuesta adicional, representantes de Nexa confirman que se suscribieron contratos con Vietnam para tecnología informática ofensiva. Sin embargo, estos representantes dicen que dejaron de participar en el componente de software espía de los contratos y sólo continuaron con una parte del contrato relativa a la ciberseguridad:

> "Confirmamos que la rescisión de contratos de '*lutte informatique offensive (LIO)*' (productos de lucha informática ofensiva) es real y efectiva para los países citados. En relación con Vietnam, sólo mantuvimos la parte [del contrato] relacionada con la ciberseguridad. Una vez más, hemos tomado la decisión de pasar página y abandonar todas las acciones en el ámbito de la LIO."

A raíz de esta respuesta, EIC volvió a preguntar a Nexa Technologies sobre las ventas a Vietnam vía Delsons que se mencionan en este apartado. En el momento de la publicación de este informe, no había recibido más respuestas.

4.6 ATRIBUCIÓN DE LA RESPONSABILIDAD 4.7 DE LOS ATAQUES

Este caso práctico muestra el riesgo que representan los productos de Intellexa para el trabajo de quienes defienden los derechos humanos, periodistas, personal de instituciones internacionales y otras personas. En este capítulo se expone la investigación del Laboratorio sobre Seguridad de Amnistía Internacional sobre cómo el operador de la cuenta @Joseph_Gordon16 intentó infectar a los objetivos con una plataforma de software espía de 1 clic. Amnistía Internacional tiene un alto grado de confianza en que los intentos de

[68] I-Globe, https://iglobe.com.vn/en/ (consultado por última vez el 26 de septiembre de 2023).
[69] "i-Globe Techno J. is Specialised company who serves for customers from MoD, MoPS and other." Véase: Facebook, I-Globe Technology Investment & Development Joint Stock Company, 15 de noviembre de 2021, https://www.facebook.com/connectingworldtechnologies/posts/pfbid025VoHTQp81AUVAskXRK14hRUkZvu48cgnZTCAx5ZnvMBqhW76B8MfsambnDuaU67SI.

ataque descritos en este informe están ligados al software espía Predator de Intellexa y a la infraestructura de software espía asociada.

Las URL de infección de Predator válidas y con duración limitada que se usaron en este ataque sólo pudieron ser generadas mediante el acceso a la interfaz administrativa de *backend* de Predator de un cliente. Esto sugiere que el operador que estaba detrás de @Joseph_Gordon16 es un cliente directo de Intellexa o una entidad con una relación operativa continuada y en tiempo real con el cliente de Predator de Intellexa. Como se ha indicado en el apartado anterior, los registros de envío y otros documentos muestran que Vietnam ha comprado software espía de la alianza Intellexa.

Esta campaña recién identificada estaba dirigida contra la sociedad civil y periodistas vietnamitas, así como contra figuras políticas que trabajaban en cuestiones de interés para el gobierno de Vietnam. La campaña de software espía usó URL diseñadas para imitar sitios web vietnamitas legítimos. Amnistía Internacional compartió indicadores técnicos sobre esta campaña de ataques con personal investigador del Grupo de Análisis de Amenazas de Google, que confirmó a socios de EIC que creía que esta campaña está "asociada a un actor gubernamental en Vietnam". Personal investigador de seguridad de Meta también había identificado con anterioridad un cliente de Predator de Cytrox (parte de la alianza Intellexa) que creía estaba radicado en Vietnam.[70]

En este capítulo también se ha expuesto el historial de Intellexa de venta de software espía a Vietnam, recurriendo especialmente a las investigaciones realizadas por socios de EIC en el marco de la investigación sobre los Archivos Predator. La combinación de la investigación técnica y los datos de las ventas de la alianza Intellexa a Vietnam indica que el operador de la cuenta estaba estrechamente vinculado a Vietnam y podría haber estado actuando en nombre de autoridades o grupos de interés vietnamitas. Amnistía Internacional compartió estas conclusiones con las autoridades vietnamitas antes de la publicación. En el momento de publicar este informe, no habíamos recibido ninguna respuesta.

[70] Meta, *Threat Report on the Surveillance-for-Hire Industry* (antes citado), https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf.

5. IMPLICACIONES PARA LOS DERECHOS HUMANOS RELACIONADAS CON EL USO DE SOFTWARE ESPÍA

5.1 PROHIBICIÓN DEL SOFTWARE ESPÍA ALTAMENTE INVASIVO

La vigilancia digital selectiva sólo pueden llevarla a cabo legalmente los Estados si existen unas salvaguardias de derechos humanos adecuadas para evitar abusos. Las normas internacionales de derechos humanos exigen que la vigilancia selectiva se efectúe sólo sobre la base de sospechas razonables individualizadas, de conformidad con la ley, si es estrictamente necesaria para lograr un objetivo legítimo y si se lleva a cabo de manera proporcionada a ese objetivo y no discriminatoria.[71]

Sin embargo, ni siquiera un marco normativo que respetara los derechos humanos sería suficiente para impedir las violaciones de estos derechos asociadas al uso de ciertos tipos de software espía altamente invasivos. El software espía altamente invasivo permite el acceso ilimitado a un dispositivo, y su uso no se puede auditar de forma independiente. Este tipo de software espía altamente invasivo no puede usarse nunca de un modo respetuoso con los derechos humanos y debe prohibirse permanentemente. Como señala el supervisor europeo de Protección de Datos, con el uso de este tipo de herramientas altamente invasivas, "[e]l nivel de interferencia con el derecho a la privacidad es tan grave que, de hecho, la persona se ve privada de él. En otras palabras, afecta a la esencia misma del derecho. Por lo tanto, su uso no puede considerarse proporcionado, independientemente de que la medida pueda estimarse necesaria".[72] Esto concuerda con el razonamiento expuesto por la relatora especial sobre la lucha contra el terrorismo, quien sostiene que el software espía cuyo funcionamiento no puede limitarse de forma significativa y cuyo uso no puede auditarse de forma independiente debería ser objeto de una prohibición.[73]

---

[71] Pacto Internacional de Derechos Civiles y Políticos, Observación general núm. 34, 12 de septiembre de 2011, https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsrdB0H1l5979OVGGB%2BWPAXiks7ivEzdmLQdosDnCG8FaqoW3y%2FrwBqQ1hhVz2z2IpRr6MpU%2B%2FxEikw9fDbYE4QPFdIFW1VIMIVkoM%2B312r7R.

[72] Supervisor europeo de Protección de Datos, *Preliminary Remarks on Modern Spyware*, 15 de febrero de 2022, p. 8 (la traducción de la cita es de Amnistía Internacional).

[73] Relatora especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, *Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach*, abril de 2023, https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf, párr. 66.

El software espía Predator y sus variantes bajo denominaciones alternativas son programas espía altamente invasivos que pueden acceder a cantidades ilimitadas de datos de un dispositivo por defecto y que, en la actualidad, no pueden auditarse de forma independiente. Debido a esto, actualmente no se puede determinar si se pueden limitar sus funciones. En este sentido, la valoración de Amnistía Internacional es que Predator es un software espía altamente invasivo y, por tanto, ningún uso de Predator puede ser respetuoso con los derechos humanos.

Igualmente, los sistemas de infección estratégica se asemejan a las herramientas de vigilancia masiva puesto que, para seleccionar como objetivo a una persona e infectarla, precisan tener acceso al tráfico de Internet a gran escala.[74] Amnistía Internacional considera que no existe nada que justifique razonablemente llevar a cabo una vigilancia masiva indiscriminada. Ningún acto de vigilancia masiva indiscriminada supera la prueba de la necesidad y la proporcionalidad, que exige que los Estados usen para la vigilancia la herramienta menos restrictiva para los derechos que exista. La vigilancia masiva no puede superar estas pruebas porque recopila cantidades ilimitadas de datos y su uso no puede ser respetuoso con los derechos humanos.

5.2 INEXISTENCIA DE SALVAGUARDIAS DE DERECHOS HUMANOS

El uso de software espía altamente invasivo como Predator debe prohibirse globalmente debido a los riesgos que conlleva para los derechos humanos. Otros tipos de software espía menos invasivos cuyas funciones pueden limitarse y cuyo uso puede verificarse y someterse a una auditoría independiente deberían ser objeto de suspensión hasta que no se hayan desarrollado salvaguardias para los derechos humanos que puedan evitar su uso abusivo. Estas salvaguardias incluirían, por ejemplo, regular la exportación de tecnologías de vigilancia para garantizar la denegación de autorizaciones de exportación cuando exista un riesgo sustancial de que la exportación en cuestión pueda usarse para violar los derechos humanos; implementar leyes nacionales que impongan salvaguardias frente a los abusos y violaciones de derechos humanos cometidos a través de la vigilancia digital, y establecer mecanismos de rendición de cuentas que proporcionen a las víctimas de abusos de vigilancia una vía de recurso, entre otras.

Amnistía Internacional y numerosas organizaciones de la sociedad civil más,[75] junto con la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos,[76] varias personas expertas de la ONU y de ámbito regional,[77] y al menos un Estado —Costa Rica—[78] han pedido la suspensión de la venta, la transferencia, la exportación y el uso de software espía hasta que se instaure un sistema adecuado de salvaguardias de derechos humanos.

Tras las revelaciones del Proyecto Pegasus, ha habido algunos avances en la regulación del software espía. La Oficina de Industria y Seguridad del gobierno de Estados Unidos ha incluido a múltiples empresas de software espía en su lista de entidades por actividades informáticas maliciosas, entre ellas dos entidades corporativas de la alianza Intellexa, así como destacados proveedores de software espía como NSO Group y Candiru.[79] La Casa Blanca emitió una orden ejecutiva que prohibía al gobierno estadounidense el uso de

[74] Amnistía Internacional, *Predator Files: Technical deep-dive into Intellexa Alliance surveillance products* (antes citado), https://securitylab.amnesty.org/latest/2023/10/technical-deep-dive-into-intellexa-alliance-surveillance-products/.
[75] Amnistía Internacional, *Global Digital Compact: joint submission on targeted surveillance* (Índice: IOR 10/6726/2023) 1 de mayo de 2023, https://www.amnesty.org/es/documents/ior10/6726/2023/en/.
[76] Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, informe: *El derecho a la privacidad en la era digital*, agosto de 2022, A/HRC/51/17.
[77] Naciones Unidas: "Spyware scandal: UN experts call for moratorium on sale of 'life-threatening' surveillance tech", 12 de agosto de 2021, https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening; Organización de los Estados Americanos, "CIDH y RELE: República Dominicana debe investigar espionaje a través de Pegasus a periodista de investigación", 1 de junio de 2023, https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/prensa/comunicados/2023/106.asp; Consejo de Derechos Humanos, Informe del Grupo de Trabajo sobre Desapariciones Forzadas o Involuntarias, 11 de septiembre de 2023, A/HRC/54/22/Add.5, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G23/182/83/PDF/G2318283.pdf?OpenElement, párr. 21.
[78] Access Now, "Stop Pegasus: Costa Rica is the first country to call for a moratorium on spyware technology", 13 de abril de 2022 (actualizado el 26 de enero de 2023), https://www.accessnow.org/press-release/costa-rica-first-country-moratorium-spyware/.
[79] Departamento de Estado de Estados Unidos, "The United States Adds Foreign Companies to Entity List for Malicious Cyber Activities", 3 de noviembre de 2021, https://www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities/; Departamento de Estado de Estados Unidos, "The United States Adds Foreign Companies to Entity List for Malicious Cyber Activities" (antes citado), https://www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities-2/.

software espía comercial que "represent[as]e riesgos significativos de contrainteligencia o de seguridad para el gobierno de Estados Unidos o riesgos significativos de uso indebido por un gobierno extranjero o persona extranjera".[80] Además, once Estados se han unido para anunciar iniciativas destinadas a contrarrestar la proliferación y el uso indebido de software espía comercial.[81] En la Cumbre por la Democracia, 45 Estados respaldaron un conjunto de nuevos principios rectores sobre el uso gubernamental de las tecnologías de vigilancia.[82] Encabezados por Estados Unidos, algunos Estados han firmado un Código de Conducta de la Iniciativa para Controles de Exportaciones y Derechos Humanos.[83] Se han iniciado litigios y diversas investigaciones de ámbito nacional en múltiples jurisdicciones, como las de Tailandia, Estados Unidos, Reino Unido, Israel, España, Francia, Hungría, Polonia e India, entre otros.[84] Este año, el Parlamento Europeo concluyó la Comisión de Investigación Encargada de Examinar el Uso del Programa Espía de Vigilancia Pegasus y Otros Programas Equivalentes (PEGA) condenando el uso indebido del software espía en varios Estados miembros de la UE y pidiendo una reforma.

Se trata de medidas significativas y bien acogidas en la dirección correcta. Sin embargo, las declaraciones públicas, las recomendaciones y los compromisos voluntarios no siempre se han traducido en acciones resueltas, y aún no se han rendido cuentas ni han recibido un resarcimiento significativo las personas que, en todo el mundo, han sido objetivos ilegítimos de software espía. Si bien algunos Estados han emprendido ciertas iniciativas voluntarias, como ya se ha señalado, otros han obstruido las investigaciones y no han proporcionado una transparencia significativa. Por ejemplo, la fiscalía de Hungría puso fin a su investigación sobre el uso ilegítimo de Pegasus en el país aduciendo la inexistencia de "una recopilación no autorizada y secreta de información o uso de un dispositivo oculto."[85] En España, un juzgado de Barcelona tuvo que suspender una investigación debido a la falta de avances de las autoridades israelíes respecto a una comisión rogatoria.[86] En 2021, el Tribunal Supremo de India creó un comité técnico para investigar abusos que implicaban el uso de Pegasus. En 2022, el comité concluyó su investigación, pero el Tribunal no ha hecho públicas las conclusiones del informe.[87] Además, el Tribunal señaló que las autoridades indias "no cooperaron" con las investigaciones del comité técnico.[88]

La vigilancia ilegítima e incontrolada continúa teniendo consecuencias devastadoras, al violar el derecho a la privacidad y a la libertad de expresión, de asociación y reunión pacífica de las víctimas. Siguen siendo especialmente devastadores el impacto en las defensoras de los derechos humanos[89] y el uso de software espía contra personas que afrontan formas múltiples y entrecruzadas de discriminación por motivos de raza, etnia, identidad religiosa, discapacidad y orientación sexual e identidad de género. Las mujeres racializadas; las pertenecientes a minorías étnicas o religiosas; las lesbianas, bisexuales o transgénero; así como las personas de género diverso y las mujeres con discapacidad están expuestas a daños de carácter único y agravados.

Además, cuando el software espía sigue actuando sin control y sin ninguna salvaguardia, tiene un efecto disuasorio en el trabajo por los derechos humanos, pues las personas dedicadas al activismo se

---

[80] Casa Blanca, "Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security", 27 de marzo de 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/.
[81] Casa Blanca, "Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware", 30 de marzo de 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/30/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/.
[82] Departamento de Estado de Estados Unidos, "Guiding Principles on Government Use of Surveillance Technologies", 30 de marzo de 2023, https://www.state.gov/guiding-principles-on-government-use-of-surveillance-technologies/.
[83] Departamento de Estado de Estados Unidos, "Export Controls and Human Rights Initiative Code of Conduct Released at the Summit for Democracy", 30 de marzo de 2023, https://www.state.gov/export-controls-and-human-rights-initiative-code-of-conduct-released-at-the-summit-for-democracy/#:~: text=The%20Export%20Controls%20and%20Human, technology%20that%20violate%20human%20rights.
[84] Citizen Lab, "Litigation and other formal complaints related to mercenary spyware", 12 de diciembre de 2018 (actualizado el 31 de julio de 2023), https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/#NSO.
[85] *Al Jazeera*, "Hungary prosecutors open investigation into Pegasus spying claims", 22 de julio de 2021, https://www.aljazeera.com/news/2021/7/22/hungary-prosecutors-open-investigation-into-pegasus-spying-claims.
[86] *El Nacional*, "Judge suspends first Catalan espionage case; lawyer demands reopening and widening", 30 de mayo de 2022, https://www.elnacional.cat/en/politics/judge-closes-torrent-maragall-pegasus-spyware-catalonia_765453_102.html.
[87] *The Guardian*, "Indian supreme court orders inquiry into state's use of Pegasus spyware", 27 de octubre de 2021, https://www.theguardian.com/news/2021/oct/27/indian-supreme-court-orders-inquiry-into-states-use-of-pegasus-spyware.
[88] *The Wire*, "Pegasus: Malware Found in 5 Phones, Government 'Refused to Cooperate' With Probe, Says CJI", 25 de agosto de 2022, https://thewire.in/law/supreme-court-pegasus-technical-committee.
[89] Access Now, "Unsafe anywhere: women human rights defenders speak out about Pegasus attacks", 17 de enero de 2022 (actualizado el 8 de mayo de 2023), https://www.accessnow.org/women-human-rights-defenders-pegasus-attacks-bahrain-jordan/.

autocensuran por temor a la vigilancia.[90] Además, el impacto va más allá de las personas objeto de ataque, ya que afecta a cualquier persona que pueda abstenerse de ejercer sus derechos a la libertad de expresión, asociación y reunión pacífica, entre otros, debido a las formas en que podrían usarse en su contra los datos relativos a sus actividades.

Estas últimas revelaciones muestran que la sociedad civil, incluidos medios de comunicación, periodistas y personal de investigación del ámbito académico sigue expuesta a la lacra del software espía no regulado. Además, los ataques contra autoridades regionales, nacionales e internacionales, incluido personal diplomático, muestran una vez más lo que Amnistía Internacional lleva mucho tiempo advirtiendo. El software espía comercial tiene graves implicaciones tanto para los derechos humanos como para la seguridad del ecosistema digital en su conjunto. En ausencia de normativa, estas armas cibernéticas pueden volverse contra terceros gobiernos y autoridades, como ya ha sucedido.

Hay iniciativas voluntarias recientes de los Estados que se suman a las existentes, como el Arreglo de Wassenaar sobre el Control de las Exportaciones de Armas Convencionales y de Bienes y Tecnologías de Doble Uso, cuyos Estados participantes acuerdan armonizar los regímenes de exportación. Sin embargo, el Arreglo de Wassenaar no es jurídicamente vinculante y depende de compromisos voluntarios de los Estados. Amnistía Internacional ha señalado con anterioridad que el mandato del Arreglo no incluye la protección de los derechos humanos.[91] De hecho, tomando nota de su carácter no vinculante, en sus recomendaciones al Consejo Europeo y a la Comisión Europea tras la investigación de la Comisión PEGA, el Parlamento Europeo pidió que el Arreglo de Wassenaar se convirtiera en un acuerdo vinculante y subrayó que debía incluir un marco de derechos humanos como parte de su evaluación de las licencias de exportación.[92]

La implementación de estas declaraciones voluntarias de los Estados tiene que ser vigilada de cerca para ver si los Estados están cumpliendo realmente sus compromisos públicos y haciendo lo que han prometido. Es necesario que los Estados lleven a cabo más esfuerzos concertados para establecer salvaguardias de derechos humanos que sean vinculantes y exigibles a nivel nacional, regional e internacional.

En 2019, el anterior relator especial de las Naciones Unidas sobre la libertad de opinión y de expresión indicó: "Decir que todo un sistema completo de control y utilización de tecnologías de vigilancia selectiva ha dejado de funcionar ni siquiera se acerca a la realidad. La realidad es que apenas existe".[93] Amnistía Internacional cree que, a pesar de los progresos iniciales, la situación sigue siendo la misma. Las empresas y los Estados a los que abastecen siguen actuando en secreto para desplegar software espía invasivo contra la sociedad civil y la profesión periodística sólo porque ejercen sus derechos humanos y trabajan para proteger los derechos de otras personas. Las revelaciones más recientes deberían servir de recordatorio de que hace falta una actuación más significativa y concertada por parte de los Estados en el ámbito nacional y el internacional.

5.3 LAS OBLIGACIONES EN MATERIA DE DERECHOS HUMANOS DE LOS ESTADOS

En virtud del derecho internacional de los derechos humanos, los Estados están obligados a proteger los derechos humanos de abusos perpetrados por terceros.[94] Esto incluye la obligación de regular la conducta de las empresas que están domiciliadas en su territorio o bajo su control efectivo para impedir que cometan o contribuyan a cometer abusos contra los derechos humanos, incluso en el caso de que éstos se produzcan en otros países.[95]

---

[90] OACNUDH, informe: *El derecho a la privacidad en la era digital*, 30 de junio de 2014, doc. ONU A/HRC/27/37, párr. 20.
[91] Amnistía Internacional, *Operating in the shadows*: *Inside NSO Group's Corporate Structure* (antes citado), https://www.amnesty.org/es/documents/doc10/4182/2021/en/.
[92] Parlamento Europeo, Recomendación del Parlamento Europeo, de 15 de junio de 2023, al Consejo y a la Comisión a raíz del examen de las alegaciones de infracción y de mala administración en la aplicación del Derecho de la Unión en relación con el uso del programa espía de vigilancia Pegasus y otros programas equivalentes, 15 de junio de 2023, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_ES.html, recomendaciones 54 y 56.

[93] Consejo de Derechos Humanos de la ONU, La vigilancia y los derechos humanos. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, 28 de mayo de 2019, doc. ONU A/HCR/41/35, https://undocs.org/A/HRC/41/35, párr. 46.
[94] Comité de Derechos Humanos de la ONU, Observación general nº 31 (80): Naturaleza de la obligación jurídica general impuesta a los Estados Partes en el Pacto, 26 de mayo de 2004, doc. ONU CCPR/C/21/Rev.1/Add. 13, párr. 8.
[95] Los Estados son responsables de la protección frente a los abusos de empresas privadas incluso fuera de sus fronteras. Este principio está aceptado y es directamente aplicable a los derechos vulnerados en los casos que se revelan en el presente

Sin embargo, las revelaciones de los Archivos Predator confirman algo que sabemos desde hace tiempo: que muchos Estados tienen poco interés en respetar, no digamos proteger, los derechos humanos en lo que se refiere a la vigilancia. La inacción de los Estados donde tienen su sede las entidades corporativas de la alianza Intellexa —entre ellos Grecia, Irlanda, Francia, Alemania, República Checa, Chipre, Hungría, Suiza, Israel, Macedonia del Norte y Emiratos Árabes Unidos— a la hora de controlar de forma significativa la alianza ha sido causa de abusos contra los derechos humanos.[96]

5.4 LA RESPONSABILIDAD DE LAS EMPRESAS DE RESPETAR LOS DERECHOS HUMANOS

Tal como se establece en los Principios Rectores de la ONU, las empresas tienen también la responsabilidad de respetar los derechos humanos con independencia del lugar del mundo en el que operen. Estos principios exponen que las empresas deben tomar medidas proactivas para garantizar que en ninguna de sus operaciones causan ni contribuyen a causar abusos contra los derechos humanos, y responder a los abusos contra estos derechos si se producen y cuando se produzcan. Para cumplir esa responsabilidad, las empresas deben ejercer la diligencia debida en materia de derechos humanos a fin de "identificar, prevenir, mitigar y rendir cuentas de cómo abordan su impacto sobre los derechos humanos". La responsabilidad de las empresas de respetar los derechos humanos existe más allá de sus propias operaciones. También existe con independencia de la capacidad o voluntad de los Estados de cumplir sus propias obligaciones en materia de derechos humanos y está por encima del cumplimiento de las leyes y normas nacionales que protegen estos derechos.[97]

Esto incluye también las responsabilidades de las empresas de responder de las consecuencias negativas para los derechos humanos en toda su cadena de valor, lo que incluye el uso de sus productos y servicios. Los Principios Rectores de la ONU señalan: "Las empresas pueden estar implicadas en las consecuencias negativas sobre los derechos humanos a través de sus propias actividades o como resultado de sus relaciones comerciales con otras partes [...] sus 'relaciones comerciales' abarcan las relaciones con socios comerciales, entidades de su cadena de valor y cualquier otra entidad no estatal o estatal directamente relacionada con sus operaciones comerciales, productos o servicios".[98] Dentro de este contexto, una empresa que venda material de vigilancia puede ser cómplice de las violaciones de derechos humanos que se cometan posteriormente utilizando ese material. Un grupo de especialistas de la Comisión Internacional de Juristas ha examinado en cierta profundidad la cuestión de la complicidad de las empresas en las violaciones de derechos humanos y aclarado cuándo podría entrañar responsabilidades jurídicas, tanto civiles como penales. Así, este grupo consideró que, legalmente, se podría establecer un vínculo de responsabilidad suficiente si la conducta de la empresa permitió, agravó o facilitó los abusos y la empresa sabía, o habría debido saber, dentro de lo razonable, que los abusos ocurrirían, así como que una empresa puede permitir, agravar o facilitar dichos abusos mediante, entre otras cosas, el suministro de bienes o servicios.[99]

Las propias empresas de la alianza Intellexa no han revelado con carácter proactivo ninguna información sobre sus prácticas de diligencia debida en materia de derechos humanos. Cualquier evaluación —si es que existe— sobre el impacto de sus tecnologías de vigilancia en los derechos humanos permanece rodeada de misterio. Amnistía Internacional escribió a la alianza Intellexa solicitando sus comentarios sobre la información detallada en este informe y pidiendo información sobre sus prácticas de diligencia debida en

proyecto. Véanse, por ejemplo, Comité de Derechos Económicos, Sociales y Culturales de la ONU, Observación general núm. 24 sobre las obligaciones de los Estados en virtud del Pacto Internacional de Derechos Económicos, Sociales y Culturales en el contexto de las actividades empresariales, 10 de agosto de 2017, doc. ONU E/C.12/GC/24, párr. III.C.2.; Comité de Derechos Humanos de la ONU, Observación general núm. 36: Derecho a la vida, 3 de septiembre de 2019, doc. ONU CCPR/C/GC/36, párr. 63; Relatora especial de la ONU sobre ejecuciones extrajudiciales, sumarias o arbitrarias, anexo al informe *Investigation into the unlawful death of Mr. Jamal Khashoggi*, 19 de junio de 2019, doc. ONU A/HRC/41/CRP.1.

[96] Hubo algunos progresos en enero de 2023, cuando, según informes, la Autoridad Helénica de Protección de Datos (HDPA) impuso a Intellexa A.E. una multa de 50.000 euros por violar el Reglamento general de protección de datos (Reglamento UE 2016/679) al no haber facilitado toda la información. Véase: Haaretz, "Greek Authorities Fine Spyware Firm Owned by Former Israeli Intel Officer", 16 de enero de 2023, https://www.haaretz.com/israel-news/security-aviation/2023-01-16/ty-article/.premium/greek-authorities-fine-intellexa-chief-over-spyware-scandal/00000185-bab3-deab-ad97-fafbd8ae0000.

[97] OACNUDH, Principios rectores sobre las empresas y los derechos humanos, 2011, https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_SP.pdf.

[98] OACNUDH, Principios rectores sobre las empresas y los derechos humanos (antes citado), https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_SP.pdf, principio rector 13.

[99] Comisión Internacional de Juristas (CIJ), *Report of the ICJ Expert Legal Panel on Corporate Complicity in International Crimes*, 1 de enero de 2008, icj.org/report-of-the-international-commission-of-jurists-expert-legal-panel-on-corporate-complicity-in-international-crimes.

materia de derechos humanos, incluyendo si habían llevado a cabo una diligencia debida detallada en materia de derechos humanos en cada uno de los países usuarios finales a los que venden sus productos. En el momento de la publicación, la organización no había recibido respuesta.[100]

[100] EIC sí recibió respuesta de ex miembros del personal directivo y accionistas principales del grupo Nexa, en nombre de sus empresas, incluidas Nexa Technologies y Advanced Middle East Systems. Sus respuestas a EIC correspondientes a las preguntas que les había enviado Amnistía Internacional se incluyen en el apartado 4.1 *supra*.

6. “REGULADA Y RADICADA EN LA UE”

6.1 INACCIÓN DE LA UNIÓN EUROPEA Y DE LOS ESTADOS MIEMBROS PARA ACABAR CON EL USO INDEBIDO DE SOFTWARE ESPÍA

Las últimas revelaciones muestran un panorama desolador en lo que respecta a la inacción de la Unión Europea y sus Estados miembros a la hora de frenar a las empresas que no rinden cuentas y a los Estados miembros díscolos, que siguen aprovechándose de las grietas, visiblemente grandes, de los sistemas normativos a nivel regional y nacional en el seno de la UE. La descarada campaña de vigilancia que se detalla en este informe, efectuada con las herramientas de la alianza Intellexa, muestra los riesgos y las consecuencias muy directos de la proliferación de herramientas de cibervigilancia desde empresas reguladas y radicadas en la UE hasta operadores de terceros países que después las han usado para atacar a personas e instituciones dentro y fuera de la Unión Europea.

Las revelaciones de los Archivos Predator muestran que se concedieron licencias para la exportación de tecnologías de vigilancia a entidades corporativas que estaban dentro de la alianza Intellexa en Francia.[101] Además, el informe de la Comisión de Investigación Encargada de Examinar el Uso del Programa Espía de Vigilancia Pegasus y Otros Programas Equivalentes (PEGA) observa que las autoridades griegas han concedido licencias de exportación a Intellexa para la venta de Predator a Madagascar y Sudán.[102]No está claro si, antes de aprobar esas licencias, estos Estados miembros llevaron a cabo alguna evaluación de los riesgos que representan para la violación de derechos humanos. Tampoco está claro si se pidieron licencias de exportación a otros Estados miembros de la UE y si éstos las concedieron, ni los detalles de cualquier evaluación de derechos humanos pertinente realizada como parte del proceso de concesión de licencias.

Las revelaciones de los Archivos Predator muestran, además, que se han eludido los mecanismos de control de la exportación en los Estados miembros de la UE, concretamente en Francia, donde, según informes, se han hecho exportaciones sin la autorización de las autoridades francesas, pues se llevaron a cabo desde una entidad de la alianza Intellexa en EAU, eludiendo así las normas de la UE.[103]

Las exportaciones de software espía desde la UE están sujetas a la concesión de licencias en virtud del Reglamento relativo a las exportaciones de productos de doble uso, para lo cual, en teoría, deberían tenerse en cuenta los riesgos para los derechos humanos que plantean dichas exportaciones. Habida cuenta de que se concedieron licencias de exportación cuando existe un riesgo sustancial de que los usuarios finales cometan violaciones de derechos humanos, así como de la elusión de las normas de la UE sobre control de las exportaciones mediante estructuras empresariales opacas y entidades en terceros países, es evidente que el Reglamento de la UE relativo a las exportaciones de doble uso adolece de deficiencias importantes, lo

[101] EIC, Projects, https://eic.network/#projects.
[102] Parlamento Europeo, Recomendación del Parlamento Europeo al Consejo y a la Comisión a raíz del examen de las alegaciones de infracción y de mala administración en la aplicación del Derecho de la Unión en relación con el uso del programa espía de vigilancia Pegasus y otros programas equivalentes (antes citado), https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_ES.html, párr. Q.
[103] EIC, Projects, https://eic.network/#projects.

que tiene implicaciones graves para los derechos humanos tanto dentro como fuera de la UE. Por ejemplo, en su informe anual, la Comisión Europea no facilita ninguna información sobre qué tipo de productos se han exportado a qué países y quién ha concedido la licencia[104] y, por tanto, incumple los requisitos sobre transparencia necesarios para un panorama de rendición de cuentas en materia de derechos humanos.[105] Dos años después de la publicación del Reglamento refundido sobre las exportaciones de doble uso, sigue sin haber ninguna orientación de la Comisión sobre cómo llevar a cabo evaluaciones de riesgos para los derechos humanos en relación con la exportación de tecnologías de cibervigilancia que ayude a los Estados y a las autoridades responsables de la concesión de licencias.[106]

Aunque los métodos de ataque que se exponen en este informe han sido poco sistemáticos, son muy claros los posibles daños derivados de la amplia proliferación de herramientas de cibervigilancia a Estados con historiales lamentables en materia de derechos humanos o que carecen de salvaguardias adecuadas para estos derechos en la ley: no sólo son causa de violaciones de derechos humanos en otros países, sino que también son una amenaza para la seguridad y para estos derechos dentro de la UE, ya que se ha descubierto que se han usado para atacar a autoridades de la propia Unión.

6.1.1 MEDIDAS REGULADORAS DE LA UE

Tras las revelaciones del Proyecto Pegasus, el Parlamento Europeo emprendió una investigación sobre el uso de Pegasus y Otros Programas Equivalentes (PEGA). Después de un año de audiencias e investigaciones, la Comisión PEGA señaló al Consejo y a la Comisión de la UE que se habían producido infracciones importantes de la legislación de la Unión y pidió a la UE y sus Estados miembros, mediante unas recomendaciones detalladas, aunque no vinculantes, que tomaran medidas significativas

La Comisión PEGA del Parlamento Europeo también señaló la ausencia de voluntad política de la Unión Europea y de sus Estados miembros al observar que "la mayoría de los Gobiernos y los Parlamentos de los Estados miembros no ha[bía]n facilitado al Parlamento Europeo información significativa sobre los marcos jurídicos que rigen el uso de programas espía en sus Estados miembros más allá de lo que ya se conocía públicamente"[107] y, al concluir, de forma más condenatoria, "que ni los Estados miembros, ni el Consejo, ni la Comisión parec[ía]n estar interesados en maximizar sus esfuerzos para investigar a fondo el abuso de los programas espía, protegiendo así a sabiendas a los Gobiernos de la Unión que viola[ba]n los derechos humanos dentro y fuera de la Unión".[108]

Como ya se ha indicado, aunque se acogen con satisfacción los mecanismos voluntarios como el Arreglo de Wassenaar y la reciente iniciativa de algunos Estados miembros de la UE de unirse a los esfuerzos de la Cumbre por la Democracia[109] encabezados por Estados Unidos para contrarrestar el uso indebido del software espía, estos mecanismos siguen siendo compromisos no vinculantes. Las investigaciones emprendidas en múltiples Estados miembros —Hungría, España y Grecia— tras las revelaciones del Proyecto Pegasus y las revelaciones sobre Predator en Grecia no han desembocado aún en la rendición de cuentas y el resarcimiento de las víctimas del software espía.[110]

Así pues, los esfuerzos reguladores en la UE son gravemente insuficientes o carecen de una aplicación adecuada. La sociedad civil lleva años advirtiendo de que el reglamento de la UE que controla las

---

[104] Comisión Europea, *Informe de la Comisión al Parlamento Europeo y al Consejo sobre la aplicación del Reglamento (UE) 2021/821, por el que se establece un régimen de la Unión de control de las exportaciones, el corretaje, la asistencia técnica, el tránsito y la transferencia de productos de doble uso,* 1 de septiembre de 2022, https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52022DC0434.

[105] Access Now, *Human Rights Organizations' Response to the Adoption of the New EU Dual Use Export Control Rules,* marzo de 2021, https://www.accessnow.org/wp-content/uploads/2021/03/Analysis-EU-Surveillance-Tech-Export-Rules.pdf. CIRCABC, 14 de junio de 2023, https://circabc.europa.eu/ui/group/654251c7-f897-4098-afc3-6eb39477797e/library/e7dc5aae-bce0-4f45-b1e5-bb15b272b66b?p=1&n=10&sort=modified_DESC.

[107] Parlamento Europeo, Recomendación del Parlamento Europeo al Consejo y a la Comisión a raíz del examen de las alegaciones de infracción y de mala administración en la aplicación del Derecho de la Unión en relación con el uso del programa espía de vigilancia Pegasus y otros programas equivalentes (antes citado), https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_ES.html, párr. V.

[108] Parlamento Europeo, Recomendación del Parlamento Europeo al Consejo y a la Comisión a raíz del examen de las alegaciones de infracción y de mala administración en la aplicación del Derecho de la Unión en relación con el uso del programa espía de vigilancia Pegasus y otros programas equivalentes (antes citado), https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_ES.html, art. 13.

[109] Departamento de Estado de Estados Unidos, "Guiding Principles on Government Use of Surveillance Technologies" (antes citado), https://www.state.gov/guiding-principles-on-government-use-of-surveillance-technologies/.

[110] En diciembre de 2022, el Parlamento griego aprobó un polémico proyecto de ley que carecía de salvaguardias efectivas para las personas sometidas a vigilancia y legalizó el uso de tecnología de software espía por las autoridades. Véase: Amnistía Internacional, *Greece's surveillance scandal must shake us out of complacency*, 26 de enero de 2023, https://www.amnesty.org/en/latest/news/2023/01/greeces-surveillance-scandal-must-shake-us-out-of-complacency/.

exportaciones de productos de doble uso —concebido para prevenir los abusos contra los derechos humanos mediante la concesión de licencias de exportaciones de software espía de la UE (véase el apartado 6.1 *supra*)— no es adecuado para su fin de prevenir las consecuencias para los derechos humanos de la exportación a países donde hay un riesgo significativo de que se cometan violaciones de derechos humanos. Pese a las advertencias de la sociedad civil, el reglamento refundido sobre la exportación de productos de doble uso adoptado en 2021 limita la obligación de los Estados a "tener en cuenta", en lugar de exigir, criterios relativos a los derechos humanos cuando evalúan la concesión de licencias de exportación, pero les deja libertad para concederlas igualmente.[111] Estas lagunas en el reglamento dan vía libre a los Estados para ignorar los riesgos para los derechos humanos que plantea la exportación de estas herramientas. La sociedad civil lleva tiempo pidiendo salvaguardias de derechos humanos, incluida una mayor transparencia en los informes sobre exportaciones, que deberían publicarse anualmente y desglosarse por usuario final, destino y uso previsto, organismo gubernamental implicado, valor de la licencia y si la licencia fue concedida o denegada y el motivo.[112]

6.2 DILIGENCIA DEBIDA OBLIGATORIA DE LAS EMPRESAS EN MATERIA DE DERECHOS HUMANOS

La Comisión PEGA ha pedido una legislación europea adicional que exija a los actores empresariales que producen o exportan tecnologías de vigilancia que incluyan marcos de diligencia debida en materia de derechos humanos en consonancia con los Principios Rectores de la ONU.[113] La Unión Europea está negociando actualmente la Directiva sobre la diligencia debida de las empresas en materia de sostenibilidad, que, de ser aprobada, exigirá a las empresas de determinado tamaño de todos los sectores que operen en la UE que ejerzan diligencia debida en materia de derechos humanos y medioambiente para evaluar y abordar los riesgos y consecuencias para los derechos humanos de sus actividades y su cadena de valor.

La Directiva ofrece una acertada oportunidad para empezar a abordar los daños del sector de la vigilancia. Sin embargo, las lagunas de las propuestas presentadas por las entidades colegisladoras de la UE podrían significar que dicha directiva no se aplicara correctamente a las empresas que comercializan tecnología de vigilancia. Por ejemplo, es probable que la Directiva se aplique únicamente a las empresas de gran tamaño, lo que podría excluir del ámbito de la ley a ciertas empresas, incluidas las de la alianza Intellexa.

Además, el Parlamento Europeo y el Consejo de la UE han propuesto que las empresas no tengan que evaluar el posible uso indebido de sus productos y servicios como parte de su diligencia debida en materia de derechos humanos y medioambiente en virtud de la Directiva.[114] Por otra parte, el Consejo de la UE ha intentado introducir una exención para las empresas que fabrican productos sometidos al control de las exportaciones, lo que incluiría las tecnologías de vigilancia.

---

[111] Reglamento (UE) 2021/821 del Parlamento Europeo y del Consejo de 20 de mayo de 2021 por el que se establece un régimen de la Unión de control de las exportaciones, el corretaje, la asistencia técnica, el tránsito y la transferencia de productos de doble uso (versión refundida), 11 de junio de 2021, PE/54/2020/REV/2, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32021R0821.

[112] Access Now, *Human Rights Organizations' Response to the Adoption of the New EU Dual Use Export Control Rules,* marzo de 2021, https://www.accessnow.org/wp-content/uploads/2021/03/Analysis-EU-Surveillance-Tech-Export-Rules.pdf.

[113] Parlamento Europeo, Recomendación del Parlamento Europeo al Consejo y a la Comisión a raíz del examen de las alegaciones de infracción y de mala administración en la aplicación del Derecho de la Unión en relación con el uso del programa espía de vigilancia Pegasus y otros programas equivalentes (antes citado), https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_ES.html, recomendación 66.

[114] Para más información sobre el análisis de Amnistía Internacional de las propuestas de directiva sobre la diligencia debida de las empresas en materia de sostenibilidad, véase Amnistía Internacional, *Eliminar las lagunas jurídicas: Recomendaciones para una ley de la UE sobre empresas y sostenibilidad que sirva para las personas titulares de derechos* (Índice: IOR 60/6539/2023), 15 de mayo de 2023, https://www.amnesty.org/es/documents/IOR60/6539/2023/es/.

7. RECOMENDACIONES

A LA UNIÓN EUROPEA Y SUS ESTADOS MIEMBROS:

Recomendaciones de acción dentro de la Unión Europea

- Todos los Estados miembros de la UE que han concedido licencias de exportación a la alianza Intellexa deben revocar inmediatamente las licencias y llevar a cabo una investigación independiente, imparcial y transparente para determinar el alcance de la posible selección ilegítima de objetivos que culmine con una declaración pública sobre los resultados de estos esfuerzos y las medidas para prevenir futuros daños.
- Los Estados miembros de la UE deben imponer una prohibición del software espía altamente invasivo cuyo funcionamiento no pueda limitarse exclusivamente a las funciones necesarias y proporcionadas a un uso y un objetivo específicos o cuyo uso no se pueda auditar de forma independiente.
- Los Estados miembros de la UE deben implementar un marco normativo de derechos humanos que regule la vigilancia y que sea conforme con las normas internacionales de derechos humanos. Hasta que exista un marco de este tipo, debería imponerse una moratoria sobre la compra, venta, transferencia y uso de todos los demás programas espía.
- Los Estados miembros de la UE deben garantizar un recurso efectivo a las víctimas de vigilancia selectiva ilegítima y exigir rendición de cuentas por estas violaciones de derechos a sus perpetradores. Además, los Estados miembros deben comprometerse a reformar las leyes existentes que supongan un obstáculo a la reparación para estas víctimas y garantizar que en la práctica existan vías de recurso, tanto judiciales como no judiciales.
- Los Estados miembros de la UE deben adoptar y hacer cumplir una legislación que exija a todos los actores empresariales el respeto de los derechos humanos y la aplicación de medidas de diligencia debida en materia de derechos humanos acordes con los Principios Rectores de la ONU. Se debe exigir a los actores empresariales que identifiquen, prevengan y mitiguen todas las consecuencias negativas, potenciales y reales, para los derechos humanos de sus actividades y en toda su cadena de valor. Por tanto, como parte de las deliberaciones en curso en torno a la Directiva sobre la diligencia debida de las empresas en materia de sostenibilidad, la UE debe:
    - Exigir a las empresas que ejerzan la diligencia debida en materia de derechos humanos con respecto a toda la cadena de valor, incluida la compra, la venta, la transferencia, la exportación y el uso de los productos.
    - Exigir a las empresas que operan en todos los sectores —incluidas las que producen software espía, así como las instituciones financieras— que apliquen los requisitos de la Directiva.
- Los Estados miembros de la UE deben adoptar y aplicar una legislación nacional que imponga salvaguardias frente a las violaciones de derechos humanos y los abusos derivados de la vigilancia digital ilegítima. Esto debe ser acorde con la sentencia del Tribunal Europeo de Derechos Humanos de 2015 en la causa ***Roman Zakharov v. Russia***, así como con los principios de necesidad y proporcionalidad.
- Los Estados miembros de la UE y la Comisión Europea deben garantizar una aplicación firme de las normas de control de las exportaciones de la UE que entraron en vigor el 9 de septiembre de 2021 con la refundición del Reglamento sobre exportaciones de doble uso. Esto incluye tomar medidas inmediatas para subrayar la obligación de ejercer la diligencia debida en materia de derechos

humanos derivada del Reglamento sobre exportaciones de doble uso y crear un mercado transparente de tecnologías de cibervigilancia sujeto a salvaguardias efectivas de derechos humanos.

  - El Reglamento establece que la Comisión publicará un informe público anual para el Parlamento y el Consejo. Este informe debería incluir, como mínimo, el número de solicitudes de licencia por artículo, el nombre de la entidad exportadora, una descripción del usuario final, el destino y uso previsto, el organismo gubernamental implicado, el valor de la licencia y si ésta fue concedida o denegada y el motivo.
  - Además, las medidas de control de las transacciones por los Estados miembros deberían incluir una evaluación de la naturaleza estratégica de los artículos y los riesgos que representan para la comisión de violaciones de derechos humanos. Las autoridades nacionales deben informar sobre el cumplimiento de las responsabilidades y obligaciones de diligencia debida, y animar a las empresas a informar a la opinión pública sobre el alcance, la naturaleza y las conclusiones de los procedimientos que han implementado para ejercer la diligencia debida en materia de derechos humanos.
  - Los Estados miembros deben garantizar que los países exportadores establecen mecanismos que proporcionen un recurso efectivo frente a las violaciones de derechos humanos cometidas mediante el uso de la tecnología transferida. Las directrices que se publiquen con arreglo al artículo 26.1 del Reglamento (UE) 2021/821/EU del Parlamento Europeo y del Consejo sobre exportaciones de doble uso deben detallar los requisitos sobre los programas de cumplimiento interno y la diligencia debida que se esperan de las entidades exportadoras en el Reglamento sobre Exportaciones de Doble Uso, basados en los Principios rectores de la ONU sobre las empresas y los derechos humanos y las Líneas Directrices de la OCDE para Empresas Multinacionales.
  - La Comisión Europea deberá poner en marcha de inmediato una investigación sobre todas las licencias de exportación concedidas por la UE y sus Estados miembros —incluida la Autorización general de exportación comunitaria n.º EU005, que incluye software diseñado para el uso de equipos de vigilancia e interceptación— y garantizar que los Estados miembros de la UE revocan todas las licencias de comercialización y exportación en las situaciones en que exista un riesgo significativo de que esta tecnología pueda contribuir a la comisión de violaciones de derechos humanos. Si se halla que la concesión de licencias de exportación por Estados miembros vulnera las normas que regulan la exportación, la Comisión Europea deberá iniciar procedimientos de infracción.

- Los Estados miembros deberán adoptar medidas firmes para poner fin a la represión transnacional de defensores y defensoras de los derechos humanos y periodistas dentro de la UE garantizando que cualquier instrumento interno de la UE sobre defensores y defensoras incluye compromisos de combatir la represión transnacional de estas personas, incluida la vigilancia selectiva ilegítima.

Recomendaciones de acciones de la Unión Europea y sus Estados miembros a través de sus instrumentos de política exterior

Dada su aspiración de ser un referente mundial en derechos humanos, la UE y sus Estados miembros pueden y deben cumplir la función de garantizar la protección de estos derechos y la adhesión al Estado de derecho en el ámbito digital dentro y fuera de su territorio. Esto se basa en las obligaciones en materia de derechos humanos de la UE y sus Estados miembros de proteger y promover globalmente estos derechos, como se establece en el artículo 21 del Tratado de Lisboa. Por otra parte, esto concuerda con los compromisos de la UE contenidos en las Conclusiones del Consejo sobre la configuración del futuro digital de Europa, el Plan de Acción de la UE para los derechos humanos y la democracia, y las directrices de la Unión sobre derechos humanos. Los dirigentes de la UE, entre ellos la presidenta de la Comisión Von Der Leyen y el alto representante Borrell, ya han destacado la importancia de proteger a la sociedad civil y de hacer cumplir el derecho a la privacidad y la libertad de expresión en Internet en la era digital.

- La UE y sus Estados miembros deben articular con claridad su posición sobre la vigilancia selectiva ilegítima, también mediante declaraciones oficiales:
  - Expresar preocupación por los ataques a periodistas, activistas y figuras políticas, subrayando que estas prácticas son inaceptables y violan los derechos a la libertad de expresión, de reunión pacífica y a la privacidad.
  - Subrayar la necesidad urgente de una mayor transparencia y rendición de cuentas legal del sector de la vigilancia ante el aumento de los ataques digitales y de la vigilancia selectiva de

personas que defienden los derechos humanos, periodistas y sociedad civil por gobiernos que quieren silenciar e intimidar a estos actores en todo el mundo.

- Pedir a los Estados que adopten medidas urgentes para garantizar una mayor regulación de la industria de la cibervigilancia, la rendición de cuentas por las violaciones y abusos contra los derechos humanos derivados, y una mayor supervisión de este sector, tan mal regulado.

- La UE y sus Estados miembros deben actuar bilateralmente para organizar gestiones diplomáticas con las autoridades pertinentes de Vietnam.
- La UE y sus Estados miembros deben solicitar aclaraciones a las autoridades vietnamitas y, entre otras cosas:
  - Instar a las autoridades pertinentes a que lleven a cabo una investigación inmediata, independiente, transparente e imparcial sobre todos los casos de vigilancia ilegítima y que, cuando proceda, emprendan acciones judiciales para proporcionar reparación a las víctimas y obligar a los perpetradores a rendir cuentas, de conformidad con las normas internacionales de derechos humanos.
  - Subrayar que el uso de software espía con fines de vigilancia es legal sólo cuando cumple determinados criterios estrictos, como establece el derecho internacional de los derechos humanos, y que esa vigilancia debe ser legal, necesaria, proporcionada y de duración limitada.
  - Instar a las autoridades de Vietnam a que cumplan sus obligaciones y compromisos contraídos en virtud del derecho internacional de los derechos humanos, incluidos los contenidos en el Pacto Internacional de Derechos Civiles y Políticos y en la Declaración de la ONU sobre los Defensores y Defensoras de los Derechos Humanos.
  - Plantear los casos de ataques a defensores y defensoras de los derechos humanos, periodistas y activistas en Vietnam y en Estados miembros de la UE ante las autoridades al más alto nivel y ofrecer a estas personas apoyo político, técnico y de otro tipo de conformidad con las Directrices de la UE sobre Defensores de los Derechos Humanos, las Directrices de la UE sobre Libertad de Expresión y el Plan de Acción de la UE para los Derechos Humanos y la Democracia.
  - Instar al gobierno de Vietnam a que ponga fin a toda vigilancia selectiva ilegítima de defensores y defensoras vietnamitas de los derechos humanos y activistas en otros países, y deje claro que esta represión transnacional es inaceptable.
- Los Estados miembros de la UE deben pedir a los Estados exportadores en terceros países que revoquen inmediatamente todas las licencias de comercialización y exportación concedidas a Intellexa y que lleven a cabo una investigación independiente, imparcial y transparente para determinar el alcance de la vigilancia digital ilegítima realizada con herramientas de Intellexa. Esto debe incluir una revisión completa y subsiguiente reforma del régimen de concesión de licencias para garantizar que es apto para el uso previsto en la ley y en la práctica, y que previene abusos futuros contra los derechos humanos relacionados con la exportación de equipos de cibervigilancia desde sus jurisdicciones. Esto debe culminar en la revelación pública de los resultados de la investigación y de las medidas adoptadas para prevenir los abusos en el futuro.
- De conformidad con la Conclusiones del Consejo de 20 de febrero de 2023 sobre las prioridades de la UE en los foros de derechos humanos de la ONU, la UE y sus Estados miembros deben participar en iniciativas multilaterales clave —en el Consejo de Derechos Humanos de la ONU, en la Asamblea General de las Naciones Unidas y en los ciclos del Examen Periódico Universal— para elaborar unas normas sólidas en materia de derechos humanos que regulen el desarrollo, la venta, la transferencia y el uso de equipos de vigilancia, e identificar objetivos inadmisibles de vigilancia digital. Esto incluye respaldar la petición de que se prohíba el uso de software espía altamente invasivo.

EL GOBIERNO DE VIETNAM DEBE:

- Comprometerse públicamente a dejar de usar de inmediato software espía para atacar ilegítimamente a personas que defienden los derechos humanos, a la sociedad civil y a periodistas dentro y fuera de Vietnam.
- Llevar a cabo una investigación independiente, imparcial y transparente sobre la vigilancia selectiva ilegítima mencionada en este informe, lo que incluye averiguar si existen vínculos entre esta campaña de software espía y alguna agencia gubernamental específica.

- Implantar un marco normativo de derechos humanos que regule la vigilancia y que sea conforme a las normas internacionales de derechos humanos. Hasta que exista un marco de este tipo, debería imponerse una moratoria sobre la compra, venta, transferencia y uso de todos los programas espía.
- Derogar o revisar los artículos 117, 118 y 331 del Código Penal de 2015, que restringen indebidamente el derecho a la libertad de expresión, de reunión pacífica y de asociación, con el fin de adecuarlas al derecho internacional de derechos humanos.
- Emprender la revisión y la reforma de la Ley de Ciberseguridad para adecuarla al derecho internacional de los derechos humanos y, en concreto:
- derogar o reformar los artículos 8, 16, 17 y 26 de la Ley de Ciberseguridad para que sean conformes a las normas internacionales de derechos humanos que regulan la libertad de expresión;
    - incluir salvaguardias concretas contra la aplicación arbitraria y discriminatoria de la ley;
    - eliminar todas las disposiciones que obligarían a las empresas de Internet y tecnológicas a revelar datos personales sin salvaguardias adecuadas para prevenir los abusos.
- Derogar o reformar los artículos 99, 100 y 101 del Decreto 15/2020/ND-CP para que sean conformes a las normas internacionales de derechos humanos que regulan la libertad de expresión y el derecho a la privacidad.
- Derogar o reformar los artículos 5, 22 y 25 del Decreto 72/2013/ND-CP para que sean conformes a las normas internacionales de derechos humanos que regulan la libertad de expresión y el derecho a la privacidad, y abstenerse de introducir la reforma del Decreto propuesta actualmente, en concreto, en lo relativo al artículo 23.d.

TODOS LOS ESTADOS DEBEN:

- Imponer una prohibición del software espía altamente invasivo cuyo funcionamiento no pueda limitarse exclusivamente a las funciones necesarias y proporcionadas a un uso y un objetivo específicos o cuyo uso no se pueda auditar de forma independiente.
- Implantar un marco normativo de derechos humanos que regule la vigilancia y que sea conforme a las normas internacionales de derechos humanos. Hasta que exista un marco de este tipo, debería imponerse una moratoria sobre la compra, venta, transferencia y uso de todos los programas espía.
- Exigir legalmente a las empresas de vigilancia que ejerzan la diligencia debida en materia de derechos humanos en relación con sus operaciones globales, incluido el uso de sus productos y servicios.
- Adoptar y aplicar un marco jurídico que exija transparencia a las empresas de vigilancia privada, incluida información sobre la autoidentificación/registro, los productos y servicios ofrecidos, y las ventas.
- Revelar información sobre todos los contratos —pasados, en vigor y futuros— que tengan con empresas de vigilancia privada, ya sea en respuesta a solicitudes de información o haciendo revelaciones de forma proactiva.
- Además, los Estados deben aplicar, como mínimo, las siguientes recomendaciones si se levanta la moratoria sobre la venta y transferencia de equipos de software espía:
    - Aplicar una legislación nacional que imponga salvaguardias contra los abusos y las violaciones de derechos humanos a través de la vigilancia digital y establecer mecanismos de rendición de cuentas que proporcionen a las víctimas de abusos de vigilancia una vía de recurso.
    - Reformar las leyes existentes que supongan un obstáculo a la reparación para las víctimas de la vigilancia ilegítima y garantizar que en la práctica existan vías de recurso, tanto judiciales como no judiciales.
    - Aplicar normas de contratación que restrinjan los contratos públicos de tecnología y servicios de vigilancia únicamente a las empresas que demuestren que respetan los derechos humanos de acuerdo con los Principios rectores de la ONU sobre las empresas y los derechos humanos y que no han prestado servicios a clientes que cometen abusos en materia de vigilancia.
    - Regular la exportación de tecnologías de vigilancia, lo que incluye:

- Garantizar que se niega la autorización para la exportación cuando exista un riesgo sustancial de que la exportación en cuestión pueda ser utilizada para violar los derechos humanos o porque el país de destino no tiene las salvaguardias jurídicas, procedimentales y técnicas adecuadas para impedir esos abusos.
- Los Estados deberían actualizar los criterios para el control de exportaciones a fin de que tengan en cuenta el historial del usuario final en materia de derechos humanos, así como la legalidad del uso de herramientas de vigilancia sofisticadas en el país de destino, estipulando que las solicitudes se rechazarán si dichas herramientas entrañan un riesgo sustancial para los derechos humanos.
- Garantizar que, en el marco de la evaluación para la concesión de licencias, todas las tecnologías pertinentes son sometidas a examen en lo que respecta a los riesgos para los derechos humanos antes de su transferencia.
- Garantizar transparencia con respecto al volumen, la naturaleza, el valor, el destino y los países usuarios finales de las transferencias de tecnologías de vigilancia, por ejemplo mediante la publicación de informes anuales sobre la importación y exportación de dichas tecnologías.
- Reformar la legislación existente que imponga restricciones demasiado amplias sobre la revelación de esa información.
- Garantizar que las herramientas de cifrado y las investigaciones legítimas de seguridad no están sujetas a controles de exportación.

- Participar en iniciativas multilaterales clave para elaborar normas sólidas en materia de derechos humanos que regulen el desarrollo, la venta y la transferencia de equipos de vigilancia, e identificar los objetivos no permitidos de la vigilancia digital.
- Establecer juntas de supervisión pública comunitarias para supervisar y aprobar la adquisición o el uso de nuevas tecnologías de vigilancia, facultadas para aprobar o rechazar —en función de las obligaciones de los Estados en materia de derechos humanos— las disposiciones relativas a la notificación pública y la presentación de informes.

LA ALIANZA INTELLEXA DEBE, COMO MÍNIMO:

- Poner fin a la producción y venta de Predator y de cualquier otro software espía altamente invasivo similar que no incluya salvaguardias técnicas que permitan su uso legítimo en virtud de un marco normativo que respete los derechos humanos.
- Poner fin inmediatamente al uso, apoyo y venta de sus tecnologías en Estados donde se haya hecho un uso indebido del software de cibervigilancia para dirigirse ilegítimamente contra defensores y defensoras de los derechos humanos, periodistas y miembros de la sociedad civil.
- Proporcionar una indemnización adecuada u otras formas de resarcimiento efectivo a las víctimas de vigilancia ilegítima.
- Adoptar con urgencia medidas proactivas para asegurarse de que no causa violaciones o abusos contra los derechos humanos ni contribuye a causarlos, y para responder a cualquier abuso contra los derechos humanos cuando se cometa. A fin de cumplir esa responsabilidad, la alianza Intellexa debe ejercer la diligencia debida en materia de derechos humanos con arreglo a las normas internacionales sobre empresas y derechos humanos, y tomar medidas para garantizar que quienes defienden los derechos humanos, la profesión periodística y la sociedad civil no siguen convirtiéndose en objetivos de vigilancia ilegal mediante el uso de tecnologías de la alianza Intellexa.
- Garantizar transparencia con respecto al volumen, la naturaleza, el valor, el destino y el usuario final de las transferencias de sus tecnologías de vigilancia.

8. ANEXOS

ANEXO I: INDICADORES DE RIESGO

Dominios de Predator de Intellexa ligados a esta campaña

La primera infraestructura de Predator empleada en esta campaña se registró en julio de 2022. Los dominios de Predator que usaban temas vietnamitas se observaron por primera vez en marzo de 2022. La nueva infraestructura de Predator asociada a los dominios de ataque empleados en esta campaña seguía activa en septiembre de 2023.

NOMBRE DEL DOMINIO	VISTO POR PRIMERA VEZ
ietnamnews[.]com	23/03/2022
lnktonews[.]co	19/07/2022
witteridea[.]co	19/07/2022
caavn[.]org	05/08/2022
xuatnhapcanhvn[.]info	05/08/2022
tokhaiytehanoi[.]org	05/08/2022
southchinapost[.]net	02/05/2023
scanningandinfo[.]online	09/05/2023
asean-news[.]net	09/05/2023
southchinapost[.]co	08/06/2023
asean-news[.]co	08/06/2023
scanningandinfo[.]co	08/06/2023
newsworldsports[.]co	13/07/2023

Tabla 7: Dominios de Predator de Intellexa ligados a esta campaña

Cuentas de X (Twitter) ligadas a esta campaña

CUENTA	VISTA POR PRIMERA VEZ	ÚLTIMA ACTIVIDAD VISTA
Joseph_Gordon	01/10/2019	Principios de junio de 2023
AlexMarcos71	04/04/2023	16/05/2023

Tabla 8: Cuentas de X (Twitter) ligadas a esta campaña

Cuentas de Facebook ligadas a esta campaña

CUENTA	NOMBRE DE LA CUENTA	VISTA POR PRIMERA VEZ	ÚLTIMA ACTIVIDAD VISTA
https://www.facebook.com/profile.php?id=100090236330335	Ahn Tran	10/02/2023	23/03/2023

Tabla 9: Cuentas de Facebook ligadas a esta campaña

ANEXO II: TUITS

En este anexo se enumeran todos los posts en redes sociales de la cuenta @Joseph_Gordon16 que incluían enlaces de ataque.

FECHA	PARA	URL	PLATAFORMA
12/04/2023	@CollinSLKoh	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
12/04/2023	@CollinSLKoh	https://lnktonews[.]co/ODFwNI	X
17/05/2023	@CollinSLKoh	https://southchinapost[.]net/WzMqB	X

Tabla 10: Tuits enviados a objetivo ligado a Singapur

FECHA	PARA	URL	PLATAFORMA
09/02/2023	@thoibao_de	https://lnktonews[.]co/MEmK	X

Tabla 11: Tuits enviados a objetivo ligado a Alemania

FECHA	PARA	URL	PLATAFORMA
12/04/2023	@FMangosingINQ	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
12/04/2023	@FMangosingINQ	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
14/04/23	@FMangosingINQ	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X
23/05/2023	@FMangosingINQ	https://southchinapost[.]net/RtQBG	X

Tabla 12: Tuits enviados a objetivo ligado a Filipinas

FECHA	PARA	URL	PLATAFORMA
10/04/2023	@ChinaDaily	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
14/04/23	@ChinaDaily	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
14/04/23	@ChinaDaily	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
12/04/2023	@PdChina	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
26/05/2023	@PDChinese	https://southchinapost[.]net/faePtONi	X
14/04/23	@SpotlightonCN	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X

Tabla 13: Tuits enviados a objetivo ligado a China

FECHA	PARA	URL	PLATAFORMA
10/04/2023	@Duandang	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X

Tabla 14: Tuits enviados a objetivo ligado a Vietnam

FECHA	PARA	URL	PLATAFORMA
14/04/23	@jojjeols	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X

Tabla 15: Tuits enviados a objetivo ligado a Suecia

FECHA	PARA	URL	PLATAFORMA
10/04/2023	@willripleyCNN @CNN @jimsciutto @EricCheungw	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X
12/04/2023	@GMFAsia	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X

Tabla 16: Tuits enviados a objetivos ligados a Estados Unidos

FECHA	PARA	URL	PLATAFORMA
12/04/2023	@Indopac_INFO	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
12/04/2023	@Indopac_INFO	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
14/04/23	@Indopac_INFO	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X
14/04/23	@Indopac_INFO	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X
17/05/2023	@Indopac_INFO	https://southchinapost[.]net/WzMqB	X
22/05/23	@IMOSINT	https://southchinapost[.]net/fLwoASy	X
12/04/2023	@ItsTheEnforcer	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X

Tabla 17: Tuits enviados a cuentas relacionadas con información de fuentes abiertas

FECHA	PARA	URL	PLATAFORMA
12/04/2023	@Manu_FAO	https://witteridea[.]co/LFJeZQu	X
16/05/2023	@HugBallesteros	https://asean-news[.]net/HpjXXwRU	X

Tabla 18: Tuits enviados a autoridades y personal de investigación relacionados con el sector marítimo o el de la pesca

FECHA	PARA	URL	PLATAFORMA
08/03/2023	@SariArhoHavren	https://lnktonews[.]co/CVqp	X
14/03/2023	@SariArhoHavren	https://witteridea[.]co/mBxp	X
21/05/2023	@ElBridgeColby	https://southchinapost[.]net/fLwoASy	X
12/04/2023	@AsiaMTI	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
14/04/23	@AsiaMTI @cnnphilippines	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
14/04/23	@AsiaMTI	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
17/05/2023	@GordianKnotRay	https://southchinapost[.]net/WzMqB	X

Tabla 19: Tuits enviados a grupos consultivos y personal de investigación

FECHA	PARA	URL	PLATAFORMA
08/02/2023	@vitcheva_eu @EMODnet @cinea_eu @Pierre_Ka @EUgreenresearch @CMEMS_EU @FSUMDC @UNDPOceanInnov @REA_research @EU_ENV @EUClimateAction @eumissionocean	https://witteridea[.]co/LFJeZQu	X
08/02/2023	@vitcheva_eu	https://witteridea[.]co/LFJeZQu	X
08/03/2023	@GermanAmbUSA	https://Inktonews[.]co/CVgp	X
01/06/2023	@EP_President	https://southchinapost[.]net/VuAfn	X
01/06/2023	@EU_Commission	https://southchinapost[.]net/VuAfn	X
01/06/2023	@EU_Commission	https://southchinapost[.]net/VuAfn	X
01/06/2023	@eumissionocean	https://southchinapost[.]net/VuAfn	X

Tabla 20: Tuits enviados a funcionarios/as e instituciones europeos

FECHA	PARA	URL	PLATAFORMA
14/04/23	@iingwen @SenJohnHoeven	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
14/04/23	@MofaTaiwan @RepMcCaul	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X
22/05/23	@iingwen	https://southchinapost[.]net/RtQBG	X

Tabla 21: Tuits enviados a altos cargos e instituciones estadounidenses y taiwaneses

FECHA	PARA	URL	PLATAFORMA
01/06/2023	@erionveliaj	https://southchinapost[.]net/eNISDKnI	X
01/06/2023	@AlMissionEU @AlbanianDiplo	https://southchinapost[.]net/eNISDKnI	X
01/06/2023	@AlMissionUNGen @AlbanianDiplo @AlEmbDenmark @AlMissionUN @AlMissionVienna	https://southchinapost[.]net/eNISDKnI	X
01/06/2023	MirelaKumbaro	https://southchinapost[.]net/eNISDKnI	X
01/06/2023	@GjonajEtilda @ChrisMurphyCT @GaryPeters	https://southchinapost[.]net/eNISDKnI	X
01/06/2023	@MonicaMerino_D @AlbGob @MirelaKumbaro	https://southchinapost[.]net/eNISDKnI	X

Tabla 22: Tuits enviados a funcionarios/as e instituciones albaneses

FECHA	PARA	URL	PLATAFORMA
10/04/2023	@AnarchoTerran	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
10/04/2023	@MarioNawfal	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X

Tabla 23: Otros enlaces de Predator compartidos a cuentas de X

ANEXO III: OTROS ENLACES DE PREDATOR COMPARTIDOS EN REDES SOCIALES

FECHA	PARA	URL	PLATAFORMA
23/03/2023	Liën Minh Dân Chù	http://caavn[.]org/tin-tuc/chien-su-ukraine	Facebook
23/03/2023	Liën Minh Dân Chù	http://caavn[.]org/tin-tuc/quan-he-my-trung-sau-no-khi-cau	Facebook

Tabla 24: Enlaces dirigidos a una organización política vietnamita radicada en Estados Unidos

ANEXO IV: ANÁLISIS DE CUENTAS DE REDES SOCIALES PRESUNTAMENTE RELACIONADAS CON EL ATACANTE

Amnistía Internacional analizó otras cuentas seguidas por la cuenta @Joseph_Gordon16, controlada por el atacante, o que la siguen. Entre las cuentas de X seguidas por @Joseph_Gordon16 hay múltiples cuentas objetivo que posteriormente recibieron enlaces de ataque de Predator.

Del pequeño número de cuentas que siguen a @Joseph_Gordon16, muchas estaban aparentemente interesadas en temas relacionados con Vietnam y la ciberseguridad. Varias de ellas incluían fotos de perfil copiadas de un destacado empresario vietnamita. Algunas de estas cuentas podrían ser avatares adicionales en las redes sociales ligados al operador que está detrás de esta campaña o controlados por éste.

Entre estos seguidores de @Joseph_Gordon16 está la cuenta en X @bisngoo27345032, cuyo nombre de perfil es Bí Ngô, que en vietnamita significa *calabaza*. Esta cuenta seguía a múltiples personas vietnamitas que investigan sobre seguridad así como a empresas de ciberseguridad radicadas en Vietnam. La cuenta parece tener gran interés en la ciberseguridad y nuevas técnicas de ataque.

Otro seguidor de la cuenta @Joseph_Gordon16 es @AlexMarcos71. Esta cuenta dice que está radicada en Filipinas, pero sigue a un gran grupo de cuentas vietnamitas y también tuitea en vietnamita.

Figura 23: Perfil de cuenta ligada al atacante @ AlexMarcos71

Las cuentas en X @AlexMarcos71 y @Joseph_Gordon16 enviaron a una persona del ámbito académico radicada en la UE que investiga la pesca ilegal tuits en los que comentaban el tema de la "tarjeta amarilla" emitida por la UE a Vietnam. El tuit enviado desde @Joseph_Gordon16 incluía un enlace al software espía Predator.

La cuenta @AlexMarcos71 también tuiteó sobre el sistema de la "tarjeta amarilla" (véase la figura 24) y envió un mensaje de respuesta en el que mencionaba a la persona del ámbito académico de la UE a la que @Joseph_Gordon16 había enviado un enlace de ataque (véase la figura 25). La coordinación entre estas cuentas sugiere que ambas están controladas o gestionadas por el operador que está detrás de esta campaña de ataques.

Figura 24: Tuits de la cuenta @AlexMarcos71 en español sobre el sistema de la "tarjeta amarilla"

Figura 25: @AlexMarcos71 envía tuit de respuesta mencionando al objetivo del ámbito académico español

AMNISTÍA INTERNACIONAL ES UN MOVIMIENTO GLOBAL DE DERECHOS HUMANOS. LAS INJUSTICIAS QUE AFECTAN A UNA SOLA PERSONA NOS AFECTAN A TODAS LAS DEMÁS.

CONTÁCTANOS

info@amnesty.org

+44 (0)20 7413 5500

ÚNETE A LA CONVERSACIÓN

www.facebook.com/AmnestyGlobal

@Amnesty

LOS ARCHIVOS PREDATOR: EMBOSCADA EN LA RED

LA AMENAZA GLOBAL DEL SOFTWARE ESPÍA “REGULADO POR LA UE”

ÍNDICE: ACT 10/7245/2023 SPANISH
OCTUBRE DE 2023
IDIOMA: ESPAÑOL

amnesty.org

AMNISTÍA INTERNACIONAL