Diciembre 2021

Informe de Amenazas en la industria de servicios de vigilancia por contratación

16 de diciembre de 2021

Por Mike Dvilyanski, líder de investigaciones de Ciberespionaje

David Agranovich, director de disrupciones de amenazas, y

Nathaniel Gleicher, líder de Políticas de Seguridad

Meta

Resumen

- La industria global de servicios de vigilancia por contratación se dirige a personas para recolectar, manipular y comprometer sus dispositivos y cuentas en Internet.

- Si bien estos “ciber-mercenarios” a menudo argumentan que sus servicios solo se dirigen a criminales y terroristas, nuestra investigación de varios meses concluye que esta acción es indiscriminada e incluye a periodistas, disidentes políticos, críticos de regímenes autoritarios, familias de la oposición y activistas de derechos humanos.

- Deshabilitamos siete entidades que se dirigían a personas en Internet en más de 100 países; compartimos nuestros hallazgos con investigadores de seguridad, otras plataformas y legisladores; mandamos alertas de Cese y Desistimiento; y también notificamos a las personas que creemos fueron blancos de estos ataques para ayudarlas a fortalecer la seguridad de sus cuentas.

Este reporte es el resultado de meses de investigación y la disrupción de siete entidades que ofrecían servicios de vigilancia por contratación dirigidos a personas en Internet, incluidos periodistas y defensores de derechos humanos. Detalla las acciones que tomamos en su contra e incluye nuestra investigación sobre lo que llamamos “cadena de vigilancia” – fases de ataque que observamos durante nuestra investigación. Esperamos contribuir a que haya un entendimiento más amplio de los daños que esta industria representa a nivel global y hacer un llamado a los gobiernos democráticos para tomar más medidas para proteger a las personas y vigilar a los vendedores de *spyware* ubicuo.

¿Qué es la contratación de servicios de vigilancia y cómo funciona?

En meses recientes, ha habido un mayor enfoque en NSO, la compañía detrás del *spyware* Pegasus (software usado para facilitar el espionaje) contra el que actuamos y demandamos en 2019. Sin embargo, es importante entender que NSO es solo una pieza de un ecosistema global más amplio de ciber-mercenarios. Como un esfuerzo aparte, hoy, estamos compartiendo nuestros hallazgos sobre siete entidades relacionadas con actividad de vigilancia y seguiremos tomando acciones sobre otras conforme las detectemos.

La industria de contratación de servicios de vigilancia apunta a personas en internet para recolectar información, manipularlos para revelar información y comprometer sus dispositivos y cuentas. Mientras que los ciber-mercenarios a menudo dicen que sus servicios y software de vigilancia están diseñados para enfocarse en criminales y terroristas, nuestra investigación encontró que, de hecho, atacan regularmente a periodistas, disidentes, críticos de regímenes autoritarios, familias de la oposición y defensores de derechos humanos alrededor del mundo. Estas compañías son parte de una industria en expansión que ofrece herramientas de software intrusivas y servicios de vigilancia de forma indiscriminada a cualquier cliente - sin importar a quién se dirija o si habilita violaciones a derechos humanos.

El ecosistema funciona para dar poderosas capacidades a sus clientes en contra de víctimas quienes, en la mayoría de los casos, no tienen forma de saber que son blancos de ataques. En cierta forma, esta industria “democratiza” estas amenazas, haciéndolas accesibles a gobiernos y grupos no gubernamentales que de otra forma no podrían causar daños. En efecto, aumentan exponencialmente la oferta de actores maliciosos en el mundo.

Observamos tres fases de actividad en estos actores comerciales, mismas que integran su "cadena de vigilancia": *Reconocimiento, Involucramiento* y *Explotación*. Cada fase informa a la siguiente y a menudo se repiten en ciclos. Si bien, algunas de estas entidades se especializan en una fase en particular, otras apoyan la cadena de principio a fin. A pesar de que hasta el momento el debate público se ha enfocado en la fase de ***explotación***, es fundamental desactivar todo el ciclo de vida del ataque, porque las primeras etapas habilitan las posteriores. Si colectivamente podemos combatir esta amenaza en una etapa temprana de la cadena de vigilancia, ayudaríamos a frenar el daño antes de que llegue a su etapa final, cuando se comprometen los dispositivos y cuentas de las personas.

A continuación más detalles y TTPs (tácticas, técnicas y procedimientos) característicos de cada etapa de la cadena de ataque.

Reconocimiento

Esta primera etapa de la cadena de vigilancia es comúnmente la menos evidente para las personas a las que se dirige, quienes son silenciosamente perfiladas por cibermercenarios a nombre de sus clientes, a menudo usando un software para automatizar la recolección de datos a lo largo de Internet. Usualmente, las empresas que venden estos servicios se promocionan como "servicios de inteligencia web" para facilitar la recolección, retención, análisis y capacidad de búsqueda, tanto de forma direccionada como a escala.

Comúnmente, estos servicios y aplicaciones están diseñados para recolectar información sobre las víctimas de todos los registros digitales disponibles. Típicamente, obtienen y guardan datos disponibles en sitios web públicos como blogs, redes sociales, plataformas de gestión de conocimiento como Wikipedia y Wikidata, medios de noticias, foros y sitios de la "dark web". Los softwares de vigilancia a menudo permiten ocultar el origen de la actividad a través de una infraestructura no atribuible.

Uno de los principales objetivos de la recolección de información en redes sociales es el uso de cuentas falsas. Estos recursos inauténticos pueden ser usados para buscar y ver perfiles de otras personas, Amigos, reacciones y otra información pública disponible, unirse a Grupos y Eventos y seguir o hacerse amigos de las personas que son blancos de los ataques. Por lo general, son administradas por el proveedor de servicio para sus clientes, u operadas por los propios clientes a través del software que proveé la firma de contratación de servicios de vigilancia. El nivel de sofisticación de estas cuentas falsas varía considerablemente por cada cibermercenario y cliente.

Involucramiento

La segunda fase de la cadena de vigilancia es, a menudo, la más visible para las víctimas y la más importante de ser detectada para evitar que la cuenta o dispositivo sean comprometidos. Está diseñada para establecer contacto con los individuos que son blancos de los ataques o personas cercanas a ellos, en un intento de ganarse su confianza, solicitar información y engañarlos para que den clic a enlaces o descarguen archivos (para habilitar la fase de "explotación").

Para hacer esto, los operadores usan tácticas de ingeniería social y crean personajes ficticios para contactar a las personas a través de correo electrónico, llamadas telefónicas, mensajes de texto o redes sociales. Estos personajes están hechos a la medida de cada víctima para que sean creíbles y evitar sospechas de intentos malintencionados. Generalmente, estos esfuerzos son prolongados e implican la creación de resguardos para personas y organizaciones falsas en múltiples servicios de Internet para que parezcan más legítimos y no caigan ante el escrutinio. Los objetivos de la ingeniería social pueden ir desde obtener información sensible que desee el cliente, hasta usar *malware* para habilitar la vigilancia digital de todo el dispositivo. Para lograrlo, los operadores pueden intentar dirigir a las personas a canales más directos como llamadas de voz o video, o incluso reuniones en persona.

Explotación

La etapa final de la cadena de vigilancia manifiesta lo que comúnmente se conoce como "*hacking for hire*". Los proveedores pueden crear dominios de *phishing* diseñados para engañar a las personas para que entreguen su información personal sobre servicios como su correo electrónico, redes sociales, servicios financieros y redes corporativas. Hemos visto que falsifican dominios de organizaciones de noticias, proveedores de servicios de telecomunicación, bancos y servicios que acortan las URLs para engañar a sus víctimas.

Para permitir la entrega de "carga útil" maliciosa, los operadores pueden usar su propio software exploit personalizado o adquirir herramientas maliciosas de otros proveedores. La sofisticación de herramientas varía significativamente en esta industria, yendo del *malware* estándar que es detectado fácilmente por la mayoría de los programas antivirus a enlaces de un solo clic o incluso de cero clics enviados a las víctimas. El objetivo final es permitir la vigilancia del dispositivo y el monitoreo de celulares y computadoras. En ese punto, dependiendo del software exploit, el atacante puede acceder a cualquier información en el dispositivo o computadora de la persona, incluyendo contraseñas, cookies, tokens de

acceso, fotos, videos, mensajes, carpetas de direcciones, así como activar silenciosamente el micrófono, la cámara y el rastreo de geolocalización.

Nuestros hallazgos de la investigación y las acciones que tomamos

Como resultado de nuestra investigación de varios meses, tomamos acciones contra siete diferentes entidades de vigilancia por contratación para interrumpir su capacidad de usar la infraestructura digital para abusar de las plataformas de redes sociales y permitir la vigilancia de personas a lo largo de Internet. Estas ofrecían servicios en las tres fases de la cadena de vigilancia que eran usados para apuntar a personas de forma indiscriminada. Estos proveedores de vigilancia están basados en China, Israel, India y el norte de Macedonia. Se dirigía a personas en más de 100 países a nombre de sus clientes.

Para desactivar estas actividades, bloqueamos infraestructura que estuviera relacionada, prohibimos estas entidades de nuestra plataforma y mandamos alertas de Cese y Desistimiento, para hacerles saber a cada una de ellas que su actividad no tiene lugar en nuestra plataforma y está en contra de nuestras Normas Comunitarias. También, compartimos nuestros hallazgos con investigadores de seguridad, otras plataformas y legisladores para que ellos a su vez puedan tomar las acciones apropiadas. Asimismo, notificamos a las personas que creemos pudieron haber sido blancos de ataques para ayudarles a tomar medidas para fortalecer la seguridad de sus cuentas.

Las entidades detrás de estas operaciones de vigilancia son persistentes y esperamos que sus tácticas evolucionen. Sin embargo, nuestros sistemas de detección e investigadores de amenazas, así como otros equipos en la comunidad de seguridad siguen mejorando para dificultar que no sean detectados. Seguiremos compartiendo nuestros descubrimientos cuando sea posible para que las personas estén al tanto de las amenazas que estamos detectando y puedan tomar medidas para fortalecer la seguridad de sus cuentas.

Esto es lo que detectamos

1. Cobwebs Technologies

Fases de la cadena de vigilancia: Reconocimiento e Involucramiento

Eliminamos cerca de 200 cuentas que eran operadas por Cobwebs y sus clientes alrededor del mundo. Esta empresa se fundó en Israel con oficinas en Estados Unidos y vende accesos a su plataforma que permite el reconocimiento de personas a lo largo de Internet, incluyendo Facebook, WhatsApp, Twitter, Flickr, sitios web públicos y de la "dark web". Además de recolectar información sobre sus objetivos, las cuentas usadas por los clientes de Cobwebs también se involucraron en técnicas de ingeniería social para unirse a comunidades y foros privados y engañar a las personas para que revelaran información personal.

Nuestra investigación identificó clientes en Arabia Saudita, Bangladesh, Estados Unidos, Hong Kong, Nueva Zelanda, México, Polonia y otros países. Además de los ataques relacionados con las actividades relacionadas al orden público, también observamos ataques frecuentes contra activistas, políticos de la oposición y funcionarios gubernamentales en Hong Kong y México.

2. Cognyte

Fases de la cadena de vigilancia: Reconocimiento e Involucramiento

Eliminamos cerca de 100 cuentas en Facebook e Instagram que estaban relacionadas a Cognyte (antes conocida como WebintPro) y sus clientes. Esta compañía está basada en Israel y vende accesos a su plataforma, que permite el manejo de cuentas falsas en redes sociales como Facebook, Instagram, Twitter, YouTube y VKontakte (VK) y otros sitios web para aplicar tácticas de ingeniería social y recolectar información.

Nuestra investigación identificó clientes en Israel, Serbia, Colombia, Kenia, Marruecos, México, Jordania, Tailandia e Indonesia. Sus objetivos incluían periodistas y políticos alrededor del mundo.

3. Black Cube

Fases de la cadena de vigilancia: Reconocimiento, Involucramiento y Explotación

Eliminamos cerca de 300 cuentas de Facebook e Instagram relacionadas a Black Cube, una firma israelí con oficinas en Reino Unido, Israel y España. Provee servicios de vigilancia que incluyen ingeniería social y la recolección de datos. Black Cube manejaba personajes ficticios hechos a la medida de sus objetivos: algunos de ellos se hacían pasar por estudiantes de posgrado, trabajadores de organizaciones y derechos humanos, así como productores de cine y televisión. Luego intentaban organizar llamadas para obtener los correos electrónicos personales de las víctimas, posiblemente para realizar ataques de *phishing* posteriormente. Black Cube se basaba en diferentes tácticas para ocultar su identidad, incluyendo realizar actividades no relacionadas, en un posible intento de esconder sus actividades maliciosas detrás de un "ruido" aparentemente inofensivo en redes sociales.

Nuestra investigación detectó una amplia variedad de clientes, incluyendo individuos privados, negocios y bufetes de abogados alrededor del mundo. Los ataques de Black Cube a nombre de sus clientes también se extendieron geográficamente en diversas industrias, incluyendo la de salud, la minera y la energética. También, incluyeron organizaciones en África, Europa del Este y Sudamérica, así como activistas palestinos. Igualmente, se dirigían a personas en Rusia asociadas a universidades, telecomunicaciones, tecnología, consultoría, industrias financieras, desarrollo de bienes raíces y medios de comunicación.

4. Bluehawk CI

Fases de la cadena de vigilancia: Reconocimiento, Involucramiento y Explotación

Eliminamos alrededor de 100 cuentas de Facebook relacionadas a Bluehawk, una firma basada en Israel con oficinas en Reino Unido y Estados Unidos. Colaboramos en esta investigación con The Daily Beast, quien identificó un subconjunto de esta actividad y nos llevó a descubrir su alcance completo y a su responsable a principios de este año. Bluehawk vende una amplia gama de actividades de vigilancia, que incluían ingeniería social, recopilación de información relacionada con litigios sobre personas y el manejo de cuentas falsas para engañar a las víctimas para que instalaran *malware*. Los individuos detrás de esta empresa fueron persistentes y siguieron intentando regresar a nuestra plataforma después de que eliminamos docenas de sus cuentas.

Estas cuentas falsas se hacían pasar por periodistas de grupos de medios existentes como La Stampa en Italia y Fox News en Estados Unidos, para que sus víctimas dieran una entrevista a cámara. Como lo reportó The Daily Beast, algunas de estas cuentas se dirigían a

opositores de Ras al-Khaimah en Emiratos Árabes Unidos, mientras que otras intentaron aplicar tácticas de ingeniería social a personas en Catar y políticos y hombres de negocios en Medio Oriente. Recientemente, Bluehwak intentó crear cuentas afirmando estar basada en Argentina.

5. BellTroX

Fases de la cadena de vigilancia: Reconocimiento, Involucramiento y Explotación

Eliminamos cerca de 400 cuentas de Facebook, la gran mayoría de las cuales estuvieron inactivas por años, relacionadas a BellTroX y usadas para reconocimiento, ingeniería social y el envío de enlaces maliciosos. BellTroX está basada en India y vende lo que se conoce como servicios de "*hacking for hire*", que fueron reportados por investigadores del Citizen Lab y Reuters. Su actividad en nuestra plataforma fue limitada y esporádica entre 2013 y 2019, y después se detuvo. BellTroX manejaba cuentas falsas para hacerse pasar por un político, por periodistas y activistas del medioambiente, en un intento de aplicar tácticas de ingeniería social a sus objetivos para solicitar información como su correo electrónico, posiblemente para ataques de *phishing* en una etapa posterior.

Esta actividad, usando exactamente las mismas maniobras, reanudó actividades en 2021 con un número pequeño de cuentas que se hacían pasar por periodistas y personalidades de medios para mandar enlaces de *phishing* y solicitar a sus víctimas sus correos electrónicos. Dentro de las personas a las que se dirigieron los ataques, estaban: abogados, doctores, activistas y miembros del clero en países como Australia, Angola, Arabia Saudita e Islandia.

6. Cytrox

Fases de la cadena de vigilancia: principalmente Explotación

Eliminamos alrededor de 300 cuentas en Facebook e Instagram relacionadas a Cytrox. Esta compañía del norte de Macedonia desarrolla software exploit y vende herramientas de vigilancia y malware que permite a sus clientes comprometer dispositivos iOS y Android. En colaboración con Citizen Lab, obtuvimos copias del malware iOS y Android para su análisis. Como resultado, nuestro equipo en Meta fue capaz de detectar una vasta infraestructura de dominio que creemos que Cytrox usaba para falsificar entidades de noticias en los países de su interés e imitar servicios legítimos de redes sociales y acortamiento de URLs (vea la lista completa de dominios en el Apéndice). Usaban estos dominios como parte de sus campañas de phishing y vulneración de dispositivos. Cytrox y sus clientes emprendieron acciones para personalizar sus ataques a personas específicas solo infectándolas con malware cuando pasaban ciertas verificaciones técnicas, incluida la dirección de IP y el tipo

de dispositivo. Si las verificaciones fallaban, las personas podían ser redirigidas a sitios legítimos de noticias u otros.

Nuestra investigación identificó clientes en Egipto, Armenia, Grecia, Arabia Saudita, Omán, Colombia, Costa de Marfil, Vietnam, Filipinas y Alemania. Nuestras investigaciones sugieren que Cytrox seguramente proveía servicios a otro actor de amenazas conocido en la comunidad de seguridad como Sphinx, que se dirigía a personas en Egipto y sus países vecinos.

7. Una entidad desconocida en China

Fases de la cadena de vigilancia: principalmente Reconocimiento y Explotación

Eliminamos cerca de 100 cuentas de Facebook e Instagram relacionadas a una entidad desconocida en China, responsable por el desarrollo de software de vigilancia para sistemas operativos Android, iOS y también Linux, Mac OS X y Solaris. También, está relacionada con actividad de reconocimiento e ingeniería social antes de la entrega de carga útil maliciosa a sus víctimas. Si bien no hemos podido atribuir esta actividad a un actor en particular, nuestra investigación y análisis de los servidores de mando y control detrás de esta herramienta de vigilancia indican que fue usada por las fuerzas del orden en China.

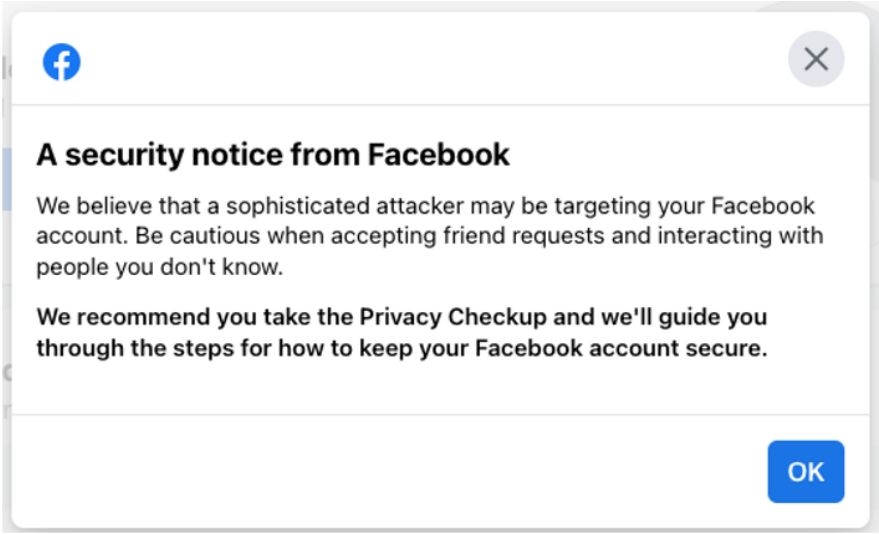
En algunas instancias, detectamos que el *malware* de este grupo se implementó junto a un software de reconocimiento facial desarrollado por una compañía con sede en Beijing. Al momento de nuestra investigación, el acceso a este sistema requería no solo de un usuario y contraseña, sino también de una llave de hardware física SuperDog de SafeNet, posiblemente para asegurar que solo los clientes autorizados a los que les fue otorgada esta llave pudieran usarlo. El análisis de las muestras de *malware* distribuidas por esta entidad proporcionaron información adicional, indicando que las personas responsables operaban en un esquema estándar de trabajo, de lunes a viernes. La mayoría del desarrollo de software ocurría los lunes, tiempo de Beijing.

Nuestra investigación detectó que las herramientas de malware fueron usadas para vigilancia contra grupos minoritarios a lo largo de la región Asia-Pacífico, incluyendo la región Xinjiang en China, Myanmar y Hong Kong.

Nuestra respuesta al abuso de los grupos de vigilancia por contratación

Las entidades de vigilancia por contratación que eliminamos y describimos en este reporte infringieron múltiples Normas Comunitarias y Términos del Servicio. Dada la severidad de

las infracciones, los hemos vetado de nuestros servicios. También, alertamos a cerca de 50,000 personas que creemos pudieron haber sido blancos de ataques maliciosos alrededor del mundo, usando el sistema de alertas que lanzamos en 2015. Recientemente, lo actualizamos para dar a las personas detalles más granulares acerca de los tipos de ataques y el actor detrás de estos, para que puedan tomar acciones para proteger sus cuentas, dependiendo de la fases de la cadena de ataques de vigilancia que detectemos en cada caso.



La existencia y proliferación de estos servicios alrededor del mundo levantan un número importante de preguntas. Si bien estos ciber-mercenarios a menudo argumentan que sus servicios y software de vigilancia están destinados a enfocarse solo a criminales y terroristas, nuestra propia investigación, investigadores independientes, nuestros pares en la industria y gobiernos han demostrado que los ataques son, en efecto, indiscriminados e incluyen a periodistas, disidentes, críticos de gobiernos autoritarios, familias de la oposición y defensores de derechos humanos. De hecho, en plataformas como las nuestras, no hay una forma escalable de discernir el propósito o la legitimidad de esta acción. Además, el uso de estos servicios de terceros oculta quién es el cliente final, que se recolecta y cómo se usa la información en contra de grupos vulnerables. Por esto, nos enfocamos en actuar en contra de este comportamiento, sin importar quién está detrás o quién pueda ser la víctima.

Para apoyar el trabajo de las autoridades, ya contamos con canales autorizados en los cuales las agencias de gobierno pueden presentar requerimientos legales de información, en lugar de recurrir a la industria de vigilancia por contratación que indiscriminadamente vende estos servicios a cualquiera que esté dispuesto a pagar, incluyendo actores maliciosos conocidos. Estos canales están diseñados para salvaguardar el debido proceso y

reportamos la cantidad y origen de estas solicitudes de forma pública para que las personas alrededor del mundo puedan tener toda la información necesaria.

Seguiremos investigando y actuando contra cualquiera que abuse de nuestras aplicaciones. Sin embargo, estos ciber-mercenarios trabajan en diferentes plataformas y más allá de los límites nacionales. Sus capacidades son usadas tanto por los estados-nación como por las empresas privadas, y reducen de forma efectiva la barrera de entrada para cualquiera que esté dispuesto a pagar. Para sus víctimas, a menudo es imposible saber si están siendo vigilados en Internet.

Proteger a las personas contra estas amenazas requiere un esfuerzo colectivo entre plataformas, legisladores y sociedad civil para contrarrestar el mercado subyacente y su estructura de incentivos. Creemos que una discusión pública acerca del uso de la tecnología de vigilancia por contratación es urgente para desalentar el abuso de estas capacidades tanto entre quienes las venden como entre quienes las compran, con base en los siguientes principios:

- **Más transparencia y supervisión:** Existe la necesidad de una supervisión internacional robusta que establezca los estándares de transparencia de "conozca a su cliente" para este mercado y regule a las entidades de vigilancia por contratación bajo estas normas.
- **Colaboración de la industria:** Los esfuerzos de vigilancia se manifiestan de manera diferente en varias plataformas tecnológicas, lo que hace que la colaboración de la industria sea fundamental si queremos comprenderlos y mitigarlos por completo. Estamos dispuestos a trabajar con nuestros colegas en la industria para investigar abusos, compartir y desactivar las amenazas de vigilancia por contratación, incluso mediante el uso de recursos legales, para que colectivamente podamos disuadir su uso e imponer costos a los servicios abusivos.
- **Gobernanza y ética:** Agradecemos los esfuerzos nacionales e internacionales para aumentar la responsabilidad de los actores a través de una legislación, controles de exportación y acciones regulatorias. También, fomentamos conversaciones más amplias dirigidas por la sociedad civil y los reguladores sobre el uso ético de estas tecnologías por parte de las fuerzas del orden y empresas privadas, así como la creación de marcos efectivos para la protección de víctimas.

Hasta hace poco, estos ciber-mercenarios rara vez enfrentaban consecuencias cuando sus productos eran usados para atacar a grupos vulnerables como activistas, periodistas y grupos minoritarios, y causaban daños severos. Nos alienta ver a nuestros pares y gobiernos unirse al esfuerzo que comenzamos en 2019 y generar consciencia sobre esta amenaza.

Para que nuestra respuesta colectiva contra el abuso sea efectiva, es necesario que las plataformas tecnológicas, la sociedad civil y los gobiernos democráticos aumenten los costos en esta industria global y desincentiven el uso de estos servicios abusivos de vigilancia por contrato. Nuestra esperanza con este informe de amenazas es contribuir a este esfuerzo global y ayudar a visibilizar la forma en la que opera esta industria.

Apéndice

Indicadores de compromiso relacionados a Cytrox

2y4nothing[.]xyz
5m5[.]io addons[.]news
adibjan[.]net
adservices[.]gr[.]com
adultpcz[.]xyz
advertsservices[.]com
advfb[.]xyz affise[.]app
almasryelyuom[.]com
alpineai[.]uk
alraeeenews[.]com
alraeesnews[.]net
altsantiri[.]news
amazing[.]lab
ancienthistory[.]xyz
android-apps[.]tech
api-apple-buy[.]com
api-telecommunication[.]com
applepps[.]com
apps-ios[.]net
aramexegypt[.]com
atheere[.]com
audit-pvv[.]com
bank-alahly[.]com
bbcsworld[.]com bitlinkin[.]xyz
bi[.]tly[.]gr[.]com bi[.]tly[.]link
bit-li[.]com
bit-li[.]ws
bit-ly[.]link
bit-ly[.]org bitlly[.]live
bitlyrs[.]com

bitt[.]fi
bity[.]ws bityl[.]me
blacktrail[.]xyz
bmw[.]gr[.]com
bookjob[.]club
browsercheck[.]services
bumabara[.]bid
burgerprince[.]us
businesnews[.]net
canyouc[.]xyz
carrefourmisr[.]com
cbbc01[.]xyz celebrnewz[.]xyz
cellconn[.]net
charmander[.]xyz
chatwithme[.]store
citroen[.]gr[.]com
ckforward[.]one
clockupdate[.]com
cloudstatistics[.]net
cloudtimesync[.]com
cnn[.]gr[.]com
connectivitycheck[.]live
connectivitycheck[.]online
connectivitychecker[.]com
covid19masks[.]shop
crashonline[.]site
cut[.]red
cyber[.]country danas[.]bid
distedc[.]com
download4you[.]xyz
dragonair[.]xyz eagerfox[.]xyz
ebill[.]cosmote[.]center
efsyn[.]online egyqaz[.]com
engine[.]ninja enigmase[.]xyz
enikos[.]news ereportaz[.]news
espressonews[.]gr[.]com
etisalategypt[.]tech
etisalatgreen[.]com ewish[.]cards
fastdownload[.]me
fastuploads[.]xyz
fbc8213450838f7ae251d4
519c195138[.]xyz
ferrari[.]gr[.]com ffoxnewz[.]com
fimes[.]gr[.]com fireup[.]xyz
fisherman[.]engine[.]ninja
flexipagez[.]com
forwardeshoptt[.]com
getsignalapps[.]com
getsignalapps[.]live
getupdatesnow[.]xyz
goldenscent[.]net
goldenscint[.]com
goldescent[.]com gosokm[.]com
guardian-tt[.]me guardnews[.]live
heaven[.]army heiiasjournai[.]com
hellasjournal[.]company
hellasjournal[.]website
hellottec[.]art hempower[.]shop
hopnope[.]xyz
icloudeu[.]com
icloudflair[.]com iibt[.]xyz
ikea-egypt[.]net ilnk[.]xyz
in-politics[.]com
infosms-a[.]site
inservices[.]digital
insider[.]gr[.]com
instagam[.]click
instagam[.]in
instagam[.]photos
instegram[.]co invoker[.]icu
ios-apps[.]store
iosmnbg[.]com
itcgr[.]live
itly[.]link
itter[.]me
jquery-updater[.]xyz
kathimerini[.]news
kinder[.]engine[.]ninja
koenigseggg[.]com
kohaicorp[.]com
koora-egypt[.]com
kormoran[.]bid
kranos[.]gr[.]com
lamborghini-s[.]shop
landingpg[.]xyz
landingpge[.]xyz
leanwithme[.]xyz
lexpress[.]me
lifestyleshops[.]net
limk[.]one linkit[.]digital

linktothisa[.]xyz link-m[.]xyz
link-protection[.]com
liponals[.]store
livingwithbadkidny[.]xyz
llinkedin[.]net lnkedin[.]org
localegem[.]net
lylink[.]online
makeitshort[.]xyz
mifcbook[.]link
md-news-direct[.]com
miniiosapps[.]xyz
mitube1[.]link mlinks[.]ws
mobnetlink1[.]com
mobnetlink2[.]com
mobnetlink3[.]com
mozillaupdate[.]xyz
msas[.]ws
mycoffeeshop[.]shop
myfcbk[.]net mytrips[.]quest
myutbe[.]net
mywebsitevpstest[.]xyz
nabd[.]site
nabde[.]app
nassosblog[.]gr[.]com
nemshi-news[.]xyz
nemshi[.]net
networkenterprise[.]net
newsbeast[.]gr[.]com
newslive2[.]xyz newzeto[.]xyz
newzgroup[.]xyz
niceonase[.]com
niceonesa[.]net nikjol[.]xyz
nissan[.]gr[.]com novosti[.]bid
oilgy[.]xyz olexegy[.]com
olxeg[.]com omanreal[.]net
omeega[.]xyz
onlineservices[.]gr[.]com
orangegypt[.]co
orchomenos[.]news
otaupdatesios[.]com
paok-24[.]com pastepast[.]net
pdfviewer[.]app playestore[.]net
pocopoc[.]xyz politika[.]bid
politique-koaci[.]info
prmopromo[.]com
pronews[.]gr[.]com
protothema[.]live proupload[.]xyz
ps1link[.]xyz ps2link[.]xyz
quickupdates[.]xyz qwert[.]xyz
qwxzyl[.]com redeitt[.]com
safelyredirecting[.]com
safelyredirecting[.]digital
sepenet[.]gr[.]com
sephoragroup[.]com
servers-mobile[.]info
serviceupdaterequest[.]com
sextape225[.]me
shorten[.]fi shortenurls[.]me
shortmee[.]one
shortwidgets[.]com
shortxyz[.]com
simetricode[.]uk
sinai-new[.]com
sitepref[.]xyz smsuns[.]com
snapfire[.]xyz sniper[.]pet
solargoup[.]xyz
solargroup[.]xyz
speedy[.]sbs
speedygonzales[.]xyz
speedymax[.]shop
sportsnewz[.]site
sports-mdg[.]xyz
static-graph[.]com
stonisi[.]news
supportset[.]net
suzuki[.]gr[.]com
svetovid[.]bid symoty[.]com
syncservices[.]one
synctimestamp[.]com
syncupdate[.]site
telecomegy-ads[.]com
telenorconn[.]com
tesla-s[.]shop teslal[.]shop
teslal[.]xyz teslali[.]com

tgrthgsrgwrthwrtgwr[.]xyz
timestampsync[.]com
timeupdate[.]xyz
timeupdateservice[.]com
tiny[.]gr[.]com
tinylinks[.]live tinyulrs[.]com
tinyurl[.]cloud tiol[.]xyz
tly[.]gr[.]com tly[.]link
tovima[.]live trecv[.]xyz
trecvf[.]xyz trkc[.]online
tsrt[.]xyz tw[.]itter[.]me
twtter[.]net ube[.]gr[.]com
uberegypt[.]cn[.]com
updates4you[.]xyz
updateservice[.]center
updatetime[.]zone
updatingnews[.]xyz
updete[.]xyz
url-promo[.]club url-tiny[.]app
userviceschеck[.]com
uservicesforyou[.]com
utube[.]digital viva[.]gr[.]com
vodafoneegypt[.]tech
vodafonegypt[.]com
wavekli[.]xyz
we-site[.]net weathear[.]live
weathernewz[.]xyz
weathersite[.]online
webaffise[.]com wha[.]tsapp[.]me
worldnws[.]xyz wtc1111[.]com
wtc2222[.]com wtc3333[.]com
xf[.]actor
xnxx-hub[.]com xyvok[.]xyz
yallakora-egy[.]com
yo[.]utube[.]digital yo[.]utube[.]to
youarefired[.]xyz
yout[.]ube[.]gr[.]com
youtu-be[.]net youtub[.]app
youtube[.]gr[.]live youtube[.]voto
youtubesyncapi[.]com
youtubewatch[.]co
yuom7[.]net z2a[.]digital
z2adigital[.]cloud z2digital[.]cloud
zougla[.]gr[.]com zougla[.]news