Cómo pueden los hackers y los espías sabotear la lucha contra el coronavirus

Por Bruce Schneier y Margaret Bourdeaux

Foreign Policy
28 de febrero de 2020

Fotografía de Jonathan Chng (publicada en Unsplash).

Maquetación: Alejandra J. García Romero
Wordsbridge Linguistic Services

Los servicios de inteligencia cuentan con un largo historial de manipulaciones de información sobre temas relacionados con la salud, y las epidemias son especialmente tentadoras para realizar manipulaciones.

¿Por qué no estamos mejor preparados?

El mundo está tratando de contener la expansión del nuevo coronavirus, que se propaga por todo el planeta a una velocidad alarmante. En estos momentos, los expertos en enfermedades pandémicas de la Organización Mundial de la Salud (OMS) y los Centros para el Control y la Prevención de Enfermedades de los Estados Unidos (CDC), así como otros organismos de salud pública, se encuentran reuniendo información para determinar cómo y dónde se está propagando el virus. Para ello, utilizan una variedad de sistemas de comunicaciones y vigilancia digitales.

Al igual que la mayoría de las instalaciones médicas, estos sistemas son muy vulnerables a los ataques de los hackers y a las interferencias. Tal vulnerabilidad debería generar una gran preocupación.

Desde hace algún tiempo, los gobiernos y los servicios de inteligencia han manifestado su interés en manipular la información relacionada con la salud, tanto en sus propios países como en el extranjero. Es posible que lo hagan para evitar el pánico generalizado, prevenir el daño a sus economías o evitar el descontento público (por ejemplo, en casos en que las autoridades cometan errores graves en la contención de un brote).Desde hace algún tiempo, los gobiernos y los servicios de inteligencia han manifestado su interés en manipular la información relacionada con la salud, tanto en sus propios países como en el extranjero. Es posible que lo hagan para evitar el pánico generalizado, prevenir el daño a sus economías o evitar el descontento público (por ejemplo, en casos en que las autoridades cometan errores graves en la contención de un brote).

Fuera de sus fronteras, los estados pueden recurrir a la desinformación para debilitar a sus adversarios o romper una alianza entre otras naciones. Una epidemia que se produce de forma repentina, durante la cual los países se esfuerzan por controlar no solo el brote, sino también sus consecuencias sociales, económicas y políticas, resulta especialmente tentadora en lo que se refiere a las manipulaciones.

En el caso del coronavirus, tales manipulaciones son ya una realidad, lo cual no debería ser una sorpresa. Aquellos países hostiles hacia Occidente poseen un largo historial de manipulaciones de información sobre temas relacionados con la salud para sembrar la desconfianza. Por ejemplo, en la década de 1980, la Unión Soviética difundió una historia falsa según la cual el Departamento de Defensa de los

Estados Unidos había realizado operaciones de ingeniería biológica del VIH con el fin de asesinar a personas afroamericanas. Esta propaganda fue bastante efectiva: aproximadamente 20 años después de la primera campaña de desinformación soviética, una encuesta realizada en 2005 reveló que el 48 % de la población afroamericana estaba convencida de que el VIH se había fabricado en un laboratorio, mientras que el 15 % pensaba que se trataba de un instrumento de genocidio dirigido a sus comunidades.

Posteriormente, en 2018, Rusia llevó a cabo una exhaustiva campaña de desinformación para impulsar el movimiento antivacunas a través de plataformas de redes sociales como Twitter y Facebook. Recientemente, también en 2018, Rusia realizó una investigación que confirmó que trolls y bots rusos tuiteaban mensajes antivacuna hasta 22 veces más rápido que la media de los usuarios. Según otros investigadores, la exposición a estos mensajes provocó una importante disminución en la aplicación de la vacuna, lo que pone en peligro la vida de las personas y la salud pública.

La semana pasada, las autoridades estadounidenses acusaron a Rusia de difundir desinformación sobre el coronavirus en otra campaña coordinada. A mediados de enero, miles de cuentas de Twitter, Facebook e Instagram, (muchas de las cuales habían estado previamente vinculadas a Rusia), empezaron a publicar mensajes casi idénticos en inglés, alemán, francés y otros idiomas, señalando a los Estados Unidos como responsable del brote. Algunos de los mensajes afirmaban que el virus forma parte de una iniciativa de los EE. UU. para iniciar una guerra económica contra China, mientras que otros afirmaban que se trata de un arma biológica diseñada por la CIA.

Por mucho que esta desinformación pueda sembrar la discordia y socavar la confianza de los ciudadanos, el mayor peligro se encuentra en las infraestructuras de respuesta a emergencias de los Estados Unidos con escasa protección, especialmente los sistemas de vigilancia sanitaria utilizados para supervisar y hacer un seguimiento de la epidemia. Al piratear estos sistemas y corromper los datos médicos, los estados que poseen una capacidad cibernética extraordinaria pueden cambiar y manipular los datos directamente en la fuente.

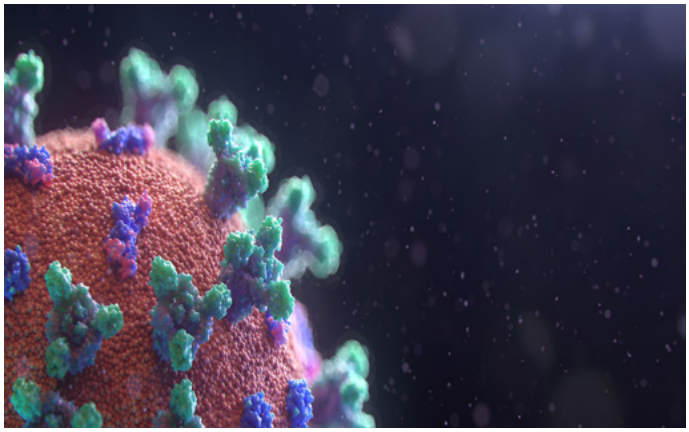
Así es como funcionaría, y la razón por la que deberíamos estar muy preocupados. Los numerosos sistemas de vigilancia sanitaria supervisan la propagación de los casos de coronavirus, incluida la red de vigilancia contra la gripe del CDC. Casi todas las pruebas se realizan a nivel local o regional, y los organismos de salud pública como el CDC únicamente recopilan y analizan los datos. Solo se envía una muestra biológica real a un laboratorio gubernamental de alto nivel en contadas ocasiones. De hecho, muchas de las clínicas y laboratorios que proporcionan resultados al CDC ya no archivan informes del mismo modo que antes, sino que disponen de varias capas de software para almacenar y transmitir los datos.

Las posibles vulnerabilidades de estos sistemas son numerosas como, por ejemplo, hackers que explotan los errores del software, accesos no autorizados a los servidores de los laboratorios por otras vías o intromisiones en las comunicaciones digitales entre los laboratorios y el CDC. Resulta especialmente preocupante que los programas informáticos que intervienen en el seguimiento de las enfermedades puedan, en ocasiones, acceder a los registros médicos electrónicos ya que, con frecuencia, esos registros están integrados en la red de dispositivos digitales de una clínica u hospital. Un dispositivo de este tipo conectado a la red de un determinado hospital puede, en teoría, utilizarse para atacar toda la base de datos de coronavirus del CDC.

En la práctica, hackear los sistemas de un hospital puede ser increíblemente fácil. Como parte de un estudio sobre ciberseguridad, investigadores israelíes de la Universidad Ben-Gurion consiguieron piratear la red de un hospital a través del sistema de Wi-Fi público. Una vez dentro, pudieron acceder a la mayoría de las bases de datos y sistemas de diagnóstico del hospital. Al obtener el control de la base de datos de imágenes no encriptadas del hospital, los investigadores instalaron un malware que alteró las tomografías de los pacientes sanos para mostrar tumores inexistentes.

Los radiólogos que examinaron estas imágenes únicamente pudieron distinguir entre las tomografías reales y las modificadas el 60 % de las veces, incluso después de saber que algunas de ellas habían sido manipuladas.

Otro estudio directamente relacionado con las emergencias de sanidad pública mostró que una iniciativa de seguridad biológica muy importante de los Estados Unidos, el programa BioWatch del Departamento de Seguridad Nacional, era vulnerable a los ciberataques desde hacía más de una década. Este programa hace un seguimiento de más de 30 jurisdicciones de los Estados Unidos y permite a las autoridades sanitarias detectar rápidamente un ataque con armas biológicas. Hackear este programa puede encubrir un ataque o hacer creer a las autoridades que se ha producido uno.



Fotografía de Fusion Medical Animation (publicada en Unsplash).

Afortunadamente, no ha salido a la luz ningún caso de sabotaje de los servicios sanitarios por parte de los servicios de inteligencia o de hackers (lo más parecido ha sido una serie de ataques de ransomware para extorsionar dinero a los hospitales, lo que ha causado importantes filtraciones de datos e interrupciones de los servicios médicos). Pero, con frecuencia, otras infraestructuras críticas también se consideran un objetivo. Los rusos han hackeado la red eléctrica nacional de Ucrania en repetidas ocasiones, y también han realizado sondeos en las centrales e infraestructuras eléctricas de los Estados Unidos. Por otro lado, tanto Estados Unidos como Israel han hackeado el programa nuclear iraní, al tiempo que Irán ha atacado la infraestructura petrolífera de Arabia Saudí. No hay razón para pensar que no puedan acceder a la infraestructura del sistema de salud pública.

A pesar de estos precedentes y de los riesgos demostrados, todavía no se ha realizado una evaluación detallada de la vulnerabilidad de los sistemas de vigilancia sanitaria de los Estados Unidos frente a infiltraciones y manipulaciones. Con el coronavirus a punto de convertirse en una pandemia, los Estados Unidos corren el riesgo de no disponer de datos fiables, algo que, a su vez, puede paralizar la capacidad de respuesta de nuestro país.

En condiciones normales, las autoridades sanitarias disponen de mucho tiempo para detectar patrones inusuales en los datos y rastrear la información incorrecta y, si es necesario, también pueden recurrir al método tradicional de hacer una llamada al laboratorio. Pero, en el transcurso de una epidemia, cuando hay decenas de miles de casos que rastrear y analizar, es muy fácil que los agotados expertos en enfermedades y las autoridades sanitarias se vean engañados por datos corruptos. La confusión resultante puede conducir a una mala asignación de recursos, ofrecer falsas esperanzas de que el número de casos está disminuyendo, o desperdiciar un tiempo precioso cuando los encargados de tomar las decisiones tratan de validar datos incoherentes.

Ante una posible pandemia mundial, las autoridades de la salud pública de los Estados Unidos y de otros países deben evaluar y reforzar sin demora la seguridad de los sistemas sanitarios digitales de sus respectivos países. Asimismo, tienen un importante papel que desempeñar en el gran debate sobre la ciberseguridad. Hacer que la infraestructura sanitaria estadounidense sea segura requiere una reorientación radical de la ciberseguridad, que se centre en la defensa y no en el ataque.

La posición de muchos gobiernos, incluido el de los Estados Unidos, sobre la necesidad de mantener vulnerable la infraestructura de Internet para poder espiar mejor a los demás ya no es sostenible. La carrera armamentista digital, en la que cada vez más países adquieren capacidades de ataque cibernético cada vez más sofisticadas, no hace sino aumentar la vulnerabilidad de los Estados Unidos en áreas críticas como, por ejemplo, el control de pandemias. Al resaltar la importancia de proteger la infraestructura sanitaria digital, las autoridades de la sanidad pública pueden y deben pedir una Internet bien defendida y pacífica como base para un mundo saludable y seguro.

Fuente: https://www.schneier.com/essays/archives/2020/02/how_hackers_and_spie.html

Traducción: https://wordsbridge.co.uk/como-pueden-los-hackers-y-los-espias-sabotear-la-lucha-contra-el-coronavirus/