# Hackeo informático gubernamental

## ¿Qué es y cuándo debe utilizarse?

Agosto de 2022

El cifrado es un componente fundamental de nuestra vida cotidiana. Para gran parte del mundo, los aspectos básicos de la vida dependen del cifrado para funcionar. Los sistemas de energía, el transporte, los mercados financieros y los monitores para bebés[1] son más confiables debido al cifrado. El cifrado protege nuestros datos más vulnerables de los criminales y terroristas, pero también puede ocultar contenido criminal de los gobiernos.

El hackeo informático gubernamental es uno de los enfoques que utilizan las agencias de seguridad nacional y de aplicación de la ley para obtener acceso a información cifrada (por ejemplo, el FBI contrató a una empresa de piratería para desbloquear el iPhone en el caso del centro de San Bernardino[2]). Complementa sus otros esfuerzos para obtener acceso excepcional[3] al solicitar o exigir a las empresas de tecnología que tengan la capacidad técnica de descifrar el contenido de los usuarios cuando se solicita con fines policiales.

Internet Society considera que un cifrado sólido es vital para la salud de Internet y está profundamente preocupada por cualquier política o acción que pueda ponerla en peligro, independientemente de su motivación. El hackeo informático gubernamental plantea un riesgo de daño colateral tanto para Internet como para sus usuarios y, como tal, solo debe considerarse como una herramienta de último recurso, que se implementará bajo condiciones estrictas y salvaguardas verificables.

## Definición de hackeo informático gubernamental

Definimos como "hackeo informático gubernamental" al aprovechamiento de las vulnerabilidades en los sistemas, software o hardware para obtener acceso a información que está cifrada o es inaccesible por parte de entidades gubernamentales (por ejemplo, agencias de seguridad nacional o de aplicación de la ley o actores privados en su nombre).

---

1 Los monitores de bebés y las cámaras de seguridad bien diseñados deben proteger sus datos para garantizar su confidencialidad en Internet; no todos lo hacen.

2 https://en.wikipedia.org/wiki/FBI%E2%80%93Apple_encryption_dispute#Apple_ordered_to_assist_the_FBI

3 https://www.internetsociety.org/wp-content/uploads/2019/05/FactSheet-EncryptionVsLawful-Access-EN.pdf

CC BY-NC-SA 4.0

# Peligros del hackeo informático gubernamental

El aprovechamiento de vulnerabilidades de cualquier tipo ya sea para hacer cumplir la ley, realizar pruebas de seguridad o con cualquier otra finalidad, no debe tomarse a la ligera. Desde una perspectiva técnica, hackear un recurso de tecnología, información o comunicaciones (TIC) sin el consentimiento del usuario o propietario es siempre un ataque, independientemente de su motivación. Los ataques pueden dañar un dispositivo, un sistema o un flujo de comunicaciones activas, o bien dejarlos en condiciones menos seguras. Esto aumenta de manera significativa el riesgo de fallas futuras, pudiendo perjudicar a todos los usuarios del sistema.[4]

Los riesgos aumentan cuando los gobiernos se aprovechan de las "vulnerabilidades del día cero": vulnerabilidades en software o hardware que el proveedor desconoce o que aún no se han mitigado (por ejemplo, no se ha lanzado ningún parche). Este enfoque es particularmente peligroso ya que expone a Internet y a sus usuarios a nuevos riesgos de seguridad para los cuales no existe una defensa preparada. Debido a esto, debe haber procesos claros para la divulgación responsable y la mitigación coordinada de las vulnerabilidades de seguridad descubiertas lo antes posible para que puedan ser tratadas.[5]

**Las vulnerabilidades pueden ser robadas, filtradas o replicadas.** Incluso las entidades gubernamentales con los niveles más altos de seguridad se han visto comprometidas. Por ejemplo: el grupo ShadowBrokers pirateó a la Agencia de Seguridad Nacional de los EE. UU., y expuso públicamente la vulnerabilidad que se aprovechó el día cero de EternalBlue de la agencia[6]; la empresa de seguridad italiana, Hacking Team, fue pirateada en 2015[7]; y un conjunto de herramientas de piratería de la Agencia Central de Inteligencia conocido como Vault 7 se filtró en 2017.[8]

Cualquier aprovechamiento de vulnerabilidades, independientemente de su origen, puede ser reutilizado por delincuentes o actores estatales para atacar a los usuarios inocentes. El ransomware Petya/NoPetya (basado en EternalBlue) causó consecuencias en la vida real, como retrasos en tratamientos médicos, la suspensión de operaciones bancarias y la interrupción de servicios

4 La piratería técnica también puede dañar la integridad de la evidencia digital, socavando así la aplicación efectiva de la ley y el proceso judicial.

5 Esto va más allá de una llamada para crear Procesos equitativos de vulnerabilidad (como por ejemplo https://cyberstability.org/norms/#toggle-id-5) en el sentido de que llama a revelar cada vulnerabilidad.

6 https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html

7 https://www.vice.com/en_us/article/3k9zzk/hacking-team-hacker-phineas-fisher-has-gotten-away-with-it

8 https://es.wikipedia.org/wiki/Vault_7

CC BY-NC-SA 4.0

portuarios.[9] Estos incidentes resaltan los peligros de cualquier entidad, incluidos los gobiernos, que acumule vulnerabilidades de día cero y cree y almacene vulnerabilidades.

**Los equipos de piratería comercial no venden sus servicios solamente a "los tipos buenos".** En 2019, los investigadores de seguridad descubrieron que el software del Grupo NSO, una empresa de inteligencia cibernética israelí utilizada por muchas agencias gubernamentales, se había utilizado para piratear las cuentas de WhatsApp de periodistas y activistas para inspeccionar en secreto sus comunicaciones. Otros informes de noticias similares indican que este no fue de ninguna manera el único uso de la tecnología.[10] [11] [12] [13]

**Un objetivo puede convertirse en varios.** El hackeo informático gubernamental puede estar destinada a ser dirigida y quirúrgica, una técnica de piratería o aprovechamiento que funciona en un objetivo puede volverse contra otros dispositivos del mismo tipo y, a menudo, también contra otros dispositivos y sistemas. Las vulnerabilidades y las herramientas también pueden descubrirse o divulgarse de manera incorrecta, o usarse para otros fines, por ejemplo, para participar en ataques o guerra cibernéticos por parte de actores de amenazas persistentes avanzadas (APT)[14], que a menudo están alineados con el estado. Es posible que el ejemplo más famoso de una APT sea el virus Stuxnet, presuntamente creado por los gobiernos de EE. UU. e Israel para destruir las centrifugadoras nucleares iraníes, que luego se propagó a todo el mundo (mucho más allá del objetivo previsto) afectando a millones de otros sistemas.[15]

**Los atacantes descubren las vulnerabilidades existentes en los sistemas informáticos todo el tiempo.** Mantener en secreto una vulnerabilidad (para aprovecharla más adelante) no evitará que otros la descubran. Por ejemplo, para el sistema operativo Android, la tasa de redescubrimiento de vulnerabilidades de gravedad alta y crítica es de hasta un 23 % en un año.[16] Dada la existencia de debilidades, los más motivados, como criminales, terroristas y gobiernos hostiles, trabajarán más duro que nadie para encontrarlas y aprovecharse de ellas. Su valor queda demostrado por los

9 https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how
10 https://www.nytimes.com/2019/05/13/technology/nso-group-whatsapp-spying.html
11 https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html
12 https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/
13 https://www.wired.com/story/nso-group-pegasus-el-salvador/
14 https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html
15 https://www.cybereason.com/blog/advanced-persistent-threat-apt
16 Herr & Schneier: "What You See Is What You Get: Revisions to Our Paper on Estimating Vulnerability Rediscovery" (Lawfare 2017) https://www.belfercenter.org/sites/default/files/files/publication/Vulnerability%20Rediscovery%20%28belfer-revision%29.pdf

CC BY-NC-SA 4.0

precios y la demanda que existe en los mercados negro y gris.[17] Usar aprovechamientos de trabajo para realizar ingeniería inversa lo hará aún más fácil.

**Cruzar jurisdicciones.** También existe el riesgo de infiltrarse o alterar inadvertidamente las redes o sistemas de una nación extranjera, un acto que podría considerarse como un ataque contra la nación, sus intereses o sus ciudadanos, con las consecuencias políticas, económicas y potenciales de ciberataque asociadas. Esto también puede alentar a algunos países a seguir un enfoque soberano de Internet.

## La posición de Internet Society acerca del cifrado y el hackeo informático gubernamental

Como fundamento técnico a favor de la confianza en Internet, el cifrado fomenta la libertad de expresión, el comercio, la privacidad y la confianza de los usuarios, además de ayudar a proteger los datos y las comunicaciones de daños accidentales y maliciosos. Internet Society cree que el cifrado debe ser la norma para el tráfico de Internet y el almacenamiento de datos, y no es el único que cree en ello. Por ejemplo, el relator especial de la ONU sobre Derechos Humanos y la OCDE han hecho declaraciones firmes en apoyo de las herramientas de cifrado.[18]

Los intentos legales y técnicos de limitar el uso del cifrado, incluso con buenas intenciones, afectarán negativamente la seguridad de los ciudadanos respetuosos de la ley y de Internet en general.

**El hackeo del gobierno para eludir el cifrado** también pone en riesgo la seguridad de usuarios inocentes, sistemas críticos (incluidas redes y servicios gubernamentales) y la Internet.

No apoyamos el hackeo informático del gobierno que representa un riesgo para la seguridad de Internet y sus usuarios. Debido al riesgo de daños colaterales, nunca debe convertirse en un enfoque rutinario de las fuerzas del orden o de los gobiernos, el tener acceso al contenido cifrado. También nos oponemos a las leyes y otras reglamentaciones que exigen que las compañías tecnológicas incorporen vulnerabilidades de seguridad en sus productos y servicios. Existe abundante evidencia de que tales vulnerabilidades son inevitablemente filtradas o descubiertas y utilizadas para causar daño.

17 Consulte por ejemplo https://en.wikipedia.org/wiki/Cyber-arms_industry#Notable_markets para encontrar algunos ejemplos que se nombran de esos mercados

18 Consulte https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx y http://www.oecd.org/sti/ieconomy/cryptography.htm respectivamente.

CC BY-NC-SA 4.0

El riesgo es particularmente grave para la piratería gubernamental que se basa en aprovechamientos y vulnerabilidades de día cero (como se señaló anteriormente). Sin embargo, también es un riesgo cuando se conocen las vulnerabilidades, pero no se corrigen, quizás porque los sistemas son demasiado antiguos, porque las personas no pueden pagar dispositivos más seguros o debido a procedimientos de parcheo inadecuados.

Como principio general, la explotación de fallas en cualquier sistema crea un peligro inherente. Incluso en un escenario perfecto donde una entidad gubernamental utiliza un aprovechamiento con las mejores intenciones, con la debida autorización y con un resultado positivo, existe un alto riesgo de que el aprovechamiento no se quede dentro de los límites de ese gobierno. El sistema, en su conjunto, se vuelve menos seguro simplemente porque se ha utilizado el aprovechamiento, independientemente de la intención.

Dados los riesgos inherentes, los gobiernos no deben recopilar, solicitar, comprar, crear, almacenar o aprovecharse de las vulnerabilidades con el fin de obtener acceso a la información a los fines de la seguridad nacional u otros fines de aplicación de la ley a menos que se apliquen las siguientes condiciones:

- Grave: cuando se puede demostrar que es necesario proteger la vida humana, contrarrestar los riesgos inminentes y significativos para la seguridad pública, o prevenir los delitos más graves.
- Último recurso: cuando no existe otra alternativa viable.
- Judicial: cuando se realiza conforme a una orden judicial debidamente ejecutada.
- Proporcional: una operación puede considerarse objetivamente como una empresa específica y proporcionada con un alcance lo más limitado posible.
- Mitigar el riesgo: no existe un riesgo previsible de pérdidas u otros daños a la seguridad de los demás.
- De procedimiento: una evaluación de impacto, basada en criterios establecidos, debe completarse y evaluarse de antemano. Los criterios deben ser transparentes y definidos por los actores pertinentes, y deben revisarse periódicamente. Este proceso debe incluir, entre otros, a las fuerzas del orden, los funcionarios judiciales, los especialistas técnicos y la sociedad civil.
- Limitado: cada instancia de hackeo informático gubernamental debe autorizarse en función de los criterios aprobados previamente y con una fecha de finalización clara. Las autorizaciones “continuas” (que se renuevan por defecto cada pocas semanas o meses) no deben utilizarse como medio para subvertir este requisito.

CC BY-NC-SA 4.0

Nunca en la historia de la humanidad ha habido tantos datos disponibles para los gobiernos y sus organismos encargados de hacer cumplir la ley: de hecho, en algunos casos, la aplicación ha fallado no por falta de datos, sino por un exceso de ellos.[19] [20]

Internet Society insta a los gobiernos a dar prioridad a otras vías para la recopilación, el análisis y el uso de información y pruebas, a fin de no socavar la seguridad de los dispositivos, el software y los servicios de Internet. Esto incluye el análisis de la riqueza de la inteligencia del código abierto, los datos accesibles en poder de los proveedores de servicios, los metadatos de comunicaciones relevantes y la recopilación de evidencia no digital, como la información de testigos y documentos.

19 https://www.theguardian.com/uk/2006/may/11/july7.uksecurity [2006]

20 https://www.techdirt.com/2013/09/10/problem-with-too-much-data-mistaking-signal-noise/ [2013]

CC BY-NC-SA 4.0