Hackeo gubernamental

¿Qué es y cuándo utilizarlo?

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 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 hackeo 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 sea necesario para fines de aplicación de la ley.

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 del gobierno plantea un riesgo de daños colaterales tanto a Internet como a sus usuarios, y como tal, solo debe considerarse como una herramienta de último recurso.

Definición de hackeo gubernamental

Definimos como "hackeo 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).

Peligros del hackeo 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

[1] Los monitores para bebés y las cámaras de seguridad bien diseñados deben enviar sus datos de forma confidencial a través de 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

comunicaciones activas, o bien dejarlos en condiciones menos seguras. Esto aumenta de manera significativa el riesgo de violaciones de seguridad futuras, pudiendo perjudicar a todos los usuarios del sistema.[4]

Los riesgos se exacerban 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. Por lo tanto, debe haber una divulgación coordinada de las vulnerabilidades de seguridad descubiertas lo antes posible para que puedan ser parchadas.[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 hackeó a la Agencia de Seguridad Nacional de los EE. UU., y expuso públicamente la vulnerabilidad de día cero EternalBlue de la Agencia[6]; la empresa de seguridad italiana, Hacking Team, fue pirateada en 2015[7]; y un conjunto de herramientas de hackeo 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 reubicado 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 portuarios.[9] Estos incidentes resaltan los peligros de acaparar vulnerabilidades de día cero, y crear y almacenar los aprovechamientos de estos.

Los equipos de hackeo 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 hackear secretamente las cuentas de WhatsApp de periodistas y activistas para vigilar sus comunicaciones.[10] [11]

Un objetivo puede convertirse en varios. Si bien, idealmente por diseño, el hackeo gubernamental pretende ser focalizado y altamente preciso, los aprovechamientos y las técnicas de hackeo, aun cuando estuvieran previstos para un solo objetivo, pueden también utilizarse contra una gran cantidad y variedad de dispositivos o software. Además, los países también pueden aprovechar las vulnerabilidades con otros fines; por ejemplo, para participar en ciberataques o guerras cibernéticas, por parte de los diferentes actores de amenazas persistentes avanzadas (APT)[12] 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.[13]

---

[4] Además, existe el riesgo de que al aprovechar las vulnerabilidades se pueda dañar la integridad de la evidencia digital.

[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://en.wikipedia.org/wiki/Vault_7

[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://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/

[12] https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html

[13] https://www.cybereason.com/blog/advanced-persistent-threat-apt

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.[14] 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 precios y la demanda que existe en los mercados negro y gris.[15] Contar con vulnerabilidades funcionales 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 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 contra actores maliciosos. Internet Society considera[16] que el cifrado debe ser la norma para el tráfico de Internet y el almacenamiento de datos.

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) e Internet.

No apoyamos el hackeo 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.

El riesgo es particularmente grave para el hackeo gubernamental que se basa en aprovechamientos de vulnerabilidades y vulnerabilidades de día cero (como se señaló anteriormente). Sin embargo, también es un riesgo incluso cuando se conocen las vulnerabilidades, pero ha habido parches mínimos en Internet (por ejemplo, debido a que el equipo es demasiado viejo, las personas no pueden permitirse dispositivos más nuevos y más seguros, o debido a procedimientos de parche inadecuados o laxos).

Una preocupación principal es que cualquier aprovechamiento de vulnerabilidades de cualquier sistema crea un peligro inherente. Incluso en un escenario perfecto donde una entidad gubernamental utiliza una vulnerabilidad con las mejores intenciones, con la autorización adecuada y con un resultado positivo, existe un alto riesgo de que el aprovechamiento de ésta no se quede dentro de los límites de ese gobierno. El sistema en su conjunto se vuelve menos seguro simplemente por aprovechar la vulnerabilidad, independientemente de la intención.

---

[14] 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

[15] Consulte por ej., https://en.wikipedia.org/wiki/Cyber-arms_industry#Notable_markets para encontrar algunos ejemplos que se nombran de esos mercados

[16] Internet Society no está sola en esta convicción. 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. Consulte https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx y http://www.oecd.org/sti/ieconomy/cryptography.htm respectivamente.

Dados los riesgos inherentes, los gobiernos no deben recopilar, 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 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. Esto debe incluir, entre otros, a las fuerzas del orden, funcionarios judiciales, técnicos especialistas y la sociedad civil. **Cada instancia** del hackeo gubernamental debe aprobarse en función de los criterios aprobados previamente.

Internet Society insta a los gobiernos dar prioridad a otras vías de recopilación de información y evidencia que no presenten un riesgo para 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.