Computación

Ciberescándalo: Google para un hackeo antiterrorista de un país aliado

La empresa detectó que un grupo "experto" de hackers usaba 11 poderosas vulnerabilidades para comprometer dispositivos iOS, Android y Windows, y corrigió los fallos. Los atacantes resultaron ser agentes de inteligencia occidentales cuya misión quedó paralizada, lo que podría ponerles en peligro

por Patrick Howell O'Neill | traducido por Ana Milutinovic

12 Abril, 2021

- **Los equipos de seguridad de Google expusieron públicamente una operación de hackeo de nueve meses**
- **Lo que no reveló: detuvo una operación antiterrorista activa que estaba llevando a cabo el gobierno de un país occidental**
- **La decisión ha levantado alarmas dentro de Google y en otros lugares.**

Google realiza algunas de las operaciones de ciberseguridad más importantes del planeta: su equipo Project Zero, por ejemplo, se dedica a destapar grandes vulnerabilidades de seguridad no identificadas, mientras que su Threat Analysis Group o Grupo de Análisis de Amenazas contrarresta directamente ciberataques respaldados por los gobiernos, incluidos los de Corea del Norte, China y Rusia. Ahora resulta que esos dos equipos han capturado un pez inesperadamente gordo: **un grupo "experto" de hackers que usaba 11 poderosas vulnerabilidades** para comprometer los dispositivos que ejecutan iOS, Android y Windows.

Pero *MIT Technology Review* ha podido saber que **los hackers en cuestión eran en realidad agentes gubernamentales** de un país occidental que trabajaban activamente en una operación antiterrorista. La decisión de la compañía de detener y hacer público el ataque provocó una división interna en Google y generó interrogantes dentro de las comunidades de inteligencia de Estados Unidos y sus aliados.

Dos recientes publicaciones de blog de Google detallan el conjunto de vulnerabilidades de día cero que los hackers usaron durante nueve meses. Los *exploits*, que se remontan a principios de 2020 y se basan en técnicas nunca vistas, eran **ataques tipo "pozo" que, mediante páginas web infectadas introducían malware** a los visitantes. Llamaron la atención de los expertos en ciberseguridad de Google por su escala, sofisticación y velocidad.

Sin embargo, la publicación de **Google omitió flagrantemente algunos detalles clave**, incluido quién fue el responsable del hackeo y a quién estaba atacando, así como importante información técnica sobre el malware y los dominios utilizados en la operación. Normalmente, al menos parte de esa información se haría pública de alguna manera, algo que llevó a un experto en seguridad a criticar el informe y calificarlo de "agujero negro".

"Diferentes cuestiones éticas"

Las empresas de seguridad detienen regularmente los *exploits* que están siendo utilizados por algunos gobiernos de países aliados, pero **tales acciones rara vez se hacen públicas**. En respuesta a este incidente, algunos empleados de Google argumentan que las misiones antiterroristas no deberían divulgarse públicamente; otros creen que la compañía estaba completamente en su derecho y que la publicación protege a los usuarios y hace que internet sea más seguro.

En un comunicado, un portavoz de Google afirma: "Project Zero se dedica a encontrar y corregir vulnerabilidades de día cero y a publicar investigaciones técnicas diseñadas para avanzar en la comprensión de las nuevas vulnerabilidades de seguridad y técnicas de explotación en toda la comunidad de investigación. **Creemos que compartir esta investigación conduce a mejores estrategias defensivas** y aumenta la seguridad para todos. No realizamos atribuciones como parte de esta investigación".

Es cierto que Project Zero no atribuye formalmente los hackeos a grupos específicos. Pero Threat Analysis Group, que también participó en este proyecto, sí. Google omitió muchos más detalles además del nombre del gobierno detrás de los ataques y, a través de esa información, **los equipos sabían internamente quiénes eran los hackers y los objetivos**. No se sabe si Google notificó con antelación a las autoridades del gobierno en cuestión que harían público el método de ataque y que lo detendrían.

Pero las operaciones occidentales son reconocibles, afirma un alto exfuncionario de inteligencia estadounidense. Dado que no está autorizado a comentar sobre las operaciones, habló bajo la condición de anonimato: "**Hay ciertos sellos distintivos en las operaciones occidentales** que no están presentes en otras entidades... se pueden ver traducidos en el código. Y aquí es donde creo que entra en juego una de las dimensiones éticas clave. La forma en la que se trata la actividad de inteligencia o la policial realizada bajo la supervisión democrática dentro de un gobierno representativo legítimamente elegido es muy diferente de la de un régimen autoritario. La supervisión está incluida en las operaciones occidentales a nivel técnico, comercial y de procedimientos".

> ***"Hay ciertos sellos distintivos en las operaciones occidentales que no están presentes en otras entidades... se pueden ver traducidos en el código".***

Google descubrió que el grupo hacker explotó 11 vulnerabilidades de día cero en solo nueve meses, **una gran cantidad de *exploits* en un período corto**. El software que había sido atacado incluyó el navegador Safari en iPhones, pero también muchos productos de Google, como el navegador Chrome en los teléfonos Android y los ordenadores con Windows.

Pero la conclusión dentro de Google fue que **quién hackea y por qué no son cuestiones tan importantes** como las vulnerabilidades de seguridad en sí mismas. A principios de este año, la investigadora de seguridad de Project Zero Maddie Stone argumentó que a los hackers les resultaba demasiado fácil encontrar y usar las poderosas vulnerabilidades de día cero y que su equipo se enfrentaba a una batalla cuesta arriba para detectar su uso.

En vez de centrarse en quién estaba detrás y quién era el objetivo de una operación específica, Google decidió actuar de forma más amplia para todos. La justificación consistía en que incluso si un gobierno de algún país occidental fuera el que explotara esas vulnerabilidades en la actualidad, con el tiempo serán utilizadas por otros, por lo que **la opción correcta es siempre corregir la vulnerabilidad al momento**.

"No es su trabajo averiguarlo"

No es la primera vez que un equipo de ciberseguridad occidental captura a hackers de países aliados. Pero, **algunas empresas tienen norma de guardar silencio** y no exponer públicamente tales operaciones de hackeo si tanto el equipo de seguridad como los hackers son considerados amistosos, por ejemplo, si son miembros de la alianza de inteligencia "Five Eyes", compuesta por Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda. Varios miembros de los equipos de seguridad de Google son veteranos de las agencias de inteligencia occidentales y algunos han realizado campañas de hackeo para estos gobiernos.

En algunos casos, las empresas de seguridad quitarán el llamado malware "amistoso", pero evitarán hacerlo público. El antiguo funcionario del Pentágono Sasha Romanosky, quien recientemente publicó un estudio de las investigaciones de ciberseguridad del sector privado, afirma: "En general, **no atribuyen a nadie las operaciones que ocurren en Estados Unidos**. Nos afirmaron específicamente que se apartaban. No es su trabajo averiguarlo; se hacen a un lado por cortesía. Eso no es nada inesperado".

Si bien lo ocurrido en Google es de alguna manera inusual, se han producido casos similares en el pasado. La empresa rusa de ciberseguridad Kaspersky fue muy criticada en 2018 cuando **expuso una ciberoperación antiterrorista dirigida por Estados Unidos contra los miembros de Al Qaeda e ISIS** en el Medio Oriente. Kaspersky, al igual que Google, no atribuyó a nadie explícitamente la amenaza, pero sí que la expuso y la inutilizó, según las autoridades estadounidenses, lo que provocó que los operativos perdieran el acceso a un valioso programa de vigilancia e incluso pusieran en riesgo la vida de los soldados sobre el terreno.

Kaspersky ya recibía fuertes críticas por su relación con el Gobierno ruso en ese momento, y la compañía finalmente fue excluida de los sistemas gubernamentales de EE. UU. **Kaspersky siempre ha negado tener una relación especial con el Kremlin.**

Google también ha estado en situaciones parecidas. En 2019, publicó una investigación sobre lo que pudo haber sido un grupo de hackers estadounidenses, aunque nunca se hizo una atribución específica. Pero esa investigación fue sobre una operación pasada. Las recientes publicaciones de Google, en cambio, **pusieron el foco en una operación de ciberespionaje activa.**

¿A quién se protege de verdad?

Las alarmas generadas tanto dentro del Gobierno estadounidense como en Google demuestran que **la empresa se encuentra en una posición difícil**.

Los equipos de seguridad de Google tienen una responsabilidad con sus clientes y se espera que hagan todo lo posible para proteger los productos y, por lo tanto, a los usuarios que están bajo ataque. En este incidente, se ve que las técnicas utilizadas afectaron no solo a los productos de Google como Chrome y Android, **sino también a los iPhones.**

Aunque cada equipos establece sus propios límites, **Project Zero destaca por abordar las vulnerabilidades críticas en todo internet**, no solo las que se encuentran en los productos de Google. Cuando se publicó la última investigación, una de los miembros más respetados del equipo de seguridad Maddie Stone afirmó en un tuit: "Cada paso que damos para dificultar el día 0, nos hace más seguros a todos".

Pero, aunque es importante proteger a los clientes de los ataques, hay quien argumenta que **las operaciones antiterroristas son diferentes, con posibles consecuencias de vida o muerte** que van más allá de la seguridad diaria de internet.

Cuando los hackers respaldados por gobiernos de países occidentales encuentran defectos de ciberseguridad, existen métodos establecidos para calcular los posibles costes y beneficios de revelar ese error de seguridad a la empresa afectada. En Estados Unidos eso se denomina **"proceso de valoración de vulnerabilidades".**

A los críticos les preocupa que la inteligencia estadounidense acumule una gran cantidad de *exploits*, pero su sistema es más formal, transparente y expansivo que el que se lleva a cabo en casi todos los demás países del mundo, incluidos los aliados occidentales. El proceso está pensado para permitir que las autoridades **valoren las ventajas de mantener en secreto los defectos** para usarlos con fines de inteligencia frente a los beneficios más amplios de informar a una empresa de tecnología sobre una vulnerabilidad para que la solucione.

> ***"El nivel de supervisión incluso en las democracias occidentales sobre lo que están haciendo realmente sus agencias de seguridad nacional es, en muchos casos, bastante menor que el que tenemos en Estados Unidos".***

El año pasado, la Agencia de Seguridad Nacional (NSA) de EE. UU. tomó la inusual decisión de atribuirse el mérito de haber revelado un viejo fallo en Microsoft Windows. Ese tipo de comunicación del Gobierno a la industria **normalmente se mantiene en el anonimato y, a menudo, en secreto**.

Pero, aunque el proceso de revelación del sistema de inteligencia estadounidense puede parecer opaco, **los procesos en otros países occidentales suelen ser más reducidos**, más secretos o simplemente informales y, por lo tanto, fáciles de omitir.

El antiguo coordinador de Ciberseguridad de la Casa Blanca para la administración de Obama, Michael Daniel, afirma: "Incluso en las democracias occidentales, el nivel de supervisión sobre lo que están haciendo sus agencias de seguridad nacional es, **en muchos casos, bastante menor que el que de Estados Unidos.** La supervisión parlamentaria es mucho menor. Estos países no cuentan con los fuertes procesos interinstitucionales que tiene EE. UU. Normalmente no soy de los que presumen de Estados Unidos, porque tenemos muchos problemas, pero esta es un área en la que tenemos procesos sólidos que otras democracias occidentales simplemente no tienen".

El hecho de que el grupo de hackers afectado por la investigación de Google tuviera y utilizara tantas vulnerabilidades de día cero con tanta rapidez podría indicar un desequilibrio problemático. Pero a algunos expertos les preocupa que las ciberoperaciones de contraterrorismo activas **se detengan en momentos potencialmente decisivos** sin la posibilidad de reanudarlas rápidamente.

"No todos los aliados de Estados Unidos tienen la capacidad de reiniciar operaciones completas tan rápido como otros", dijo el antiguo alto funcionario de inteligencia de Estados Unidos. La preocupación por perder repentinamente el acceso a una posibilidad de *exploit* o ser detectado por un objetivo es particularmente alta para las misiones antiterroristas, especialmente durante los "períodos de gran exposición" cuando se está llevando a cabo mucha actividad, explicó. Es probable que **la capacidad de Google para detener una operación de este tipo dé lugar a más conflictos**.

Y concluye: "Esto todavía no se ha abordado bien. La gente se está dando cuenta poco a poco de la posibilidad de que **alguien como Google pueda destruir tanta capacidad tan rápidamente**".

Su nombre

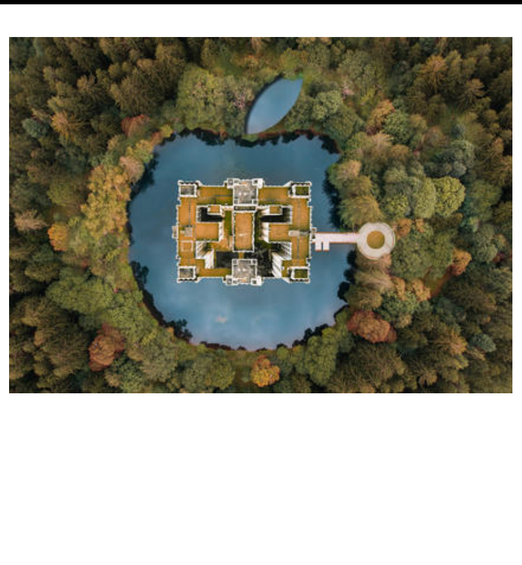
Comment *

GUARDAR

Computación

Las máquinas cada vez más potentes están acelerando los avances científicos, los negocios y la vida.

01

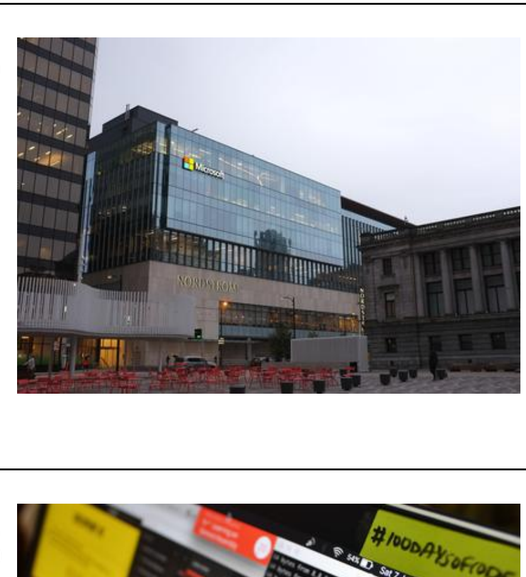


El dilema de seguridad de Apple: el sistema protege a los hackers que logran entrar

El diseño ultrabloqueado del iPhone evita la mayor parte de los ataques, pero los más sofisticados siempre encuentran una entrada. Una vez dentro, las propias defensas del sistema los esconden. A pesar de ello, parece el mejor enfoque y el resto del sector empieza a moverse en la misma dirección

Por Patrick Howell O'Neill

02



Microsoft alerta de que el ciberataque a Exchange es cada vez mayor

Cuatro grupos de hackers carroñeros se han unido a la sofisticada campaña de ataque de Hafnium, lo que podría aumentar el número de víctimas a cientos de miles

Por Patrick Howell O'Neill

03

Google alerta: lanzar parches de software da vía libre a los hackers

El gigante advierte que, en lugar de solucionar el problema de raíz, este enfoque superficial hace que explotar vulnerabilidades de día cero resulte muy fácil, lo que permite a los ciberdelincuentes hacerlo una y otra vez

Por Patrick Howell O'Neill

Más información sobre Computación

Síguenos