Los ciberataques (conocidos) más importantes

Lino González Veiguela

Las filtraciones de Edward Snowden sobre el funcionamiento y los programas secretos de la Agencia de Seguridad Nacional estadounidense (la NSA) han abierto un debate, que muchos creían necesario, sobre los límites que han de tener las agencias de espionaje a la hora de espiar las comunicaciones privadas de los ciudadanos en Internet. Las filtraciones también han permitido saber algo más sobre ataques de la NSA contra empresas, organizaciones de otros países y a los aliados como la UE, México, Japón o India. Una buena parte de los ciberataques registrados en los últimos años han sido obra de piratas informáticos con ánimo de lucro, afán de protagonismo o con motivaciones políticas. Pero otros muchos han sido obra de los servicios de seguridad nacionales. He aquí una lista con algunos de los ciberataques entre los Estados más relevantes de los últimos años.

1. SNOWDENGATE

Año: 2013 y años anteriores

Supuestos agresores: de momento, se habla de China, de las embajadas de treinta y ocho países en suelo estadounidense, incluidas las delegaciones de la Unión Europea y de las comunicaciones de la población de Estados Unidos

Agredidos: China, Estados Unidos, UE, Japón, Corea del Sur, India, Naciones Unidas y Turquía

Contexto: el ex analista de la CIA y de la NSA Edward Snowden podría tener en su poder miles de documentos clasificados sobre diversos programas de la NSA. El escándalo ha surgido por las revelaciones de Snowden en las que acusa a la NSA de espiar indiscriminadamente a los propios ciudadanos estadounidenses mediante el programa PRISMA. Snowden también ha revelado –pocos lo dudaban- que los servicios de espionaje estadounidense y británico (este último, a través del Centro de Escuchas y Decodificación británico, el GCHQ) colaboran estrechamente desde hace años en varios proyectos de espionaje a través de la Red. A nivel diplomático, causará ciertos quebraderos de cabeza a los funcionarios del Foreign Office tener que explicar a sus homólogos del G-20 si expiaron o no las comunicaciones de las delegaciones que participaron en la reunión del grupo celebrada en Londres en 2009. Los esfuerzos diplomáticos estadounidenses tendrán que ser aún más intensos si quieren contentar con sus explicaciones a los casi cuarenta países –muchos de ellos supuestos aliados- cuyas delegaciones en suelo estadounidense habrían sido espiadas por la NSA. Entre ellas, se encontrarían las de la Unión Europea. Snowden, que estaría negociando la concesión de asilo con varios países, ha acusado a Barack Obama de presionar a muchos gobiernos para que se le deniegue el asilo. Si, finalmente, fuese extraditado a EE UU, se enfrentaría un juicio parecido al que está teniendo el soldado Bradley Manning por sus filtraciones a Wikileaks, en el que se podría pedir su condena a muerte por traición y en el que, difícilmente, se libraría de una larga condena. Cabe esperar que las filtraciones de Snowden destapen más ciberataques en las próximas semanas, delimitando con más precisión algunos de los escenarios del campo de batalla cibernético de una guerra entre agencias de seguridad que, o eso parece al menos, no ha hecho aún más que empezar.

2. DARKSEOUL

Año: 2011 y 2013

Supuestos agresores: Corea del Norte

Agredidos: Corea del Sur

Objetivo: canales de televisión en Corea del Sur y sistemas informáticos de bancos

Contexto: el pasado marzo, los sistemas informáticos de medios de comunicación surcoreanos sufrieron un importante ciberataque que inutilizó numerosos ordenadores. Algunas fuentes hablan de unos 50.000 ordenadores afectados. En algunas pantallas aparecieron calaveras tras producirse el fallo del sistema. El virus, según las autoridades surcoreanas, no comprometió el funcionamiento de ningún sistema informático estatal. El objetivo esta vez eran los bancos surcoreanos, pero no es el primer ataque similar que sufre Corea del Sur. En 2011, otro asalto paralizó gran parte de las operaciones de uno de los principales bancos del país, el Nonghyup. En 2009, un ataque tuvo como objetivos agencias gubernamentales. En aquella ocasión, el Gobierno de Seúl acusó de ser el responsable al Laboratorio 110, una división de informáticos del Ejército norcoreano encargada, entre otros asuntos, de llevar a cabo ciberataques. Corea del Sur ha acusado, repetidamente, a las autoridades del vecino del Norte de ser las responsables de los ataques. Algo que desde Pyongyang niegan.

Días antes del último asalto en marzo 2013, Corea del Norte había denunciado un ciberataque contra varios de los sistemas informáticos del país, incluidas páginas oficiales. Pyonyang acusó a Estados Unidos de haber orquestado esas operaciones aprovechando que el Ejército estadounidense se encontraba realizando unas maniobras conjuntas con los militares surcoreanos.

3. FLAME

Año: 2012

Supuestos agresores: desconocido

Agredidos: Irán (el país más afectado), Palestina (Cisjordania), Arabia Saudí, Sudán, Líbano y Egipto

Objetivos: sin objetivos concretos o conocidos. Apunta a ser más un ataque destinado a recopilar información de inteligencia de todo tipo, desde correos electrónicos hasta documentos secretos.

Contexto: según Yevgueni Kasperski, el director de la compañía de seguridad que lleva su apellido, si a su equipo de informáticos les llevó seis meses analizar en profundidad el complejo virus Stuxnet, las primeras previsiones cuando se descubrió Flame en mayo de 2012 parecían indicar que era un virus veinte veces más complejo. También afirmó que dicha complejidad, sumada a la conflictiva zona geográfica donde habían tenido lugar los ataques, hacía pensar en que detrás de Flame se encontraba algún Estado. Muchos indicios –incluidas algunas supuestas fuentes de la inteligencia israelí- señalan a Israel como el patrocinador. Aunque, el hecho de que algunos sistemas informáticos israelíes resultasen también afectados pone en cuestión la autoría de los servicios secretos del Estado hebreo. Aunque no se descarta. La amplitud de su espectro, por lo que respecta a sus objetivos, ha motivado que muchos señalen a Flame como el precursor de un nueva modalidad de ciberespionaje. El peso del contenido de este virus, unos 20MB, fue altísimo, comparado con los *gusanos informáticos* anteriores como Duqu, 300KB, o Stuxnet, unos 500KB.

4. SHAMOON

Año: 2012

Supuestos agresores: Irán

Agredidos: Arabia Saudí y Qatar

Objetivo: los sistemas informáticos de la compañía saudí de petróleo Aramco y de la segunda empresa gasística mundial, la catarí RasGAs

Contexto: los ataques contra Aramco y RasGas se produjeron con pocos días de diferencia en agosto de 2012. Una de las características principales del virus Shamoon es que, además de robar información de los sistemas informáticos, borra ingentes cantidades de datos de los sistemas infectados. Algunas fuentes señalaron que hasta treinta mil ordenadores de Aramco pudieron sufrir los efectos de Shamoon: la pérdida podría ascender hasta los tres cuartos de todos los datos almacenados por la empresa estatal saudí. Al parecer, la parte del virus destinada a borrar archivos compartía el código con el virus Flame, que unos meses antes había atacado el sistema informático de la red energética iraní. Una de las particularidades de Shamoon es que en las pantallas de los ordenadores infectados generaba la imagen de una bandera de EE UU en llamas. Como es sabido, tanto Arabia Saudí como Qatar, además de potencias regionales rivales de Irán, son firmes aliados de Estados Unidos. El Ejército estadounidense cuenta incluso con una base militar a escasos kilómetros de Doha. Ni Aramco ni RasGas

se han pronunciado de forma oficial sobre los ataques informáticos sufridos.

5. STUXNET

Año: 2008, 2009 y 2010

Supuestos agresores: Estados Unidos e Israel

Agredidos: Irán

Objetivo: instalaciones nucleares iraníes

Contexto: mientras que fuentes iraníes han minimizado los daños causados en sus sistemas nucleares por el *gusano informático* Stuxnet, algunos analistas afirman que podría haber retrasado de forma notable el programa nuclear iraní, afectando seriamente a la principal planta nuclear iraní llamada Natanz. Ni las autoridades estadounidenses ni las israelíes han confirmado estar detrás del ataque. Stuxnet estaba diseñado para afectar en especial a los sistemas con software SCADA (Supervisión, Control y Adquisición de Datos), un tipo de

sistema informático que permite gestionar sistemas industriales. A finales de 2012 se supo que Stuxnet podría haber infectado también los sistemas de las empresas occidentales como Chevron. Algo que confirmaría que los virus como Stuxnet no siempre pueden ser controlados una vez que se deciden lanzar al campo de batalla cibernético. El ataque, cuyo nombre en clave fue Juegos Olímpicos, habría motivado que Irán reforzase su seguridad informática y crease grupos operativos que le permitiesen responder a los ataques cibernéticos sufridos.

A finales de 2008, Alí Ashtari, vendedor de componentes electrónicos, fue ahorcado en el patio de la prisión de Evin –la principal cárcel de Teherán-: se le había condenado a muerte acusado de facilitar a Israel información sobre el programa nuclear iraní, entre la que estarían incluidos posibles objetivos para el ataque de Stuxnet. El Mossad negó cualquier relación con Ashtari.

6. OPERACIÓN AURORA

Año: 2009

Supuestos agresores: China

Agredidos: Estados Unidos

Objetivos: los sistemas informáticos de hasta 34 compañías estadounidenses como Google, Yahoo, Symantec, Adobe, Northrop Grumman y Dow Chemicanl, entre otras.

Contexto: a principios de 2010, Google denunció que había detectado un ciberataque procedente de China que habría vulnerado el muro de seguridad de la compañía y tenido acceso a sus servidores. En un primer momento, se denunció que los atacantes querían sobre todo tener acceso a las cuentas del correo electrónico (gmail) de destacados opositores chinos, como Ai Weiwei. Google no facilitó la investigación puesta en marcha por el FBI en su sede de Mountain View y comenzó una disputa legal con la agencia de seguridad estadounidense para impedir que sus agentes pudiesen acceder a información sensible de la compañía relacionada con su funcionamiento técnico. Hace unos meses, según una noticia publicada en el periódico *Washington Post*, se supo que los ciberataques contra Google y otras compañías estadounidenses, además de tener una vertiente de espionaje industrial y anti oposición, podrían haber tenido como principal finalidad el contraespionaje. Según estas fuentes, piratas informáticos al servicio de agencias estatales chinas habrían lanzado la Operación Aurora para controlar la información en poder de agencias estadounidenses sobre agentes de inteligencia chinos operando dentro del territorio de Estados Unidos. El Ejército chino contaría con una

unidad especializada en ciberataques denominada la Unidad 61398, cuya sede estaría en un gris edificio de doce plantas ubicado en el barrio de Pudong, en Shanghai.

Unos años antes de que se produjera este ataque, otro asalto proveniente de China consiguió vulnerar las defensas del sistema informático militar estadounidense manteniéndose activo durante casi dos años, entre 2003 y 2005. Aquel ataque, conocido como Titan Rain, se infiltró principalmente en contratistas privados de defensa, aunque también penetró en los sistemas de la NASA.

7. OSETIO


YOU
ARE THE NEXT!!!

Año: 2008

Supuestos agresores: piratas informáticos trabajando desde Rusia. Las autoridades rusas han negado las acusaciones que relacionaban a sus servicios secretos con el ataque

Agredidos: Georgia y Azerbaiyán

Objetivos: las webs de los medios de comunicación y de las instituciones de Georgia y Azerbaiyán

Contexto: en agosto del 2008, pocos días antes del inicio de la breve guerra entre Georgia y Rusia por el control de Osetia del Sur, medios de comunicación y webs de instituciones georgianas y azerís comenzaron a sufrir ataques que inutilizaron su funcionamiento. En la página del Ministerio de Asuntos Exteriores georgiano apareció la imagen del presidente, Mikheil Saakashvili, caracterizado como Hitler antes de bloquearse su funcionamiento. Desde el Kremlin se negó que los servicios secretos rusos estuviesen implicados en dichos ataques y se acusó a piratas informáticos independientes. Los analistas no se ponen de acuerdo sobre la implicación oficial de Rusia en dichos ciberataques. No se descarta que el FSB (servicio de inteligencia ruso) coordinase los ataques llevados a cabo por piratas informáticos no pertenecientes al propio FSB.

Un año antes, en la primavera de 2007, un ataque similar en cuanto a objetivos, también procedente de Rusia, afectó a los sistemas informáticos de las empresas y los organismos estonios. El Kremlin negó también toda implicación. El asalto, conocido como Black Hat, se produjo en un momento de tensión política entre Moscú y Tallín por algunas políticas del Gobierno de Estonia contrarias, según los rusos, a los derechos de los estonios de origen ruso.

8. OPERACIÓN HUERTO

Año: 2007

Supuestos agresores: Israel

Agredidos: Siria

Objetivos: defensas antiaéreas de Siria

Contexto: en septiembre de 2007, la aviación israelí llevó a cabo un ataque contra supuestas instalaciones nucleares sirias. Según Israel, Siria estaba desarrollando un programa nuclear

con la ayuda de expertos y tecnología procedentes de Corea del Norte. La operación Huerto habría comenzado a gestarse a finales de 2006, cuando agentes del Mossad accedieron al ordenador portátil que un alto oficial sirio tenía en su habitación de un lujoso hotel londinense. Para hacerse con esa información usaron viejos métodos: allanamiento de morada. Aprovecharon la operación para inocular en el portátil un virus troyano con la intención de que les continuara suministrando información. El material contenido en el ordenador del oficial sirio, siempre según fuentes israelíes, contenía indicios de un programa nuclear secreto. Este *descubrimiento* se vería reforzado meses más tarde por el testimonio de un alto oficial iraní desertor que pidió protección a la CIA –a través de su base en Estambul- para él y su familia a cambio de información. La reciente victoria de Ahmadineyah había generado una serie de purgas dentro del régimen. El oficial iraní habría suministrado tanto información sobre el programa nuclear iraní como sobre el sirio que, supuestamente, Irán estaba ayudando a financiar. Una vez que Tel Aviv dio el visto bueno a la operación militar contra las instalaciones sirias que albergaban las supuestas instalaciones nucleares faltaba planificar cómo se superarían las defensas antiaéreas sirias. Y en esa parte de la coreografía de guerra es donde habría entrado en juego el componente de ciberguerra de la operación: un programa informático –desarrollado por Estados Unidos- denominado Suter, que permite interceptar las comunicaciones enemigas, infiltrarse en su sistema y llegar a bloquear dichas comunicaciones, por ejemplo las señales electrónicas que forman un sistema de radares antiaéreos. De confirmarse todos estos extremos, la operación Huerto habría supuesto una combinación entre armas de guerra tradicionales y armas de guerra cibernéticas que ofrece sinergias aún poco exploradas

9. MOONLIGHT MAZE

Año: entre 1998 y 2000

Supuestos agresores: piratas informáticos operando desde Rusia

Agredidos: Estados Unidos

Objetivos: sistemas informáticos del Pentágono, la NASA, el Departamento de Energía estadounidense y, también, universidades privadas de EE UU

Contexto: los intrusos en los sistemas informáticos tuvieron acceso a miles de documentos clasificados, muchos de ellos relacionados con información del Ejército: mapas de instalaciones militares, por ejemplo, o planes de despliegue de tropas. Las investigaciones, aún en curso,

han establecido que el ataque comenzó en la primavera de 1998 y duró casi dos años. Se rastreó la procedencia del sofisticado asalto hasta conexiones ubicadas en Rusia. Las autoridades rusas negaron estar implicadas. No se ha podido probar quiénes fueron los autores materiales ni quiénes los eventuales patrocinadores del ataque que, se sospecha, pudieron haber sido agencias de espionaje estatales.

10. LOGIC BOMB

Año: 1982

Supuestos agresores: Estados Unidos

Agredido: Rusia

Objetivos: gaseoducto soviético en Siberia

Contexto: en junio de 1982 los satélites estadounidenses que orbitaban sobre la Unión Soviética fotografiaron la explosión no nuclear más grande registrada hasta la fecha. No fue

hasta más de veinte años más tarde que se supo que aquella explosión -que no causó víctimas- había sido el resultado de una operación de la CIA. La Agencia de Inteligencia estadounidense había conseguido una información valiosa: el KGB estaba tratando de robar en Occidente nuevos programas informáticos que permitiesen mejorar las prestaciones de su sistema de producción y transporte de recursos energéticos. El gas y el petróleo constituían los activos más económicos de la economía soviética, lastrada desde 1980 por el excesivo gasto militar que representaba la invasión de Afganistán. A través de un doble agente soviético, la CIA consiguió hacer llegar al KGB un software defectuoso para controlar el transporte de gas: afectaba al control de la presión del gas en los gaseoductos y sería el culpable de la gran explosión. El agente del KGB implicado en la operación, el coronel Vladimir Vetrov, fue descubierto y ejecutado en 1983.

- Consulte todas las Listas de esglobal

Fecha de creación
2 julio, 2013