

Rincón de Internet

Se ha cumplido más de un año de los trágicos sucesos del 11 de Septiembre. Un tiempo que ha servido para reflexionar y debatir en profundidad sobre muchos aspectos de la vida y la sociedad. El atentado contra las torres gemelas de Nueva York también nos sorprendió al mostrarnos, de la forma más cruel, una nueva cara del terrorismo desconocida hasta entonces. Pero, por otra parte los métodos utilizados fueron los, por desgracia, de sobra conocidos. Sin embargo, ¿podríamos llegar a pensar que una tecnología como Internet pueda representar una amenaza en el futuro?

El terrorista del mañana puede ser capaz de hacer más con un teclado que con una bomba

Informe "Computers at risk" del National Research Council (1991)

Ciberterrorismo. La amenaza fantasma

Incidentes en el ciberespacio que han seguido al conflicto entre Israel y Palestina, Cachemira o Kosovo, y de forma más reciente a los ataques del 11S son tan solo algunos de los ejemplos que muestran la creciente utilización de Internet en un nuevo "frente virtual". Una realidad que no podemos eludir. Asomémonos por un momento al otro lado, el lado

oscuro de Internet en sus múltiples facetas.

Internet como medio de apoyo al terrorismo

Internet es utilizado cada vez más como un medio de apoyo al terrorismo. Así, muchos de los terroristas últimamente utilizan Internet como medio de formación en fabricación de bombas, tácticas de guerrilla urba-

na o utilización de armamento.

Pero no es esta la única forma en que las organizaciones terroristas emplean Internet. Las sedes de Al-Qaeda en Afganistán contaban con ordenadores y equipos de comunicaciones desde 1996 y en los atentados del 11S así como en otras muchas acciones. Ya sea mediante el uso del correo electrónico, los grupos de noticias, chats o las páginas web, Internet es utilizada como un medio de coordinación entre terroristas en diversas de sus actividades. Mapas, fotos o detalles de la preparación de los ataques son transmitidos en formatos encriptados. De la misma forma, Internet sirvió como medio de apoyo logístico en la diversificación de la circulación y protección de las finanzas de Al-Qaeda.

Otra de las formas en que Internet es utilizada por los terroristas es como apoyo publicitario para la difusión de su causa, con lo que se logra obtener mediante costes relativamente bajos "campañas" de propaganda a gran escala internacional.

Ciberataques

Pero un grado más allá de lo que podría ser considerado como un mero medio de apoyo, los ciberataques tienen como objetivo atacar la propia infraestructura de Internet. De esta forma, el mecanismo más frecuente consiste en saturar los servidores de la Red enviándoles muchas más peticiones de servicio de las que son capaces de atender. Son los ataques denominados de "denegación de servicio". Instituciones oficiales, financieras, ISPs e incluso ser-

Direcciones de interés

Dorothy Denning <http://www.cs.georgetown.edu/~denning>

Law Enforcement Online (LEO) <http://www.fbi.gov/hq/cjsid/leo.htm>

Ley Patriótica <http://www.epic.org/privacy/terrorism/hr3162.html>

HTCIA <http://www.htcia2002.org>

The Center for the Study of Technology and Society <http://www.tecsoc.org>

The Terrorism Research Center <http://www.terrorism.com>

vidores de e-commerce son, frecuentemente, los blancos preferidos en este tipo de ataques. En algunas ocasiones los autores han habilitado y publicitado entre sus seguidores una página web de forma que con un simple click de ratón pudieran contribuir a saturar un determinado servidor. El pasado mes de octubre se produjo un ataque que las autoridades estadounidenses calificaron como "el mayor y más sofisticado en la historia de la Red" que afectó a 9 de los 13 grandes servidores raíz de la Red. Sin embargo, en este caso el propio diseño en origen de Internet en forma distribuida para evitar este tipo de situaciones, fue el que actuó como su gran defensa. Estos ataques, además de ocasionar pérdidas millonarias a las compañías de que son víctima, contribuyen a generar desconfianza en usuarios y empresas hacia Internet y el comercio electrónico. Otro de los ciberataques más empleado y vinculado desde sus orígenes al terrorismo consiste en la difusión de virus de carácter masivo. Los "gusanos", permiten desde un cliente realizar un ataque que pueda llegar a desembocar una auténtica reacción en cadena. Así el "gusano" se va propagando por múltiples servidores en los que va instalando su software de ataque. De esta forma, posteriormente se puede coordinar una determinada acción ofensiva. Los ya tristemente celebres "gusanos"

"Nimda" y "Código Rojo" (un millón de servidores afectados y pérdidas por valor de 2.6 billones de dólares) son tan solo dos entre una larga lista de ejemplos.

Completan el catálogo de ciberataques las entradas sin autorización en los sistemas, el robo de datos, comercialización de secretos, actividades de vandalismo en las páginas web, sabotaje de sistemas o realización de transacciones comerciales fraudulentas.

Sin embargo las motivaciones de los ciberataques en general, y en particular en los casos en que se han producido los daños más costosos, han obedecido a otras motivaciones no directamente vinculadas al terrorismo como venganzas, retos, exaltaciones del ego, acciones de protesta y otras tantas.

Ciberterrorismo

Hasta aquí hemos visto algunos de los efectos de los ciberataques. Sin embargo, y aunque en ocasiones este tipo de acciones sean protagonizadas por grupos terroristas, en un principio no podríamos llegar a calificar este tipo de actos como terroristas.

Pero ¿qué sería entonces ciberterrorismo?, ¿hay motivos para estar preocupados?. ¿Se puede llegar a ocasionar con un teclado y un ratón tanto daño como con una bomba?. La doctora Dorothy Denning, profesora de la Universidad de Georgetown es una de las figuras que más ha estudiado este fenómeno y define el ciberterrorismo como el ataque o amenaza de ataque mediante medios informáticos con el objetivo de intimidar o coaccionar a los gobiernos por

motivos políticos, religiosos o ideológicos. El ataque debe de ser lo suficientemente destructivo como para generar un temor comparable al de los actos físicos de terrorismo. Una sociedad en la que las telecomunicaciones, la energía, la banca, el comercio, la defensa y el transporte cada vez son más dependientes del medio digital, la amenaza parece estar presente y se puede pensar en numerosos escenarios en los que se logre la desestabilización y pérdida de confianza en el sistema. Sin embargo, y partiendo de la premisa de que teóricamente todo es posible, el CSTIW (Center for the Study of Terrorism and Irregular Warfare) de EE.UU. concluyó en un informe a finales del 2000 que aunque es una posibilidad real, el grado de complejidad de los sistemas hace que el ciberterrorismo presente una serie de inconvenientes para los terroristas. Así, hoy en día, realizar un determinado tipo de daño puede ser más difícil por medios digitales que físicos. Lo que no quita que para las generaciones venideras, más afines a la tecnología y en un mundo cada vez más interconectado (incluyendo los automóviles, electrodomésticos y todo tipo de dispositivos en red) sea una posibilidad cada vez más a tener en cuenta.

Antiterrorismo

Y después de ver este panorama, ¿qué se ha hecho o qué queda por hacer en materia de antiterrorismo?

Poco después de los atentados del 11S, el Congreso de los Estados Unidos aprobó la llamada "Ley Patriótica". Su fin era poder monitorizar comunicaciones

de cualquier tipo hipotéticamente vinculadas a acciones terroristas y concedía nuevos poderes a la policía fomentando la cooperación entre el gobierno estadounidense, las empresas telefónicas y los proveedores de acceso a Internet. Como en otras ocasiones esta ley ha desatado la polémica reavivando el debate entre privacidad vs seguridad. También en Noviembre del 2001, más de 40 países a instancias del Consejo de Europa y entre los que se encontraban la casi totalidad de los miembros de la UE, Estados Unidos, Sudáfrica y una decena de países no comunitarios firmaron una convención sobre la lucha contra el cibercrimen.

Esto son algunos ejemplos en el plano legislativo y oficial, pero por otra parte, y de la misma forma que los terroristas encuentran en Internet una herramienta para lograr la consecución de sus objetivos, también algunos grupos, y mediante los mismos mecanismos descritos previamente, utilizan Internet para atacar a las organizaciones terroristas.

Sin embargo, a día de hoy, y como por desgracia comprobamos día a día, parece que los medios físicos representan una amenaza bastante más real que los digitales. Aunque los estados no deben bajar al guardia, pues de la misma forma que los atentados del 11S nos cogieron por sorpresa, la próxima amenaza quizás podría venir a través de Internet.



Juan José Sánchez Aguila-Collantes

• Ingeniero de telecomunicación por la UPM
• Key Account Manager. Samsung Electronics

• Juan J. Sánchez Aguila-Collantes
jjaguila@samsung.co.kr

