



Los ataques cibernéticos

En un mundo globalizado e interconectado, muchos aspectos de nuestra vida real, tienen su contrapartida en el mundo virtual. De esta forma, ya no nos sorprendemos al encontramos el prefijo “ciber” delante de palabras tan dispares como guerra, guerrilla, terrorismo, delincuencia, ataque, protesta, política, democracia, derechos o activismo. Además, la falsa sensación de anonimato que proporciona la Red favorece que personas u organizaciones que no harían determinada cosa en el mundo real, no tengan el más mínimo reparo para llevarla a cabo en el virtual.

La Revisión Estratégica Española, documento básico del planeamiento militar, contempla desde el año 2001, la posibilidad de sufrir ataques cibernéticos y equipara los flujos de información, en el entorno de una economía globalizada, a un recurso básico para el país. Entre las amenazas que refleja dicho documento se encuentran los ataques contra infraestructuras básicas del país, así como la penetración en las redes de comunicaciones, en los sistemas de mando y control, en el sistema de gestión de crisis, o en las bases de datos de los servicios de inteligencia. Para ello, las Fuerzas Armadas deberían dotarse de las capacidades necesarias para impedir cualquier tipo de agresión cibernética que pudiera amenazar la seguridad nacional.



Monográfico

TELECOMUNICACIONES MILITARES

En este momento, los ataques cibernéticos lejos de ser un hecho de ciencia ficción, son una realidad cotidiana para empresas y organismos públicos. Durante el año 2009 se detectaron más de 40 incidentes calificados como "graves" en instituciones y organismos públicos españoles. Uno de los casos más señalados, afectó a Javier Solana, cuyo ordenador fue accedido por servicios de inteligencia de "una gran potencia" no identificada, cuando aún era representante de la política exterior y de seguridad europea. Pero incidentes similares se han producido en otros países como EEUU, en el que los atacantes han obtenido información de sistemas del más alto nivel dentro del Departamento de Defensa.

Dentro de los riesgos crecientes se encuentra el ciberespionaje, tanto en su vertiente gubernamental como industrial. Detrás de estas acciones hay países u organizaciones con muchos recursos y por lo tanto, con una elevada capacidad para desarrollar malware específico, por lo que casi son imposibles de detectar usando los métodos tradicionales. Detrás de este ciberespionaje puede haber muchos países en este momento, pero cabe destacar la adquisición durante los últimos años de unas notables capacidades de Ciberguerra por parte del Ejército de Liberación del Pueblo Chino. A China se le atribuyen los ataques de 2007 dirigidos a Alemania, Nueva Zelanda, India, Francia,

Reino Unido y Estados Unidos, aunque este país siempre ha negado ser el origen de los mismos.

Según analistas de la OTAN, muchos organismos oficiales ni siquiera saben que tienen filtraciones de información debidas a malware en sus sistemas y por lo tanto, no están documentados un elevado porcentaje de los incidentes que se han producido, o que se están produciendo en la actualidad. Aunque en 2007 estos mismos analistas consideraban que el 90% de las amenazas a los sistemas de información se podían evitar con herramientas de seguridad ordinarias y buenas prácticas, la realidad no es tan optimista en la actualidad, dada la sofisticación de los ataques, los nuevos vectores de infección y las dificultades para detectar malware diseñado específicamente.

Asimismo, aunque hasta fechas recientes se consideraba que los ataques ciberterroristas dirigidos a dañar físicamente infraestructuras críticas tenían una probabilidad baja, la aparición del gusano Stuxnet ha activado todas las alarmas. Stuxnet está especialmente diseñado para atacar el software embebido en los sistemas de control industriales de la central nuclear de Bushehr (Irán). Hasta ahora, el malware intentaba infectar el mayor número de ordenadores posibles para destruir su información, robar información o convertirlos en esclavos, pero nunca se había visto

un malware orientado a dañar los sistemas de control industrial conectados a los ordenadores y basado en "exploits" específicos para varios sistemas distintos. Dicho de otro modo, es la primera vez que se detecta un gusano que es capaz de dañar los equipos de control industrial conectados a los ordenadores infectados. Dado lo sofisticado de Stuxnet, se considera que detrás tiene que haber un país, o una organización, con grandes capacidades informáticas y los dedos acusadores apuntan en este caso, a Israel o a los Estados Unidos.

En este momento, el ciberterrorismo se considera un riesgo creciente en países con elevada influencia exterior, como es el caso de los Estados Unidos. La amenaza del ciberterrorismo dirigido a sus infraestructuras técnicas, se está materializando como algo real y tangible prácticamente a diario. De hecho, los ataques están creciendo en severidad y sofisticación cada día que pasa y se sospecha que detrás de los mismos hay especialistas de los Emiratos Árabes Unidos, Irán, Indonesia o Malasia. Hay que señalar, que diversas fuentes de inteligencia apuntan a Malasia como un posible santuario para los especialistas informáticos pro Al-Qaeda y de la industria del malware en general.

Cara al ciberterrorista, los cibertales son una forma rentable, segura, rápida y eficaz de atacar la economía de un país, pero esto también es compartido por ciberdelincuentes de todo tipo. De esta forma, el ataque a Google de diciembre de 2009, se convirtió en una importante brecha para la seguridad online, del mismo modo, que la aparición en febrero de 2010

"Diversas fuentes de inteligencia apuntan a Malasia como un posible santuario para los especialistas informáticos pro Al-Qaeda y de la industria del malware en general"



de una nueva "botnet", que llegó a comprometer a más de 2.500 ordenadores de redes empresariales y gubernamentales en más de 196 países, así que nadie está a salvo si no toma las medidas técnicas adecuadas. Hay que señalar, que no es la primera vez que se tienen que desconectar ordenadores de la Red "in extremis", tal como ya ocurrió con 1.500 ordenadores del Departamento de Defensa de los EEUU en el año 2007.

Debemos ser conscientes de que en este momento nos enfrentamos a una peligrosa amenaza formada por una mezcla de vulnerabilidades, conocidas y no conocidas, junto con unos adversarios con unas capacidades cibernéticas en rápida expansión. Sin embargo, no disponemos de un sistema eficaz que nos permita detectar los riesgos, identificar los peligros, evaluar las amenazas y evitar, paliar o reparar los daños. En febrero de 2010, la inteligencia de los EEUU alertó de que la amenaza de un ataque masivo a las redes informáticas y de telecomunicaciones era creciente y que también se estaban incrementando las capacidades de unos enemigos cada vez más numerosos. Amenaza, que de materializarse, se podría convertir en lo que denominaron "Pearl Harbor Digital".

De forma general, la realidad de los últimos años demuestra lo siguiente:

"Debemos ser conscientes de que en este momento nos enfrentamos a una peligrosa amenaza formada por una mezcla de vulnerabilidades, conocidas y no conocidas, junto con unos adversarios con unas capacidades cibernéticas en rápida expansión"



a) Gran parte los ataques cibernéticos tienen una componente económica y van dirigidos a entidades financieras, o a sus usuarios. Por ello, hay una gran cantidad de malware específico dedicado a robar información con valor económico. También se ha producido un incremento notable de páginas web fraudulentas (phishing), según alerta INTECO en su informe de noviembre de 2010.

b) En los últimos meses, en la mayoría de los casos, como forma de ciberprotesta o ciberactivismo social, también se están incrementando los ataques de Denegación de Servicio Distribuidos (DDOS) a empresas e instituciones públicas.

En esta actividad, tiene un gran impacto la existencia de extensas redes de ordenadores "Zombi", que son controlados remotamente tras ser infectados por un troyano específico. Un caso reciente lo tenemos en los ataques sufridos por empresas como Visa, Mastercard o PayPal, a consecuencia de sus acciones contra Wikileaks y que han sido realizados por un grupo denominado "Anonymous".

c) La práctica monocultura informática existente, ya denunciada hace años por el experto en seguridad Bruce Schneier, en la que casi todos los ordenadores del mundo utilizan un mismo sistema operativo y casi las mismas aplicaciones informáticas, unido a la rapidez con la que aparece el malware que explota una determinada vulnerabilidad "zero day" (en ocasiones horas), hacen que sea muy rentable y sencillo elaborar malware. Asimismo, se está comenzando a ver malware dinámico (botnet) multi-plataforma, como el que recientemente afectaba a sistemas iPhone y



Android, o el troyano Boonana, que basado en Java, afectaba por igual a sistemas Windows, Linux o Mac y esta será una tendencia habitual los próximos meses.

d) La proliferación de "smartphones" con acceso a Internet, puede provocar que estos dispositivos también sean la estrella del malware durante los próximos años, principalmente, por su escasa capacidad para detectarlo y la posibilidad de recibir mensajes multimedia, o de capturar con la cámara códigos bidimensionales, en ambos casos, que contengan código malicioso.

e) Además, con las mejoras en las capacidades de ocultación, la aparición de nuevos vectores de infección del malware y el rápido desarrollo del mismo, los fabricantes de antivirus reconocen que tienen serias dificultades para mantener la seguridad de los sistemas. Esto ya fue admitido por Natalya Kaspersky, CEO de Kaspersky Lab, a la revista ComputerWorld en el año 2007 cuando dijo: "Ninguna compañía antivirus puede venir y decirte que puede manejarlo todo. Consideramos responsable hacerlo saber a la gente de forma clara."

Desgraciadamente, la situación, lejos de mejorar, ha empeorado bastante en los últimos meses. En realidad, la capacidad de detección de determinado malware varía enormemente entre los distintos programas antivirus, y ello, a pesar del esfuerzo de las empresas por analizar nuevo malware y que las actualizaciones de las firmas de la mayoría de ellos son diarias. La industria de desarrollo de malware ha demostrado una gran madurez y capacidad durante el año 2010 y debemos tener en cuenta además, que está compuesta por profesiona-

"La práctica monocultura informática existente hace años por el experto en seguridad Bruce Schneier, en la que casi todos los ordenadores del mundo utilizan un mismo sistema operativo y casi las mismas aplicaciones informáticas, unido a la rapidez con la que aparece el malware hacen que sea muy rentable y sencillo elaborar malware"

les que desarrollan un código malicioso de elevada calidad, casi siempre con fines económicos y en estrecha relación con los ciberdelincuentes y organizaciones que lo adquieren y explotan globalmente. Una vez infectado un sistema, el uso que se haga de él y los daños propios o a terceros que se produzcan por el malware, son tan impredecibles como variados. Debemos considerar además, que la lucha contra el malware y los ataques cibernéticos es muy desigual, ya que el atacante solamente necesita encontrar un "exploit" o vulnerabilidad, que puede ser a consecuencia un fallo "Zero day" para el que no hay solución en ese momento, para poder atacar un sistema casi con total impunidad.

f) En este momento, aproximadamente el 70% de los ordenadores domésticos se encuentra infectado por malware diverso y desgraciadamente, la seguridad sigue sin ser una prioridad para los usuarios domésticos, lo que influye muy negativamente en la seguridad global y pone las cosas muy fáciles para un potencial atacante de sistemas empresariales o gubernamentales.

g) Otra tendencia que se observa en los últimos meses, es el "Black-SEO", es decir, la técnica que permite que páginas web que contienen código malicioso oculto, aparezcan en las primeras posiciones de los buscadores, maximizando las posibilidades de infección. Hay que señalar, que también se han detectado páginas legítimas, incluso gubernamentales, que han sido modificadas para infectar con malware usando técnicas de inyección SQL.

El "Black-SEO" también está teniendo un enorme impacto en redes sociales como Facebook, que con más de 500 millones de usuarios, hace que sea muy rentable el envío masivo de mensajes con malware (especialmente troyanos), "phishing", "spam" o "scam". ☹

"Copyright 2010 Fernando Acero Martín. Verbatim copying, translation and distribution of this entire article is permitted in any digital medium, provided this notice is preserved. Quotation is allowed."

