ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

09/2015 16 enero de 2015

*Francisco J. Urueña Centeno**

CIBERATAQUES, LA MAYOR AMENAZA ACTUAL

CIBERATAQUES, LA MAYOR AMENAZA ACTUAL

Resumen:

En este artículo se van a tratar los nuevos sistemas de delincuencia, guerra y terrorismo que han aparecido recientemente con la llegada de las Tecnologías de la Información, que hoy en día están presentes en todos los ámbitos del mundo moderno. Comienza definiendo los términos informáticos utilizados para describir las nuevas amenazas, siguiendo con los métodos empleados para desarrollarlas, los medios donde se desarrollan y las medidas preventivas que las distintas organizaciones nacionales e internacionales han implementado para combatir esta nueva faceta de la delincuencia y la guerra moderna.

Abstract:

In this article we are going to treat the new systems of delinquency, war and terrorism that have appeared recently with the arrival of the Information Technologies, which nowadays are present in all the areas of the modern world. We will start by defining the IT terms that used to describe the new threats, we will follow with the methods used to develop them, the means where they develop and the preventive measures that the different national and international organizations have implemented to attack this new facet of the delinquency and the modern war.

Palabras clave:

Cibercrimen, ciberterrorismo, ciberdelincuencia, ciberguerra, ciberataque, virus informático, troyano, DDoS, ingeniería social, deep web, darknet, CSIRT, CERT.

Keywords:

Cybercrime, cyberterrorism, cyberdelinquency, cyberwar, cyberattack, IT, Trojan, DDoS, social engineering, deep web, darknet, CSIRT, CERT.

INTRODUCCIÓN

En el artículo se aborda la creciente importancia que están tomando los sistemas informáticos en todos los ámbitos de la sociedad actual. Este auge no ha pasado desapercibido por los grupos que operan al margen de la ley y por supuesto entre ellos, los estados y las organizaciones terroristas.

A lo largo del artículo se señalan las bases sobre las que se asienta el cibercrimen y la ciberguerra, las técnicas con las que se llevan a cabo los ciberataques, sus métodos de actuación y los objetivos principales sobre los que se podrían llevar a cabo los actos delictivos.

Otro de los puntos importantes que se tratan, es el medio donde estos grupos operan para que sus actividades no sean detectadas por las Agencias de Seguridad.

Se incluyen también ejemplos de ciberataques reales, con el objeto de dejar patente la realidad ya existente del cibercrimen.

Por último hace mención de las medidas de seguridad que los diferentes organismos nacionales e internacionales, han puesto en marcha para defenderse de esta amenaza emergente o utilizarla en su provecho.

Tampoco podemos olvidar que, actualmente, los ejércitos de la mayoría de países desarrollados, están creando o poseen ya secciones especializadas en la detección y el uso de ciberataques como una importante arma de guerra.

DEFINICIONES

Con objeto de clarificar la terminología utilizada y el entorno de referencia, se van a incluir una serie de definiciones, las más significativas, de los conceptos que se van a utilizar a lo largo del desarrollo del problema.

Un delito informático o ciberdelicuencia, es toda aquella acción ilegal que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Muchos de estos delitos, al no estar tipificados en la ley, se definen como abusos informáticos.

La criminalidad informática o cibercrimen tiene un alcance mayor, donde se incluyen delitos como el fraude, el robo, el chantaje, la falsificación y la malversación de caudales públicos utilizando ordenadores y redes como medio para realizarlos.

Básicamente *el Ciberterrorismo* podría definirse como:

"*El ciberterrorismo es el ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y datos que puedan resultar en violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos."*[1] *(Definición oficial del FBI).*
El ciberterrorismo, también denominado terrorismo electrónico, podemos definirlo como la forma de terrorismo que utiliza las tecnologías de información para intimidar, coaccionar o para causar daños a grupos sociales, con objeto de lograr una serie de fines políticos o religiosos.
Para calificar como ciberterrorismo, un ataque debe resultar en violencia contra personas o contra la propiedad, o al menos causar el daño suficiente como para generar miedo. Como ejemplos de ataques serían los que provocan muertos o heridos, explosiones, colisiones de aviones, contaminación de agua o pérdidas económicas, así como los ataques lanzados contra las infraestructuras críticas de un país, dependiendo de su impacto.
Por el contrario, ataques que interrumpen servicios no esenciales o que causan una molestia costosa, no se catalogan como ciberterrorismo.

La ciberguerra o guerra informática es aquel conflicto bélico que utiliza como campo de operaciones, en vez de los campos de batalla convencionales, el ciberespacio y las tecnologías de la información y como armas las aplicaciones, comandos y herramientas diversas que proporcionan la informática y las telecomunicaciones. Los objetivos más comunes son la inhabilitación de los sistemas informáticos del enemigo o la obtención de información.

Estos actos, tanto los incluidos en el cibercrimen, en la ciberguerra o en el ciberterrorismo, se denominan «CiberAtaques».

¿En qué se basan los ciberataques?

Dependiendo de la meta que se desee alcanzar o el daño que se desee provocar, veremos que los ciberataques pueden presentarse de diferentes maneras. Para alcanzar sus objetivos, el ciberdelincuente utiliza una serie de técnicas básicas, las cuales se aplican individualmente o de forma combinada. Entre las técnicas más habituales, se podrían citar:

[1] Pollit M. Mark, *Ciberterrorism: Fact or Fancy*, FBI Laboratory

Los virus informáticos: Los Virus Informáticos son esencialmente programas de carácter malicioso, que pretenden infectar a otros archivos contenidos en el sistema, con el objeto de producir modificaciones o daños en el sistema informático que han infectado. El archivo infectado con el virus, se denomina "víctima". El virus introduce en los archivos infectados una secuencia de código malicioso, dirigida fundamentalmente a los archivos ejecutables del sistema atacado. A cada ejecución de estos archivos, se produce una propagación del virus, infectando a nuevos archivos y multiplicando sus efectos.

El envío masivo de correo no deseado o SPAM: Se llama "Spam" a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente con publicidad, generalmente enviados en grandes cantidades que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. Aunque se puede hacer spam por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico.[2]

Esta técnica también puede tener como objetivo los teléfonos móviles, a través de mensajes de texto o con los sistemas de mensajería instantánea.

La suplantación de remitentes de mensajes mediante Spoofing: la idea de este ataque, otra cosa es la puesta en práctica, es muy sencilla: desde su equipo, un atacante simula la identidad de otra máquina de la red para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del host suplantado. Utilizando comandos del sistema, los accesos NFS, o la protección de servicios de red mediante TCP Wrapper, el spoofing sigue siendo en la actualidad un ataque peligroso y factible contra cualquier tipo de organización.

El envío o instalación de archivos espías o Keyloggers: Como su nombre indica un Keylogger es un programa que registra y graba la pulsación de teclas y, algunos, también los clicks del ratón. La información recolectada será utilizada luego por la persona que lo haya instalado. Actualmente existen dispositivos de hardware o bien aplicaciones (software) que realizan estas tareas.

El uso de Troyanos para el control remoto de los sistemas o la sustracción de información: Los Troyanos Informáticos o Caballos de Troya son una clase de virus que se caracteriza por engañar a los usuarios disfrazándose de programas o archivos habituales (fotos, archivos de música, archivos de correo, etc.), con el objeto de infectar y causar daño. El objetivo principal de un Troyano Informático es crear una puerta trasera (backdoor en inglés) que dé acceso a la administración remota del equipo infectado, con el objeto de robar información

[2] Asociación de Universidades Populares de Extremadura, 21 de abril de 2014, Disponible en http://www.nccextremadura.org/recursostic/

confidencial y personal. Las acciones que el atacante puede realizar dependen de los privilegios del usuario que está siendo atacado y de las características del troyano.

Como ejemplos de troyanos tenemos Back Orifice 2000, SubSeven, Cybersensor, DeepThroat v2, Dolly Trojan, Girlfriend, nCommand v1.0, NetSpher, etc.[3]

El uso de archivos BOT del IRC (Internet Relay Chat): es una contracción de la palabra robot. Es un programa que permite que el sistema sea controlado remotamente sin el conocimiento ni consentimiento del usuario. En webs de conversación online como por ejemplo los chats o programas IRC, algunos bots son utilizados para simular una persona y hacer un uso maligno, intentando hacer creer a los demás usuarios del servicio que hablaban con una persona real. Pero la utilización efectiva para el cibercrimen es el mantenimiento de salas de chat, abiertas indefinidamente, y que son utilizadas esporádicamente como canal de comunicación. Al haber un BOT funcionando continuamente, el IRC detecta a ese BOT como a una persona activa en el chat, por lo que esa sala de chat nunca es clausurada.

El uso de Rootkits: es un conjunto de herramientas que consiguen ocultar un acceso ilícito a un sistema informático. Estas herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema, a menudo con fines maliciosos.

Los rootkits, al estar diseñados para pasar desapercibidos, no pueden ser detectados. Si un usuario intenta analizar el sistema para ver qué procesos están ejecutándose, el rootkit mostrará información falsa, mostrando todos los procesos excepto él mismo y los que está ocultando.

Ciberataques realizados mediante las técnicas anteriormente descritas

Mediante el uso de las técnicas mencionadas en el apartado anterior y algunas otras, se realizan los ciberataques a los sistemas informáticos. Como hemos comentado anteriormente, aplicando estas técnicas, una sola o una combinación de varias de ellas, consiguen una serie de efectos que perjudican, inhabilitan o provocan intrusiones en los sistemas objetivo de los ciberdelincuentes. Entre los efectos que pueden provocar estos ataques podemos destacar:

Cambios en las direcciones de dominio (DNS): El cambio de dominio significa que la web o un servicio determinado va a tener otra dirección, por lo que los usuarios o el mismo propietario no tendrían acceso a un determinado recurso, provocando un grave perjuicio, dependiendo del ámbito de dicho servicio.

[3] Ingeniería social conceptos, 30 de noviembre de 2013, Disponible en http://www.slideshare.net/carlosivangallardo2/ingenieria-social-conceptos

Intrusiones no autorizadas: a día de hoy, es rara la estación de trabajo que no está conectada a Internet. La posibilidad de acceder remotamente a los equipos abre la puerta para los accesos maliciosos por parte de personas no autorizadas. Una intrusión puede tener básicamente dos efectos negativos: la filtración de información confidencial, y la destrucción de datos por parte del intruso.

En el caso de la destrucción, se puede deber al deseo de reconocimiento social o por otros motivos (conflictos políticos entre países, sabotaje industrial, etc.).

DDoS (Denegación de servicio): DDoS son las siglas de Distributed Denial of Service. La traducción es "ataque distribuido de denegación de servicio", lo que significa es que se ataca al servidor desde muchos ordenadores para que deje de prestar servicio.

El DDoS es un método relativamente sencillo, de hecho, valdría con que hubiese un número suficientemente grande de personas solicitando simultáneamente servicios de una web para colapsarla. Sin embargo, las herramientas que se suelen usar son algo más sofisticadas.

Con ellas se pueden crear muchas conexiones simultáneas o enviar paquetes alterados para multiplicar los accesos. También permiten modificar los paquetes poniendo como IP de origen una IP falsa, de forma que no pueden detectar quién es el atacante real.

Un ejemplo de este tipo de ataques fue la Operación Payback, desarrollada el 6 de diciembre de 2010, en defensa del boicot a la publicación de documentos clasificados por Wikileaks. La agrupación Anonymous, mediante comunicados basados en el uso de las redes sociales, sincronizaron a miles de usuarios para provocar una denegación de servicio en los servidores de PostFinance y PayPal en venganza por el bloqueo de las cuentas de WikiLeaks.

Otra técnica para llevar a cabo los DDoS es usar botnets: redes de ordenadores infectados por un troyano y que un atacante puede controlar remotamente. De esta forma, los que saturan el servidor son ordenadores de gente que no sabe que está participando en un ataque DDoS, por lo que es más difícil encontrar al verdadero atacante.

Saturación de correos: consiste en enviar masivamente emails a un servidor o una cuenta, de tal forma que éste se sature por la gran cantidad de datos que recibe y que llegan al límite de almacenamiento o de su capacidad de procesamiento, impidiendo la recepción y envío de los emails reales y necesarios.

Interferencia electrónica de comunicaciones: La interferencia electromagnética es la perturbación que ocurre en cualquier circuito, componente o sistema electrónico causada por una fuente de radiación electromagnética externa al mismo. También se conoce como EMI por sus siglas en inglés (ElectroMagnetic Interference), Radio Frequency Interference o RFI. Esta perturbación puede interrumpir, degradar o limitar el rendimiento de ese sistema. La fuente de la interferencia puede ser cualquier objeto, ya sea artificial o natural, que posea corrientes eléctricas que varíen rápidamente, como un circuito eléctrico, el sol o las auroras boreales.

En el tema que nos ocupa, se trata de interferencias causadas por señales emitidas intencionadamente, con el propósito expreso de producir una disfunción en los sistemas de comunicaciones, es decir, una interferencia.

El dispositivo más común es el inhibidor de frecuencias. Un inhibidor de frecuencias es un dispositivo capaz de dificultar o impedir las comunicaciones por radiofrecuencia entre otros dispositivos que están en su campo de alcance. Sirve para interrumpir la señal entre teléfonos móviles, redes WiFi, walkie talkies o bluetooth.

Su objetivo no es eliminar o suprimir determinadas frecuencias del espectro si no producir un ruido mayor que imposibilite que emisor y receptor puedan entenderse en su proceso comunicativo. El inhibidor de frecuencias está formado por un generador de onda y un transmisor. En conjunto, generan y emiten una señal de mayor potencia que la del resto de dispositivos.

BlindRadars, bloquear tráfico aéreo: se trata de una técnica de interferencia electrónica de los radares de las torres de control y de los sistemas de seguimiento de aeronaves. Mediante esta técnica los centros de control de tráfico aéreo, pierden la localización exacta de los aviones, por lo que los controladores aéreos no pueden desarrollar su labor y no pueden guiar a los aeroplanos en su ruta de viaje y en los despegues y aterrizajes, pudiéndose producir choques en el aire o que el avión se estrelle en su maniobra de aproximación a la pista de aterrizaje.

Ataque por robo de información: más del 40% de los programas maliciosos que se envían vía mail tienen como finalidad robar información personal y financiera. Muchos de ellos son dirigidos a empresas. Con el surgimiento del modelo de negocio online, fueron apareciendo nuevos y cada vez más complejos ataques informáticos que buscan obtener información confidencial de los usuarios, dando lugar a una nueva modalidad delictiva, encuadrada dentro del marco de las estafas.

De los principales métodos actuales para obtener información personal de usuarios, el primero de ellos es el phishing. El phishing es una modalidad de obtención de información llevada a cabo a través de Internet que intenta obtener, de manera completamente

involuntaria y fraudulenta, datos personales o sensibles que posibiliten realizar una estafa, utilizando metodologías de Ingeniería Social.
El segundo, son los códigos maliciosos como backdoor, keylogger o los troyanos bancarios (bankers).

Ataque por anulación de equipos: mediante el envío de virus se puede conseguir que equipos personales o servidores queden paralizados para dar el servicio requerido. Este tipo de ataque provoca unos síntomas comunes en los equipos atacados, como que el equipo funciona más lento de lo normal, deja de responder o se bloquea con frecuencia, se reinicia cada pocos minutos, las aplicaciones del equipo no funcionan correctamente, no se puede obtener acceso a determinados dispositivos o pantallas distorsionadas.

Ataque por pulso electro-magnético: el ataque de pulso electromagnético es un método de ataque militar realizado con armas generadoras de importantes cantidades de energía electromagnética ambiental que destruyen total o parcialmente el equipamiento eléctrico y electrónico dentro de su radio de acción[4].

Un EMP es un pulso de energía que se puede estar generado por fuentes naturales como rayos o tormentas solares que producen ionizaciones en la atmósfera de la Tierra, la ionosfera y el campo magnético, o también puede ser creado artificialmente mediante un arma nuclear u otros dispositivos no-nucleares.

El pulso electromagnético o EMP en sus siglas en inglés es un efecto secundario descubierto con las pruebas atómicas. Se observó que tras una explosión nuclear, los aparatos electrónicos en un cierto radio de acción quedaban dañados o totalmente inutilizados.

Las posibilidades que ofrece este fenómeno en el campo de la ciberguerra son inmensas. Los ingenieros militares se dieron prisa en desarrollar artefactos que maximizaran dicho efecto. Una bomba EMP detonada cerca de fuerzas enemigas dejaría todas sus defensas y contramedidas en tierra, inmovilizadas y más teniendo en cuenta, que hoy día la ventaja que confiere la electrónica a los ejércitos modernos es vital. Pero esta no es la única estrategia posible. Existe lo que se llama ataque de pulso electromagnético de gran altitud o HEMP, capaz de paralizar un continente entero con un solo disparo.

[4] CXO Community, 23 de octubre de 2014, disponible en http://www.cxo-community.com/articulos/blogs/blogs-el-abc-de/5780-estamos-preparados-para-un-pem-pulso-electromagnetico.html

LA PRINCIPAL PUERTA DE ACCESO – LA INGENIERÍA SOCIAL

Con el término ingeniería social se define el conjunto de técnicas psicológicas y habilidades sociales utilizadas de forma consciente y muchas veces premeditada para la obtención de información de terceros. En este caso nos centraremos en la obtención de información para el acceso no autorizado a sistemas informáticos.
No existe una limitación en cuanto al tipo de información y tampoco en la utilización posterior de la información obtenida. Puede ser ingeniería social el obtener de un profesor las preguntas de un examen o la clave de acceso de la caja fuerte de un banco. Sin embargo, el origen del término tiene que ver con las actividades de obtención de información de tipo técnico utilizadas por hackers (claves de acceso, passwords, IP's, tipos de sistemas, sistemas de seguridad, etc).
Un hecho importante es que el acto de ingeniería social acaba en el momento en que se ha conseguido la información buscada. Las acciones que esa información pueda facilitar o favorecer no se enmarcan bajo este término. En muchos casos los ingenieros sociales no tocan un ordenador ni acceden a sistemas, pero sin su colaboración otros no tendrían la posibilidad de hacerlo.[5]

¿En qué se basa la Ingeniería Social?

Toda persona padece las mismas debilidades dentro y fuera del sistema informático o de la red de trabajo.
En palabras de Kevin Mitnick, uno de los personajes más famosos del mundo por delitos utilizando la Ingeniería Social: "*usted puede tener la mejor tecnología, firewalls, sistemas de detección de ataques, dispositivos biométricos, etc. Lo único que se necesita es una llamada a un empleado desprevenido para acceder al sistema sin más. Tienen todo en sus manos*".[6]

Según su opinión, la Ingeniería Social se basa en estos cuatro principios: "*todos queremos ayudar", "el primer movimiento es siempre de confianza hacia el otro", "no nos gusta decir NO" y "a todos nos gusta que nos alaben".*

Artimañas de ingeniería social muy comunes, que permiten la introducción de programas maliciosos o de envío de información al atacante, basadas en las debilidades personales y que la mayoría de nosotros ha podido sufrir personalmente, podrían ser las siguientes:

Uso de archivos adjuntos en e-mails o chats, ofreciendo, por ejemplo, fotos "*íntimas*" de alguna persona famosa o algún programa "*gratis*".

[5] Hack Story, 22 de julio de 2013, disponible en http://hackstory.net/Ingenier%C3%ADa_social
[6] Mitnick Kevin D., *The art of deception*, John Wiley & Sons, 4 de octubre de 2002

El aprovechamiento de la confianza que el usuario tiene en alguna empresa o marca reconocida. El ejemplo típico del email solicitando la revisión de sus cuentas bancarias, donde le piden que introduzca su clave.

Valerse de personajes famosos y políticos para lograr que sus inventos se propaguen, engañando a los usuarios desprevenidos o demasiado curiosos.

Noticias sobre catástrofes: las tormentas en Europa del 2007 sirvieron para propagar Nuwar (o Gusano de la Tormenta).

Existen diferentes técnicas de Ingeniería Social que podemos dividirlas en tres tipos, según el nivel de interacción del ingeniero social:

Las Técnicas Pasivas como la observación.

Las Técnicas no presenciales como recuperación de contraseñas, teléfono, carta, fax o chats.

Las Técnicas presenciales pero no agresivas como buscar en la basura, mirar por encima del hombro, seguimientos, vigilancia de edificios, agendas y teléfonos móviles o técnicas de desinformación.

Los Métodos agresivos como suplantación de personalidad, chantaje o extorsión, despersonalización o presión psicológica.

DEEP Web

La gran mayoría de los usuarios de Internet, piensa que todos los contenidos de la red están accesibles o al menos aparecen en los buscadores cuando realizan una petición a estos servidores. Pero lo que no saben es que más del 95% de los contenidos de Internet no son accesibles por los métodos habituales, y que la mayor parte de estos contenidos, no están al alcance del usuario normal.

El concepto de deep web es sencillo. La deep web es aquella parte de la red que contiene material, información y páginas web que o están indexadas en ninguno de los buscadores existentes, como pueden ser Bing, Google, Yahoo, etc. Así, en el hipotético caso que los buscadores pudieran indexar la totalidad de contenido en la web, la deep web no existiría. No obstante esto es imposible ya que muchas de las páginas y documentos están diseñados de tal forma que no puedan ser indexados, como por ejemplo: páginas protegidas con contraseña, documentos en formatos no indexables (flash, páginas sin html, etc) o documentos a los que para acceder a la información hay que interrogar a la base de datos (Por ejemplo RAE).

Aunque no se conocen datos precisos, se estima una proporción del 4%-96% entre la web normal y la deep web. Según un estudio realizado por la Universidad de California en Berkeley en el año 2012 se estimaba que el internet profundo contaba con un volumen de datos cercano a los 91.000 Terabytes[7].

Todo lo que hay en la deep web no podemos decir que sea intrínsecamente malo. Podemos encontrar contenido interesante y diverso como por ejemplo: contenido almacenado por los gobiernos de distintos países, organizaciones que almacenan información (por ejemplo la NASA, datos de agencias meteorológicas, datos financieros, diccionario de la R.A.E., etc), bases de datos de distintos ámbitos que representan un porcentaje muy importante de la información almacenada en la deep web y foros de temáticas muy diversas.

Pero como es lógico pensar, también nos podemos encontrar contenido ilícito como lo siguiente: venta de drogas, pornografía de todo tipo, contratación de sicarios, documentos clasificados como por ejemplo los de Wikileaks, páginas, programas y material de hackers, páginas para comprar o fabricar armas, piratería de libros, películas, música, software, etc.

Afortunadamente, y esto es muy importante resaltarlo, el contenido que se acaba de describir representa un porcentaje muy pequeño de lo que es la deep web. Este tipo de contenido se clasifica dentro de una sub categoría de la deep web denominada "**darknet"**.

Cabe destacar que el 90% de contenido que existe en la deep web es accesible para la totalidad de usuarios.

El sistema que rige la 'deep web' es The Onion Router (TOR), una red de comunicaciones que pone el énfasis en el anonimato de sus integrantes. Para conseguirlo, cifra los mensajes y los hace pasar por un número indeterminado de nodos de manera que sea, si no imposible, sí más difícil obtener la dirección IP del navegante. Precisamente su nombre ("onion" es cebolla en inglés) hace referencia a las distintas capas de anonimato que cubren los datos que se mueven por TOR[8].

[7] Lesk Michael, *How much information is there in the world?*, 1997, Consultado el 16 de julio de 2012
[8] IEEE, Luis de Salvador Carrasco, *Redes de anonimización en internet: cómo funcionan y cuáles con sus límites*, 21 de febrero de 2012, disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2012/DIEEEO16-2012_RedesAnonimizacionInternet_LdeSalvador.pdf

Las direcciones web están cifradas (por ejemplo: f3ew3p7s6lbftqm5.onion/) y, en consecuencia, el tiempo de carga supera en mucho el de los contenidos indexados habituales[9].

Aunque con navegadores y sistemas de correo especiales, se puede explorar la red y enviar emails sin ser detectados, el anonimato total de la deep web *"es en relación con los demás usuarios".* Respecto a las distintas agencias de seguridad, siempre presentes en la red, la detección es posible, pero es mucho más compleja que utilizando los medios convencionales.

MEDIDAS DE PROTECCIÓN

Ante el grave peligro que supone esta nueva concepción de la delincuencia y de la propia sistemática de hacer la guerra, los diferentes gobiernos y las instituciones internacionales han comenzado a tomar medidas, para que esta grave amenaza pueda ser detectada y evitada antes de que se produzca. Como ejemplos de organismos nacionales creados para la defensa contra el cibercrimen y la ciberguerra tenemos:

Dependiente del Ministerio de Defensa español se puso en marcha el Mando Conjunto de Ciberdefensa, que dirige y coordina todas las acciones de las Fuerzas Armadas para frenar las ciberamenazas (creado el 19/02/2013)[10].

Creación del Catálogo de Infraestructuras Críticas[11] (CIC), infraestructuras susceptibles de sufrir un ciberataque.

Creación de la Red de emergencias CERT,s y CSIRT,s (son las siglas de "Computer Emergency Response Team" y "Computer Security Incident Response Team" respectivamente):

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó a finales del año 2006 como el CERT gubernamental/nacional, y su función es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y

[9] El Confidencial, Alfredo Pascual, 9 de abril de 2013, Disponible en http://www.elconfidencial.com/tecnologia/2013/04/09/deep-web-un-paseo-por-los-bajos-fondos-de-internet-4641

[10] Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas, BOD de 26 febrero 2013.

[11] Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, BOE de 21 mayo 2011.

ayude a responder de forma rápida y eficiente a las Administraciones Públicas y a las empresas estratégicas, y afrontar de forma activa las nuevas ciberamenazas[12].

El Foro CSIRT.es pretende crear una plataforma de coordinación y colaboración entre los CSIRTs de ámbito nacional que permita optimizar la cooperación entre los mismos para actuar frente a problemas de seguridad informática en las redes españolas. A su vez, fomentar la divulgación de información de interés y la mejora de la visibilidad de los CSIRTs miembros del Foro en la comunidad española e internacional.

Dentro de las Instituciones de vigilancia de organizaciones nacionales e internacionales podemos destacar las siguientes:
Agencia Europea de Seguridad de las Redes y de la Información (ENISA), que tiene una función de asesoramiento y coordinación de las medidas adoptadas por la Comisión y los países de la Unión para dar seguridad a sus redes y sistemas de información[13].

Centro de Ciberdefensa de la OTAN, creado en 2008 y cuyas funciones son analizar y responder a los ataques informáticos y las amenazas procedentes de Internet. El centro está situado en Estonia.

Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), es el órgano que se encarga de impulsar, coordinar y supervisar todas las actividades que tiene encomendadas la Secretaría de Estado de Seguridad del Ministerio del Interior en relación con la protección de las infraestructuras críticas españolas, aprobada en el Consejo de Ministros de 2 de noviembre de 2007.

¿POR QUÉ ES LA MAYOR AMENAZA ACTUAL?

«Los ciberataques sustituyen al terrorismo convencional como primera amenaza para los E.E.U.U.»

El ex secretario de Defensa, León Panetta, aseguró el otoño pasado, que cualquiera de los potenciales ataques a los que se exponen las instituciones estadounidenses podría convertirse en el "*próximo Pearl Harbour*"[14].

[12] Sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, BOE de 7 mayo 2002, el Real Decreto 421/2004 de regulación del CCN, BOE de 19 marzo 2004 y en el Real Decreto 3/2010, de 8 de enero por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, BOE de 29 enero 2010.

[13] Reglamento (CE) nº 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información, DOUE de 13 abril 2004.
[14] Comparecencia en el Museo del Espacio en Nueva York, 12 octubre 2012.

Los ciberataques están aumentando de forma exponencial en su faceta de sustracción de información confidencial y de secretos industriales, que están produciendo graves pérdidas en las industrias punteras de los estados y transfiriendo conocimiento tecnológico avanzado a estados que practican este tipo de ataques.

Por poner un ejemplo, el comité de Asuntos de Espionaje de la Cámara de Representantes de Estados Unidos, ha calculado que los robos en Internet de secretos comerciales y propiedades intelectuales, en su gran mayoría dirigidos por China, le han costado a este país más de 300.000 millones de dólares en 2012[15].

Los ciberataques con fines terroristas o ciberguerra, pueden alcanzar sitios insospechados, y aun no cumpliendo total o parcialmente con su objetivo, la sola difusión mediática del hecho de que instalaciones vitales para el país o la población en general, son vulnerables a este tipo de ataques, provoca irremisiblemente el pánico entre la población.

Vamos a ver el porqué de definir los ciberataques como "*la mayor amenaza actual".* En un mundo completamente interconectado y donde la dependencia de la informática es prácticamente completa, cualquier falla o intrusión en un sistema informático puede causar daños irreparables.
Por supuesto, el ciberataque no podemos definirlo como la panacea para la nueva delincuencia. También tiene una serie de impedimentos y limitaciones que dificultan su utilización masiva.

Ventajas

Pueden producir daños a cualquier escala y en cualquier lugar: a través de Internet, el alcance de los ataques se puede realizar a cualquier escala y además sobre infraestructuras situadas en cualquier lugar del mundo, sin ningún tipo de restricción por la distancia a la que se encuentre el objetivo.

Pueden paralizar servicios básicos: la paralización de servicios básicos, tanto para la población en general, como las infraestructuras de seguridad de cualquier país, que a su vez pueden producir un efecto dominó en otros servicios dependientes de los primeros, hacen de los ciberataques un peligro mucho mayor que cualquier método de ataque convencional.

[15] El País, 20 de febrero de 2013, disponible en http://internacional.elpais.com/internacional/2013/02/20/actualidad/1361395431_105565.html

El ataque se puede realizar desde cualquier parte del mundo: lo que ofrece al ciberdelincuente varias ventajas fundamentales:

Seguridad: el atacante no tiene que exponerse físicamente a su adversario o a las fuerzas policiales, no necesita estar presente en la escena del crimen, ni necesita tener un peligroso plan de escape ya que se encontraría a cientos o miles de kilómetros del lugar del ataque.

Impunidad: muchos de estos delitos quedan impunes al no poder descubrir el lugar desde donde se perpetró el hecho, incluso hay países donde la legislación no cataloga determinados actos como delictivos, por lo que el delincuente no puede ser castigado.

Anonimato: igual que en el punto anterior, es muy complicado identificar al atacante. Hay ataques que se realizan y no dejan ninguna huella de la intrusión en el sistema, incluso dejando huellas es prácticamente imposible identificar a una persona que realiza el ataque desde miles de kilómetros de distancia.

Se pueden ejecutar con medios al alcance de cualquier persona: para realizar un ciberataque no es necesario contar con medios muy sofisticados y costosos. Bastaría con un ordenador y una conexión a Internet. Estos medios están a disposición de cualquiera, por lo que su adquisición es barata y no levanta ningún tipo de sospechas.

Gran impacto psicológico sobre la población: como hemos comentado anteriormente, aunque el objetivo del ciberataque se consiga de forma parcial, provoca una sensación de vulnerabilidad y pánico añadido a la población, que ve como sus lugares más sagrados, sus instalaciones más seguras o que afectan a la salud pública, pueden ser destruidos o inhabilitados por estas organizaciones.

Gran repercusión mediática: cualquier hecho de este tipo produce una gran difusión en los medios de comunicación, que suelen magnificar el hecho además de lanzar especulaciones sobre “lo que podría haber pasado si …”

Inconvenientes

Podemos destacar los siguientes:

El cibercriminal debe tener amplios conocimientos técnicos: no todo el mundo, más bien pocas personas están capacitadas para realizar este tipo de actos, ya que es necesario poseer unos amplios conocimientos técnicos para llevar a cabo cualquier ciberataque por pequeño que sea.

Ninguna repercusión mediática: en muchos casos la acción realizada pasa desapercibida para el público en general, incluso para la institución que ha sido atacada, porque el cibercriminal para cubrirse no deja rastro alguno de su intrusión en el sistema.

Daños colaterales no deseados: a veces un ataque realizado a un sistema provoca daños no deseados a otros sistemas dependientes del primero, o bien, inutiliza servicios que en principio no se deseaba perjudicar.

No se pueden controlar, ni medir los resultados del ataque: hay ocasiones en que los ataques, una vez lanzados son incontrolables por el factor multiplicativo de algunas de estas acciones. En otras ocasiones evaluar realmente el daño causado es bastante complejo, porque la institución atacada evita dar difusión al hecho, para no provocar el pánico en la población y para no poner en evidencia que su sistema se seguridad ha sido vulnerado.

El escenario carece de dramatismo: cuando los ciberataques se utilizan con fines terroristas, a diferencia del terrorismo clásico, donde tras el ataque observamos a través de los medios de comunicación un escenario dantesco, con multitud de muertos, heridos y destrozos de todo tipo, el ciberterrorismo es mucho más "higiénico" y raramente un ataque de este tipo produciría escenas macabras, que tanto impactan a la población.

Casos "reales" de CiberAtaques

Estos son unos pocos ejemplos de casos "reales" de ciberataques. Como todos los sucesos en este complicado campo, estos ataques son difíciles de contrastar y más complicado aún, demostrar su autoría.

Guerra de Kosovo, año 1999, un grupo formado por más de 450 expertos informáticos de diferentes nacionalidades, dirigidos por el Capitán Dragan, de diferentes nacionalidades de diferentes nacionalidades, atacaron y consiguieron acceder a los ordenadores estratégicos de la OTAN, bloquearon la web de la Casa Blanca durante todo el fin de semana e introdujeron fotos obscenas en los sistemas del portaaviones norteamericano Nimitz. Este acto sólo fue una demostración de lo que eran capaces y no causaron daños aparentemente[16].

Taiwán, año 2003 fue objeto de un ataque que dejó sin servicio infraestructuras como hospitales, la Bolsa y algunos sistemas de control de tráfico. Este ataque supuestamente

[16] El Mundo, 16 de abril de 1999, disponible en http://www.elmundo.es/navegante/99/abril/16/hackers.html

organizado y dirigido desde China, provocó el caos, mediante ataques de denegación de servicio (DDoS), virus y troyanos[17].

Irán, septiembre de 2010, mediante el uso de un virus o programa denominado Stuxnet, recibió un ciberataque a los motores de alta frecuencia de las centrifugadoras de enriquecimiento de combustible nuclear, en su central de Natanz. Irán acusó a Estados Unidos como autor del hecho, aunque existían dudas y también se pensó en una acción de los servicios secretos israelíes [18].

Varios países entre los cuales estaban Irán, Israel, Sudán, Siria, Líbano, Arabia Saudí y Egipto, mayo de 2012, se descubre un Malware dañino diseñado para realizar tareas de Ciberespionaje. Se le denominó Flame o sKyWIper.[19]

Operation Payback, 6 de diciembre de 2010, campaña de ciberataques lanzada por el grupo Anonymous en defensa de WikiLeaks, contra PostFinance y PayPal por el bloqueo de las cuentas de WikiLeaks. El ataque consiguió un efecto de denegación de servicio (DDoS) en los servidores de estas compañías. Facebook y Twitter cerraron las cuentas del grupo hacker que como venganza atacan a su vez a los servidores de Visa y Mastercard y consiguen bloquearlos.[20].

CONCLUSIONES

Internet es un medio inseguro y global, por ello es un magnífico campo de operaciones para la ciberdelincuencia y la ciberguerra.

La utilización de este medio por las agencias de seguridad nacionales y por las organizaciones que operan al margen de la ley va en aumento.
Es un medio de trabajo seguro para la integridad física de las personas que lo utilizan, ya que no se exponen a riesgos como enfrentamiento directo y fuga.

[17] Computer World, 21 de marzo de 2013, disponible en http://cso.computerworld.es/alertas/taiwan-senala-a-china-como-responsable-de-ciberataques
[18] New York Times, 1 de junio de 2012, disponible en http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=1&_r=2&hp&
[19] Budapest University of Technology and Economics, sKyWIper Analysis Team, 30 de mayo de 2012, disponible en http://www.webcitation.org/682bQ4f6J
[20] BBC Mundo, 8 de diciembre de 2010, disponible en http://www.bbc.co.uk/mundo/noticias/2010/12/101208_wikileaks_mastercard_pagos_ataque_hackers_rg.shtml

Es un medio económico y al alcance de cualquiera. Cualquier compra de material informático o la contratación de servicios de Internet, es algo tan habitual que no levanta ningún tipo de sospechas. Además el cibercriminal cuenta con servicios públicos como los numerosos cibercafés, desde donde puede operar con un coste mínimo y con un anonimato mayor que si operase desde su domicilio.

Su alcance y sus repercusiones pueden ser mucho mayores que los de la delincuencia convencional. Como ejemplos de posibles objetivos terroristas o de ciberguerra destacamos los siguientes: Sistemas de control de energía eléctrica, Aeropuertos, Red ferroviaria, Redes de satélites, Sistemas financieros, Servicios de emergencia.

Otros posibles objetivos podrían ser: centrales nucleares, industria aeroespacial, industria química, redes de aguas, etc, etc, …

Sólo hace falta un poco de imaginación para comprender lo que podría suponer un ataque a cualquiera de estos sistemas.

Los estados y por supuesto los ejércitos, deberán poseer unos sistemas de seguridad, con magníficos medios técnicos y personal muy bien entrenado para hacer frente a esta amenaza.

La ciberguerra será una de las armas más poderosas de los estados en el futuro próximo, como ya ha quedado demostrado en los ciberataques reales que se han producido en algunos conflictos.

Por todo ello los ciberataques deben ser considerados como una grave AMENAZA EMERGENTE

[i]

*Francisco J. Urueña Centeno**
Alférez (RV)