Incidentes que afectan a la Seguridad de las TIC

ATAQUES DDOS, *PHISHING*, *DEFACEMENT* Y OTROS INCIDENTES SON ALGUNAS DE LAS AMENAZAS MÁS FRECUENTES QUE AFECTAN A LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE LAS TIC

Centro Criptológico Nacional
Centro Nacional de Inteligencia

Entre las amenazas más comunes que afectan a los Sistemas de Información, se encuentra el ataque DDoS (siglas en inglés de *Distributed Denial of Service*) que consiste en privar a los usuarios de un determinado servicio o recurso mediante el consumo del ancho de banda, de la reducción de eficacia del servidor o de la interrupción del canal de comunicación entre el sistema y la red. Dicho ataque se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le denomina "denegación", pues hace que el servidor no dé abasto a la cantidad de usuarios.

Actualmente, los ataques más eficaces son los que se dirigen al conjunto de protocolos TCP/IP, gracias a los cuales es posible la transmisión de datos entre redes de ordenadores. Estos ataques se realizan mediante la inundación de paquetes TCP SYN y la saturación del ancho de banda. También son frecuentes los ataques a los servicios Web, a los servicios de correo electrónico y a los servidores DNS (bases de datos asociadas a nombres de dominio).

Como ejemplo práctico de la gestión defensiva realizada ante un ataque DDoS, cabe señalar el caso de Estonia, que sufrió el año pasado un ciberataque contra su infraestructura de Internet.

Entre el 27 de abril y el 11 de mayo de 2007, el cambio de ubicación en Tallin de una estatua conmemorativa soviética provocó una grave crisis diplomática entre Estonia y Rusia. En determinados foros rusos se difundieron mensajes patrióticos enardecidos y se explicó a los usuarios la forma de realizar ataques cibernéticos sencillos.

En estos ataques se emplearon *Botnets y Defacements* con propaganda rusa, modificando determinadas páginas web sin autorización de sus propietarios. Como consecuencia de ello, los sitios web gubernamentales clave resultaron perjudicados, en especial los del Presidente, el Primer Ministro y el Parlamento. Los ataques electrónicos también afectaron a la Policía, a los Ministerios de Economía, Agricultura, Medio Ambiente, Asuntos Sociales y al Departamento de Comunicaciones.

Con el fin de resolver el problema en el menor tiempo posible, fue necesaria la coordinación de diversos CERTs a nivel internacional, entre ellos el CCN-CERT, cuya misión consistió fundamentalmente en desactivar las Botnets y filtrar los puntos de entrada.

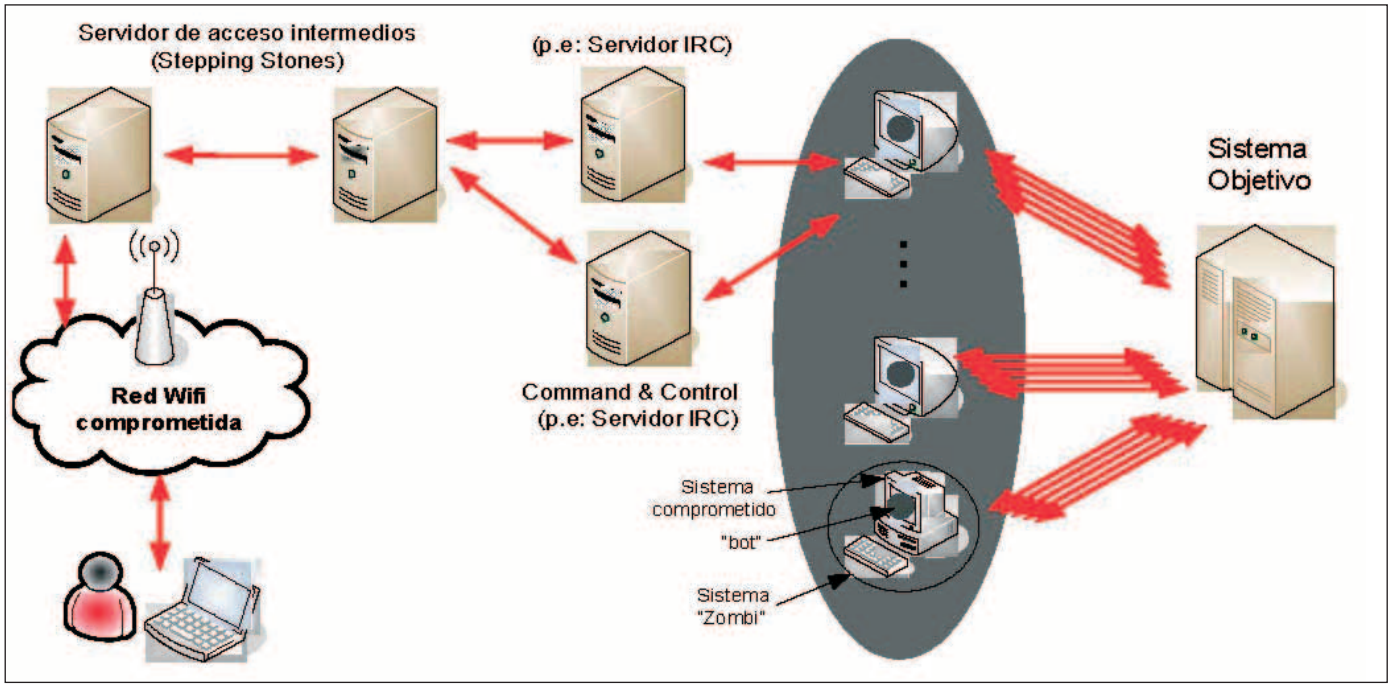
> Las vías de ataque suelen ser ataques a aplicaciones web a través de inyección de código

Como medida adicional, se "*desconectó*" el país de Internet para poder seguir usando los servicios online internos.

La peligrosidad de este tipo de ataques es creciente. Con el aumento del número de ordenadores y de la banda ancha, se crean Botnets más

USO DE BOTNETs

Command & Control BotNet



potentes. En esta perspectiva, es necesario prevenir y proteger los sistemas informáticos, invirtiendo más en infraestructura y coordinando los distintos CERTs.

Phishing

Otra clase de ataque es el *Phishing*, delito encuadrado dentro del ámbito de las estafas y que se comete mediante el uso de un tipo de ingeniería social y subterfugios técnicos, con el objetivo de adquirir información confidencial de forma fraudulenta, como puede ser una contraseña o los datos bancarios. El estafador, conocido como phisher, se hace pasar por una persona o empresa de confianza a través de correos electrónicos, mensajes instantáneos o incluso llamadas telefónicas.

El esquema básico de ingeniería social consiste en un mail diseñado para atraer a la víctima y en la creación de sitios web fraudulentos con la imagen corporativa de la entidad suplantada. A su vez, los subterfugios técnicos se encargan de dar la verosimilitud del mensaje.

Al igual que en el caso de los ataques DDoS, existe un creciente número de denuncias de incidentes relacionados con el phishing que requieren métodos adicionales de protección y de concienciación del usuario.

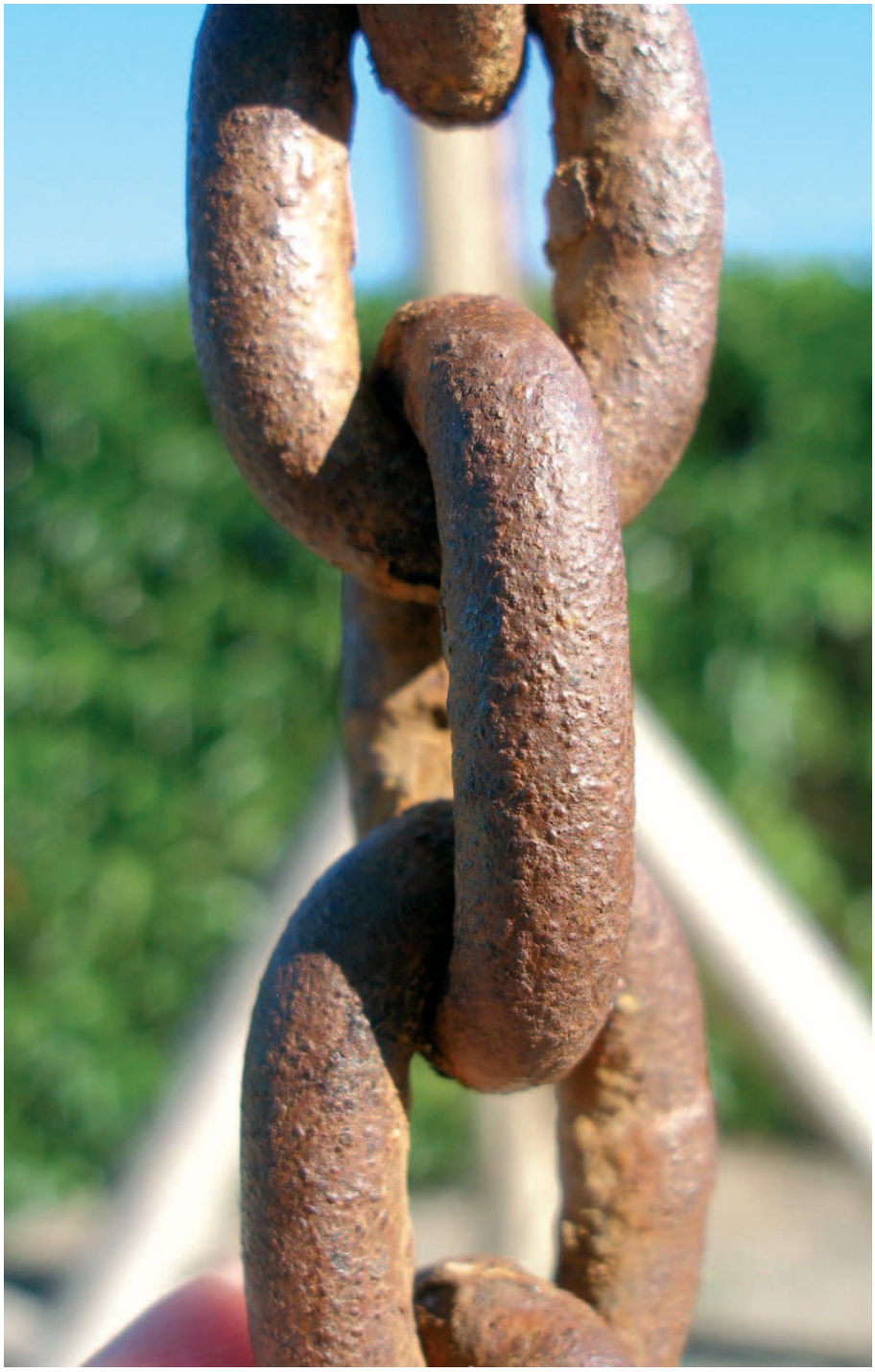
Según *Gartner*, consultora americana especializada en tecnologías, el impacto económico del *phishing* se eleva a 1.244 dólares por víctima, con una tasa de recuperación del 54%. Para el gobierno de los Estados Unidos supone un coste anual de 2.800 millones de dólares.

La preparación de un ataque phishing a través de la web comienza con la elección de una población de víctimas potenciales, investigando los servicios on-line donde existan transacciones de fondos. A continuación, el estafador construye el sitio web falso, la página de grabación de datos y el mecanismo de recogida de los mismos. También es fundamental la recopilación de bases de datos con las direcciones email de las víctimas y la elección del tema del engaño. Finalmente, se procede a enviar los emails y se espera a que las víctimas caigan en la trampa.

Claros ejemplos de *phishing* son los que se producen a través del spam contra entidades financieras u organismos públicos, como la Agencia Tributaria.

Intrusiones

Existen distintos tipos de intrusión. De esta forma, y en función de la intencionalidad del ataque, se distinguen dos tipos: dirigidos y no dirigidos. Mientras, en función del impacto del ataque podemos distinguir entre: robo de información,



defacement, *defacement* silencioso, destrucción o alteración de datos, inclusión en *Botnets* y distribución de contenido ilícito.

Un ataque dirigido consta de una serie de fases: reconocimiento (búsqueda de información sobre la empresa o sistema a atacar), escaneo de los puertos abiertos y del sistema operativo, enumeración de los servicios en ejecución, entrada al sistema (buscar vulnerabilidades en el servidor y en la aplicación web), escalada de privilegios (obtener privilegios del administrador), mantenimiento del acceso (instalar una puerta trasera para poder acceder al servidor en el futuro) y limpieza del rastro (borrado u ocultación de las pruebas de los ataques).

A su vez, los ataques no dirigidos parten de la búsqueda de una vulnerabilidad a atacar y sus fases son similares a las de los ataques dirigidos: escaneo (búsqueda de la vulnerabilidad de forma aleatoria o a través de Google), entrada al sistema (explotación de la vulnerabilidad para obtener un primer acceso), escalada de privilegios, mantenimiento del acceso (cliente IRC en *Botnets* y llamadas al Centro de Control) y limpieza del rastro.

En cuanto a las técnicas empleadas, las vías de ataque suelen ser ataques a aplicaciones web a través de inyección de código: SQL (escribir mensajes en la base de datos que luego aparece en la pantalla), Código en servidor (inyectar código PHP, ASP, Perl...) o Cross-Site Scripting (XSS, cambiar el aspecto mediante código HTML o JavaScript inyectado). También existen otras vías como ataques por fuerza bruta a contraseñas, la explotación de vulnerabilidades en los servicios, ataques vía servidores de terceros (por ejemplo, banners de publicidad) o manipulación de proxies, cachés, etc.

Ante todos estos ataques e intrusiones es imprescindible la colaboración a nivel internacional que permita saber el origen de los incidentes (otros servidores, países remotos o proveedores de acceso a Internet con poca infraestructura). Por todo ello, los Equipos de Respuesta a Incidentes, como es el caso del CCN-CERT, deben ser miembros de distintos foros internacionales como FIRST o TERENA TF-CSIRT, en donde se comparten objetivos, ideas e información sobre la seguridad de forma global.