LOS ATAQUES PASO A PASO

Los llamados Ataques Persistentes Avanzados (APT) son las ciberamenazas más temidas por gobiernos y empresas. Se trata de ataques planificados con mucho sigilo y de consecuencias terribles por lo que suponen de pérdida de información e, incluso, del control del sistema. Luis Jiménez, subdirector del Centro Criptólogico Nacional (CNN), explica cómo se llevan a cabo

ISTOCHEV / 123RF

Todos los sistemas informáticos se pueden infectar por tres razones: por estar mal configurado su sistema de seguridad, por tener un software vulnerable o porque su usuario es ingenuo y se deja engañar; por ejemplo, al abrir un e-mail infectado o al visitar una web con programas maliciosos, que no se ven a simple vista. Para garantizar su éxito, según ha explicado el subdirector del Centro Criptólogico Nacional (CCN), Luis Jiménez, en una reciente conferencia, los atacantes crean infraestructuras, con ordenadores en todo el mundo, para mantenerse ocultos y garantizar su éxito. Se ha dado el caso de ataques de 24 horas, que han enviado la información a un dominio que es borrado poco después, no dejando el más mínimo rastro del robo de información. En otros ataques, los *hackers* utilizan cientos de dominios, creados automáticamente, para recibir la información. Dominios que son borrados tras recibirla.

"Lo más preocupante de las actuales amenazas es que cada vez se detectan más las que tienen como objetivo hacerse con el control de una infraestructura -desde un banco a una central eléctrica-, más que obtener información y que, para ello, realizan una colonización silenciosa. Lo que más alarma no es lo que se va a producir, es lo que ya se está produciendo. Los ataques a infraestructuras críticas ya han comenzado, intentando infectar sus sistemas informáticos y esperando el momento adecuado. No se trata de ataques realizados de un día a otro, sino una continua labor de zapa", ha resaltado Jiménez. /J.M.V.

CÓMO SE REALIZA UN ATAQUE PERSISTENTES AVANZADO (APT)

Lo peor de este tipo de ataques es que se realizan y pueden durar incluso meses o años, sin causar alarma. Según el CCN los sectores más atacados en 2012, en España, han sido el energético, el aeroespacial, el de defensa y el farmacéutico. Así se realizan:

→ Lo primero que hace un atacante es estudiar su objetivo. Luego lanza una intrusión -enviando un correo infectado o captando al usuario a través de webs con programas maliciosos insertados-.

→ Una vez que ha conseguido infectar el ordenador, el atacante establece una puerta trasera para entrar y salir de él sin ser detectado. Además, establece mecanismos que le permiten tener privilegios en la máquina atacada. Para ello, instala herramientas con las que puede acceder a todos los archivos que le interesen -por ejemplo, recopilando los *password* de su usuario e, incluso, monitorizando su actividad-.

→ El siguiente paso consiste en colonizar la red corporativa o el resto de ordenadores con los que se relaciona el PC infectado. Conforme lo va haciendo, el atacante instala utilidades para poder optimizar su ATP, con sistemas de cifrado y protocolos de comunicaciones que le permiten pasar inadvertido. Además, 'inyecta' programas y utilidades que rastrean bases de datos obteniendo todo tipo de información. Es lo que se llama la fase de explotación.

→ Por fin, da el último paso: el de exfiltración de la información. Para ello, el atacante tiene una infraestructura bien diseñada, con servidores de mando y control repartidos por todo el mundo, para evitar ser identificado. Además, utiliza puertos normales del PC -el de navegación por Internet, el del correo, etc-, con el fin de no levantar la más mínima alarma. Además, por si no puede sacar la información a través de una máquina, durante la fase de explotación, infecta otros sistemas para utilizarlos de 'plan B'.