La economía de la ciberdelincuencia

Los países se preparan para la guerra codificada

Por David Goldman @CNNMoneyTech, 4 de agosto de 2011

LAS VEGAS (CNNMoney) - Reiterados y constantes ataques cibernéticos contra los Estados Unidos han llevado al país a evaluar las amenazas de seguridad nacional que se ciernen sobre su cabeza.

Hace tan solo cinco años, a la CIA le preocupaban sobre todo amenazas físicas tales como atentados o guerra química. Pero ahora la CIA cree que los ataques cibernéticos constituyen el segundo mayor potencial para la destrucción nacional, sólo detrás de un ataque nuclear.

"El ciberespacio será parte de cualquier conflicto futuro, ya sea con un Estado o ante el terrorismo", dijo Cofer Black, ex director del centro de contraterrorismo de la CIA en la conferencia de seguridad cibernética en Black Hat, Las Vegas, el miércoles.

No es sólo que el factor electrónico pasará a formar parte de la guerra. Ya lo ha hecho.

McAfee, una compañía de seguridad cibernética propiedad de Intel (INTC, Fortune 500), anunció el martes que descubrieron un ataque cibernético mundial de amplio alcance, que impactó a 72 organizaciones.

Un total de 36 empresas, 12 organizaciones no lucrativas y 22 organizaciones del gobierno se vieron afectadas, inclusive 15 agencias gubernamentales de Estados Unidos y de las Naciones Unidas.

La naturaleza de la amplia agresión significa que cada país y cada empresa debe dar por hecho que está comprometida, argumentó un ejecutivo de McAfee.

"No se puede implantar un *firewall,* o barrera de control de accesos, y suponer que se está a salvo", dijo Toralv Dirro, estratega de seguridad de McAfee. "De una u otra manera alguien se meterá en una computadora y atacará su sistema."

McAfee descubrió que un país patrocinó y puso en marcha un esquema de espionaje electrónico, pero no fue tan lejos como para precisar cuál fue la nación responsable. Aunque McAfee informó a las empresas y los organismos que se encontraban entre los afectados, la mayoría no quiso que la empresa de seguridad revelara sus nombres.

Cómo te asaltan los piratas informáticos

La parte más aterradora del esquema no es que impactaran a tantas organizaciones del

mundo entero, sino que durante los últimos cinco años esto siga sucediendo sin que sea detectado. Lo cierto es que McAfee descubrió el ataque cuando los piratas informáticos cometieron finalmente un error —en un servidor de comando y control dejaron rastros de sus incursiones, que McAfee descubrió en 2009.

El espionaje cibernético representa una gran amenaza, ya que pone a las naciones que auspician los ataques en ventaja en la diplomacia, la competencia empresarial y, en caso de conflicto, la guerra.

Algunos países han demostrado que los ataques cibernéticos pueden ser utilizados para mitigar las defensas rivales.

En septiembre de 2007, cazas F15 y F16 israelíes bombardearon un sitio donde Siria construía un reactor nuclear. Los radares sirios nunca registraron a los aviones que cruzaron su frontera porque Israel había intervenido el software del radar sirio.

El ejemplo más infame es Stuxnet, un virus tan sofisticado que retrasó significativamente el programa nuclear de Irán. El gusano, que probablemente se introdujo en el sistema mediante una memoria USB, puso a girar fuera de control a las centrifugadoras de una instalación nuclear iraní, destruyéndolas en última instancia. Mientras eso ocurría, Stuxnet hizo que cuantos indicadores que los ingenieros iraníes leían, dijeran que todo funcionaba con normalidad.

"Estoy aquí para decirles —y pueden citar mis palabras— que el ataque Stuxnet es el Rubicón de nuestro futuro[1] —dijo Black—. La destrucción física de un recurso nacional es enorme".

Sin embargo, podría no tratarse únicamente de naciones que un día patrocinan estos ataques. Black dijo que la capacidad de Al Qaeda para lanzar ataques físicos contra Estados Unidos ha sido neutralizada en gran medida, pero su potencial para emprender una guerra cibernética podría causar estragos en nuestros recursos.

"La inclinación natural de Al Qaeda consistiría en replegarse y entrar en el mundo cibernético", argumentó.

Aunque no es probable que otras naciones ataquen nuestros sistemas por miedo a la respuesta de los Estados Unidos, los terroristas no dudarían en hacerlo. Esa es una preocupación. Nuestro gobierno está muy mal preparado para tal eventualidad.

"Al igual que la amenaza terrorista antes del 9/11, nuestros líderes oyen hablar de esto,

1. La expresión "cruzar el Rubicón" —río del noreste de Italia— significa pasar por un punto de no retorno. Alude al ejército de Julio César, que cruzó el río en el año 49 aC. El cruce fue considerado como un acto de insurrección. Debido a que el curso del río ha cambiado mucho desde entonces, no se puede confirmar exactamente donde fluía el Rubicón cuando César y sus legiones lo cruzaron.

pero no lo creen", dijo Black a una audiencia de cerca de 8,500 *hackers* y profesionales de la seguridad. "Contamos con ustedes. La guerra codificada es la guerra de ustedes".