ieee.es
Instituto Español de Estudios Estratégicos

Documento
Informativo

56/2012 28 agosto de 2012

Mª José Caro Bejarano

DILEMA: ¿FORMAR Y RECLUTAR HACKERS?

DILEMA: ¿FORMAR Y RECLUTAR HACKERS?

Resumen:

Muchos países han aprobado o están en proceso de aprobar sus estrategias nacionales de ciberseguridad cuyo objetivo es la protección de sus redes y sistemas informáticos, así como sus infraestructuras críticas conectadas a la red. Para evitar posibles ataques en la red algunos países han optado por formar o contratar hackers como agentes informáticos. Corea del Norte ha optado por la primera y un experto de EEUU sugiere la segunda opción.

Abstract:

Many countries have approved or are in process of approving national cybersecurity strategies aimed at protecting their networks and computer systems and their critical infrastructure connected to Internet. Some countries have chosen to train or hire hackers as software agents in order to prevent possible attacks on Internet. North Korea has chosen the former option and a U.S. expert suggests the latter one.

Palabras clave:

Pirata informático, Estrategia de Ciberseguridad, ciberataques.

Keywords:

Hacker, Cyber security Strategy, cyber threats.

SE PLANTEA EL DILEMA: FORMAR Y RECLUTAR HACKERS EN LUGAR DE PERSEGUIRLOS

Muchos países han aprobado o están en proceso de aprobar sus estrategias nacionales de ciberseguridad cuyo objetivo es la protección de sus redes y sistemas informáticos, así como sus infraestructuras críticas conectadas a la red. Para evitar posibles ataques en la red algunos países han optado por formar o contratar hackers como agentes informáticos.

En el primer caso de formación de hackers se encuentra el gobierno de Corea del Sur que ha puesto en marcha un programa conocido como *Best of the best* (El mejor de los mejores) para combatir posibles ataques en la Red.

La seguridad cibernética de Corea del Sur ha sido puesta en entredicho en numerosas ocasiones en los últimos años debido a diversos ataques que han llegado a bloquear temporalmente las páginas webs de ministerios, organismos oficiales e incluso entidades bancarias.

Habitualmente el Gobierno atribuye estos ataques a *hackers* de Corea del Norte. Generalmente consisten en los conocidos como ataques de denegación de servicios distribuidos (DDoS), que sobrecargan los puntos de conexión de los servidores hasta dejarlos fuera de servicio.

El llamado DDoS ataque por Denegación de Servicio Distribuido, junto con las llamadas APTs, Amenazas Avanzadas Persistentes (Advanced Persistent Threats) son dos de los ataques que con más frecuencia se están manifestando en la red. Las conocidas como APTs consisten en un nuevo tipo de ataque organizado, se centra sobre en organizaciones internacionales, gobiernos y fuerzas de seguridad.

En el pasado mes de julio el gobierno surcoreano anunció que reclutarán y formarán a seis estudiantes *hackers* como agentes informáticos para combatir las frecuentes amenazas de seguridad cibernéticas del país, según ha informado el Ministerio de Economía y Conocimiento de Seúl.

Un grupo de expertos seleccionarán a seis *hackers* de 'sombrero blanco' (*white hat en su acepción en inglés*), una especialidad que en la jerga informática se refiere a una ética *hacker* que se centra en asegurar y proteger los sistemas y que se diferencia de la técnica 'sombrero negro' (*black hat en inglés)*, dedicada a las actividades ilegales.

El Ejecutivo surcoreano destinará al proyecto más de 1,3 millones de euros y cada uno de los alumnos seleccionados cubrirá una de las seis áreas estipuladas, que versan desde la

protección contra ataques cibernéticos a instituciones hasta la seguridad de los teléfonos inteligentes.

Durante el mes de junio, los funcionarios del gobierno surcoreano habían entrevistado a 238 piratas jóvenes altamente cualificados, todos ellos estudiantes de secundaria y posgrado, y habían seleccionado a 60, aunque solo seis llegarán a la fase final.

Los elegidos recibirán una beca de casi 14.000 euros, además de la oportunidad de estudiar en el extranjero y formar parte de la base de datos de recursos humanos de la Agencia Nacional de Inteligencia y la Policía de Corea del Sur.

El director del Instituto de Tecnología de la Información de Corea del Sur, Yoo Jun-sang, indicó al diario local Dong-a Ilbo que el Gobierno ha puesto en marcha esta iniciativa porque el país "carece de suficiente recursos humanos en seguridad" para prevenir ataques informáticos.

En el segundo caso de contratación de hackers es por lo que aboga John Arquilla[1], profesor de análisis de la defensa de la Escuela Naval de Postgrado de los EE.UU. en Monterey, California, en una entrevista concedida a The Guardian.

Según Arquilla, el gobierno de EEUU, en lugar de perseguir a los piratas informáticos de élite, debería reclutarlos para lanzar ataques cibernéticos contra los terroristas islamistas y otros enemigos.

Este destacado pensador militar y asesor del gobierno, opina que EEUU se ha quedado atrás en la carrera de cibernética y necesita establecer un "nuevo Bletchley Park" de genios informáticos y crackeadores de código para detectar, rastrear y desbaratar las redes enemigas.

El Parque Bletchley es el nombre de una mansión victoriana localizada en Buckinghamshire, Inglaterra, utilizada como instalación militar en la que se descifraron códigos alemanes durante la Segunda Guerra Mundial. En esta instalación se diseñó y construyó la primera computadora Colossus que permitió romper los códigos de la máquina alemana Enigma. El descifrado de los mensajes codificados con esta máquina permitió, según consideran algunos expertos, que la Segunda Guerra Mundial finalizara, al menos dos años antes de no contar con su descifrado.

[1] Arquilla, fue asesor del General Schwarzkopf durante la primera Guerra del Golfo y asesor del Secretario de Defensa Donald Rumsfeld durante la segunda Guerra del Golfo.

Arquilla, quien hace dos décadas acuñó el término ciberguerra, dijo que solo unos pocos hackers expertos ya han sido reclutados, pero se necesitan más. Mencionó un paralelismo con los científicos alemanes que fueron reclutados después de la Segunda Guerra Mundial, como Wernher von Braun, el mejor científico con que contaba Hitler, que se convirtió en un héroe americano tras trabajar en los cohetes y los programas espaciales de Estados Unidos.

La amenaza cibernética ya no es una exageración como era considerada por los escépticos. Una prueba de ello es que en 2011 el Pentágono dio a conocer una nueva estrategia para proteger de los hackers las redes militares y se consideró el ciberespacio como un "dominio operacional" junto con los tradicionales de tierra, mar, aire y espacio.

El gusano Stuxnet que atacó el programa nuclear de Irán mostró el verdadero potencial de lo que Arquilla calificó de "cybotage" (término que une los términos ciber y sabotaje).

El ataque cibernético, según Arquilla, era más eficaz cuando se incorpora a la estrategia militar. Rusia, dijo, fue pionera en este tipo de estrategia en agosto de 2008 durante el conflicto con Georgia.

Moscú negó haber orquestado estas ciberoperaciones, y su procedencia nunca se probó. Previamente en 2007 Estonia sufrió un ataque cibernético a sus redes informáticas y de comunicación que se considera, según algunos expertos, como el primer caso de ciberguerra. En opinión de Arquilla, "todo está aún oculto, pero los verdaderos líderes en el campo son los rusos". “China y Corea del Norte también entienden los usos estratégicos de los ataques cibernéticos".

Arquilla instó a las agencias estatales y a las empresas estadounidenses a utilizar el cifrado fuerte y computación en la nube (Cloud Computing en inglés).

Por último, acusó al Pentágono y sus dirigentes políticos de gastar miles de millones sin sentido en portaaviones, tanques y aviones a costa de aplicar una estrategia más ágil y adaptada a la realidad.

Mª José Caro Bejarano
Analista del IEEE