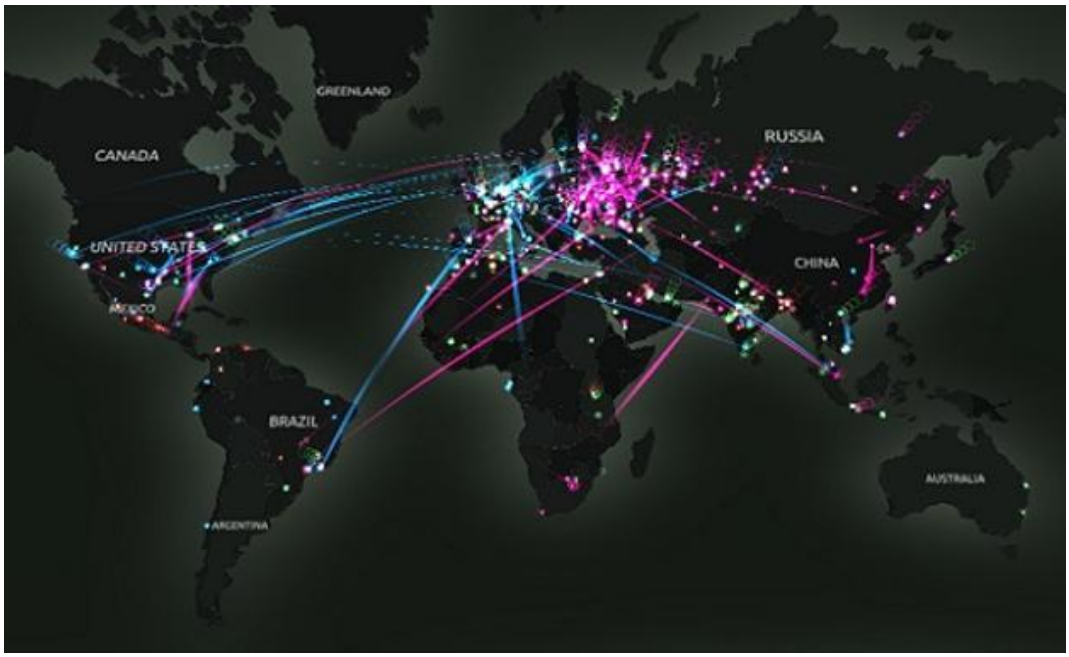
EL DIARIO VASCO

Jesús Falcón 6 agosto 2017
http://www.diariovasco.com/tecnologia/guerra-digital-20170802171800-nt.html

EL VIRUS QUE PUDO CON LOS CAÑONES

Los ciberataques crecen sin parar en número y en capacidad destructiva; hasta la misma OTAN toma cartas en el asunto.



El principal campo de batalla hoy en día no está en Oriente Medio o África, sino entre cables, chips y redes. Son guerras constantes e invisibles que de vez en cuando saltan a la arena pública debido a la evidencia de los grandes daños que provocan. Ni las multinacionales de sectores tradicionales ni las firmas que dominan el mundo digital se libran de ser víctimas de **(ciber)ladrones, (ciber)soldados o (ciber)mafiosos**. Las noticias sobre los daños causados desde el ámbito digital y los intentos por mejorar la seguridad se suceden en las últimas fechas.

El primer gran susto de este año se produjo el pasado 12 de mayo, debido a la aparición de 'WannaCry', una especie de virus especializado en secuestrar datos de los equipos infectados para pedir un rescate económico por los mismos y que afectó a más de 300.000 ordenadores de todo el mundo.

Las alarmas se encendían (si alguna vez se habían apagado) de nuevo el 27 de junio con la irrupción en miles de equipos del virus 'Petya', aún más sofisticado y potencialmente dañino que afectó al menos a 80 multinacionales. En está ocasión **el objetivo no fue tanto económico como perpretar el mayor daño posible**. Aunque tuvo poca incidencia en España, este ataque puede enmarcarse en está ciberguerra que desde hace tiempo se está dando a nivel mundial.

Virus contra cañones

«Un ciberataque puede activar el artículo cinco del tratado fundador de la Alianza, que prevé un **apoyo defensivo mutuo de los países aliados** si uno de ellos lo solicita en caso de agresión». La rotundidad del secretario general de la OTAN, Jens Stoltenberg, no deja lugar a dudas de que los daños en el ámbito digital son muy reales. Y sus consecuencias también, pues la Alianza considera ya el ámbito «ciber» como «un dominio militar» por lo que los ejércitos ya no se mueven solo en el campo terrestre, naval, aéreo y espacial. Y en este campo se halla también la **tradicional enemistad con Rusia**, fuente de todas las sospechas cada vez que saltan las alarmas.

Un ejemplo llamativo del salto de la guerra digital a la física se ha dado en Ucrania, víctima de los ataques más virulentos de los ciberguerrilleros anónimos. Hace unos días se descubría que este país **ha perdido una quinta parte de sus cañones de largo alcance D-30 debido a que había un virus** en el software que los gestiona y que revelaba su posición a los rusos. Está incipiente lucha entre códigos maliciosos y artefactos explosivos comienza a recordar a aquellas batallas en las que unos ejércitos comparecían con espadas y otros con las primeras armas de fuego.

¿Tendrán que dejar de invertir los ejércitos en aviones o misiles y apostar por los genios de la informática? Desde luego las guerras son más complejas

cuando lo primero que hay que hacer es saber con exactitud quién te ataca y desde dónde. Además, hay que moverse en espacios donde las fronteras nacionales se desdibujan y en los que la jurisdicción no está clara. Y quizá sean también más baratas y 'democráticas' pues con un simple ordenador alguien con conocimientos, ganas y capacidad puede provocar grandes daños.

Las empresas, concienciadas

Como en toda guerra, los daños económicos son un objetivo, de ahí que las instituciones y las empresas deban conocer los riesgos y aprender a defenderse. En 2016, el Incibe (Instituto Nacional de Seguridad) atendió más de 110.000 incidentes de seguridad informática, el doble que en 2015 y cinco veces más que en 2014. En este contexto se ha celebrado el pasado mes de julio **uno de los mayores ensayos de ataque informático realizados en España**, a iniciativa del organismo de ciberseguirdad ISMS Fórum con la colaboración del Centro Nacional de Inteligencia y el Departamento de Seguridad Nacional. Quince grandes empresas han tomado parte en el mismo, desde Renfe y Correos hasta el Banco Santander, Cepsa o El Corte Inglés.

Desde el nivel local al global se constata la preocupación por proteger a ciudadanos, empresas e instituciones. Así en Euskadi se ha apostado por generar conocimiento relativo a la ciberseguridad, a través de sendos centros que se ubicarán en Gipuzkoa y Álava No en vano el 70% de los ciberataques van dirigidos a pequeñas y medianas empresas.

Peor que un huracán

Los daños de los ciberataques, debido a su mayor sofisticación y poder destructivo, tienen cada vez más impacto en la economía. El estudio publicado recientemente por la aseguradora británica Lloyd's compara los eventuales daños con las pérdidas económicas que puede suponer un huracán (en una horquilla que se movería entre los 9.000 y 29.000 millones de dólares, que según las circunstancias podrían elevarse a 121.000 millones). De momento la valoración del impacto de WannaCry es de 8.000 millones de dólares. Pero esta compañía alerta de que los ciberataques podrían **aumentar hasta cien veces más en la**

próxima década. De ahí que ofrezca nuevas modalidades de pólizas para cubrir este tipo de daños.

También en dispositivos móviles

Pero las novedades que suponen en nuestra vida cotidiana este deterioro de la ciberseguridad pueden ir a más, incluso hasta nuestros bolsillos. El Centro Criptológico Nacional asegura que «se espera que durante 2017 se incrementen las campañas de ciberespionaje dirigidas a estos equipos y, en concreto, el crecimiento del 'ransomware', **troyanos bancarios y herramientas de monitorización y acceso remoto**; son probables ataques directamente contra las infraestructuras del sistema de pagos electrónico, así como la comercialización de estos ataques mediante servicios del tipo Crime-as-a-service». Estos ataques se basan en el principio de que **el agresor respetará un contrato tácito con la víctima**.

El 'Informe de Ciberamenazas y Tendencias' de este organismo advierte también de que el ciberespionaje se mantendrá muy activo este año 2017, "ya sea como parte de las operaciones de inteligencia de un Estado o dirigido por grupos organizados que proporcionarán servicios o buscarán información de interés y la podrán a la venta". La única certeza es, por lo tanto, que más tarde o temprano veremos nuevos ataques de alcance. La duda, si seremos capaz de minimizar sus daños.