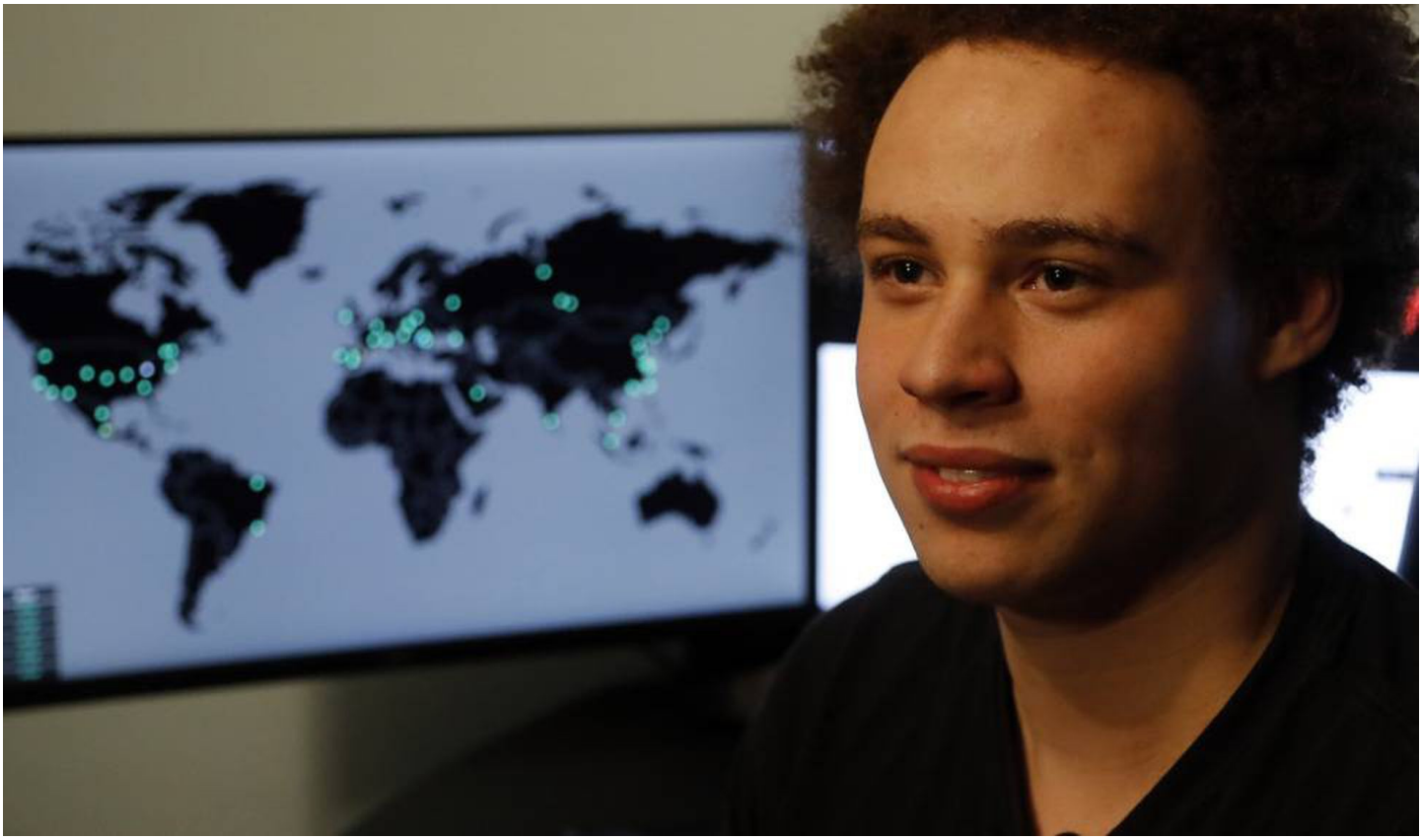
TRIBUNA

La guerra del siglo XXI

Hay que gastar en seguridad informática tanto como se invierte en la física

GLORIA LOMANA

17 MAY 2017 - 19:25 CEST



Marcus Hutchis, el experto británico que frenó el reciente ataque digital.
FRANK AUGSTEIN (AP)

En menos de una semana el término *malware* ha pasado a formar parte de nuestras vidas. El virus digital que desde el viernes ha desencadenado el mayor cibertataque de la historia no solo ha puesto en solfa a medio mundo infectando los ordenadores, sino que ha alertado sobre lo que nos espera, las nuevas formas de delincuencia y guerra del siglo XXI. Por la red, estos virus corren más rápido que la vieja pólvora. Para la ficción quedarán la guerra con pistolas de *Solo ante el peligro,* las espadas de *El señor de los anillos* o los cañones de *El día más largo.*El presente es digital.

De la gravedad de lo sucedido es preciso tomar lecciones. La primera, saber si el cibersecuestro de datos venía solo o escondía otros propósitos. El más ligero podría ser un daño industrial para robar contratos o patentes a otros países; pero nunca habría de descartarse el propósito de generar el caos para dañar a la inteligencia del adversario con un desorden masivo. El mundo del espionaje, evidentemente, es más virtuoso que un *007* de ficción y en este nivel de competencia lo mismo podría darse un catastrófico error de las agencias americanas, que la habilidad de Putin para incrustarle *hackers* negros a la NSA y culparle del ataque, que el mismo juego a la inversa. Dando por hecho que en el próximo embrollo jugarán también los chinos.

Otros artículos de la autora

hackers empotrados en el partido demócrata y ahora en los archivos de Macron. De este episodio conocemos incluso el nombre de la primera persona que lo propagó, un ultraderechista de Estados Unidos que opera en el este de Europa. La primera reacción de Hollande fue como la de Obama, prometer una "dura respuesta al ataque". Pero la pregunta es: ¿Con qué ley responder y cómo a igual escala? Las respuestas diplomáticas y comerciales tienen impacto cero sobre el atacante, lo que nos debería llevar a la alarma y al trabajo imperioso de protegernos para responder con réplicas contundentes. El aviso del último viernes no es baladí: hay dos grandes operadores informáticos en el mundo, Microsoft y Apple, y el ataque a uno de ellos ha generado el caos mundial.

Es cierto que, antes de esta gigantesca amenaza, los gobiernos y servicios secretos de los Estados punteros en inteligencia ya estaban trabajando. Nuestro CNI cuenta con grandes expertos en su Centro Criptológico Nacional y, hace ya dos años, España cambió la Ley de Enjuiciamiento Criminal para que el juez pueda autorizar el uso de troyanos por la Red con el fin de interceptar posibles ataques. Pero la realidad va al galope, por delante de leyes e incluso de la formación de los jueces y fiscales. ¿Cómo enjuiciar a un *hacker* si el juez desconoce no solo sus habilidades, sino incluso su lenguaje? ¿Qué legislación aplicar si ningún organismo internacional ha sido capaz de interpretar lo que está sucediendo? ¿Podría la OTAN sancionar a Rusia si hubiera interferido en algún país miembro, como EE UU o Francia? Claramente, no. Es la hora de rearmarse, de que Europa piense en términos de futuro, que ya son presente, y que trabaje en programas de *software* o aplicaciones derivadas. El mundo entero depende de Microsoft, Apple y, de modo incipiente, del abierto Linux. Es de suponer que los chinos ya han tomado nota de lo sucedido.

Hay que gastar en seguridad informática tanto como se invierte en seguridad física

Entretanto, en nuestra vida cotidiana hemos de esperar ciberataques a baja escala de cámaras, sensores, puertas, relojes inteligentes, sistemas de coches o robos de poca monta, similares a los que, en los años noventa, nos sacaban quinientas pesetas a punta de navaja.

Aunque también, escuchando a los expertos, uno se tranquiliza porque los dos más temibles objetivos, la navegación aérea y las centrales nucleares, están extremadamente protegidos. Garantizan que no habrá un 11-S electrónico. Pero quienes así hablan también pronostican que el punto de inflexión no será hasta que todo se deteriore tanto que haga reaccionar a la sociedad entera. Y se conmine a gastar en seguridad informática tanto como se invierte en la física. Y se obligue a los fabricantes a evitar la vulnerabilidad de los sistemas, del mismo modo que la industria del automóvil desarrolló seguridad tras cien años de muertes.

Gloria Lomana es periodista, analista política y premio Fedepe 2016 (Federación de Mujeres Directivas y Ejecutivas).

ARCHIVADO EN

Opinión · Malware · Investigaciones Cibernéticas · Seguridad internet · Software · Internet · Informática · Empresas · Telecomunicaciones · Economía · Industria · Comunicaciones