El fracaso de la ciberreserva

El impacto que causó el Wannacry a empresas españolas tuvo una respuesta política a los pocos días que se concretó en la necesidad de crear un ciberejército

El pasado año, la aparición y el impacto que causó el malware Wannacry a empresas españolas, entre ellas Telefónica, tuvo una respuesta política a los pocos días que se concretó en la necesidad de crear un ciberejército con más de 2000 hackers. Esta idea fue evolucionando hasta el concepto de "ciberreserva" en donde se reclutaría a hackers que trabajarían gratis por su patria.

No hace mucho algunos medios comunicaban las dificultades del Ministerio de Defensa de seguir adelante del con el plan de crear la ciberreserva. Si bien el Gobierno tiene muy claro que el ciberespionaje, ataques dirigidos a instituciones gubernamentales o la infección masiva de ordenadores por medio de malware, son prioridad nacional, la arriesgada idea del Ministerio de Defensa de crear una reserva de hackers "voluntarios" se queda sin el apoyo de los mismos.

La razón es muy clara: no hay presupuesto para mantener una reserva digital, por lo que los expertos tendrán que prestar sus servicios sin remuneración, de forma

voluntaria. Esta situación hizo que muchos especialistas en ciberseguridad que en algún momento pensaron en alistarse en la ciberreserva y participar de esta apuesta del Ministerio de Defensa dejaran de considerar la propuesta.

La realidad

A día de hoy ninguna empresa está libre de un ciberataque, sea grande, pequeña o un trabajador autónomo. Por otro lado, no hay que olvidar que España encabeza la lista de los países que más ciberataques recibe. Sin embargo, el general de División Carlos Gómez López de Medina, jefe del Mando Conjunto de Ciberdefensa (MCCD), ha vuelto a afirmar, esta vez en la última edición de la RootedCon celebrada en Madrid frente a más de mil especialistas en ciberseguridad, que en ningún momento se plantea pagar ningún tipo de sueldo o recompensa económica. Por este motivo se les llama "voluntarios". La respuesta del auditorio fue clara y contundente: "Si nada vais a dar, nada vais a obtener".

Cuesta creer que la ministra de Defensa, siendo consciente de la gravedad y la necesidad de contar con ciberexpertos, no destine fondos para la creación de este ciberejército. Por otro lado, países como Estados Unidos, Rusia, China, Corea del Norte y Alemania destinan cientos de millones de euros para esta causa.

El talento

La palabra talento tiene muchas interpretaciones, según la RAE lo define como: "Especial capacidad intelectual o aptitud que una persona tiene para aprender las cosas con facilidad o para desarrollar con mucha habilidad una actividad."

En el campo de la ciberseguridad se suele hablar de talento, por el grado de especialidad que debe tener un individuo en un campo "nuevo" que no obedece en muchas ocasiones a habilidades obtenidas por una formación reglada. Es decir, los mejores expertos en ciberseguridad son autodidactas entre otras cosas porque hace apenas 4 años atrás apenas se hablaba de conceptos como hacking ético o máster en ciberseguridad en las Universidades españolas.

El gobierno español con esta postura, no puede competir con el sector privado que está pagando nóminas de 30.000€ a 75000€ e incluso más a expertos en ciberseguridad. Ahora mismo las empresas del sector están hambrientas de talento, por lo que el proyecto de ciberreserva tiene poco o ningún atractivo para los verdaderos expertos en ciberseguridad.

La profesionalización del cibercrimen

Las empresas desconocen el nivel de profesionalización y complejidad que puede encerrar un archivo de menos de 700 Kb.

Los cibercriminales son ciberexpertos profesionales, con muy buenas remuneraciones e integrantes de equipos de desarrollo con más de 30 miembros, muchos más empleados de los que tienen el 93% de las empresas españolas. Trabajan de forma descentralizada y pueden llegar a ganar entre 50000 a más de 100000€ al año.

El cibercrimen está mejor organizado, es modular, multidisciplinar y cuenta con ingresos millonarios. Además, cuenta con un sistema de anonimato que hace muy difícil llegar hasta los cabecillas de la organización. Esta capa de anonimato y forma descentralizada hace que sea casi imposible desmantelar estas organizaciones, creando un halo de seguridad a quienes trabajan de forma anónima para estas mafias.

Sin lugar a dudas, es una batalla desigual donde España, una vez más, se queda a la cola por falta de inversión, como en otros campos como el I+D+i. Tendremos que esperar la llegada de un Wanacry2 con un efecto similar al primero para que el Gobierno vuelva a evaluar y a tomar conciencia de que es un riesgo que está ahí, aunque que no se vea o se sienta, pero que cuando golpea, golpea fuerte y sin dar segundas oportunidades.

Artículo realizado por la empresa experta en seguridad Dolbuck S.L.