El equipo español operó desde la base de Retamares, en Madrid, distribuidos en trece células de capacidades.

FUEGO CRUZADO EN LA RED

Más de 3.000 militares y civiles de 38 países participan en el ejercicio de ciberdefensa *Locked Shields 23* de la OTAN

EL fluido eléctrico no llega a gran parte de los hogares porque la principal planta termoeléctrica de generación de gas del país no funciona con normalidad. Sin embargo, los indicadores de suministro de energía muestran lo contrario. Están siendo falseados. La red de telecomunicaciones 5G ha sido saboteada y afecta principalmente a las Fuerzas Armadas. Sus sistemas de mando y control a través de la red de propósito general WanPG no responden. Pero aún hay más: el Banco Central tiene bloqueado su sistema de transacciones internacionales, se suceden los intentos de transferencias fraudulentas y proliferan las cuentas de criptomonedas sospechosas. La comunicación satélite ha caído y, por tanto, la defensa aérea nacional y el control de fronteras están en riesgo...

Eran las ocho y media del pasado 19 de abril, cuando la mayoría de la población todavía se desperezaba sacudiéndose el sueño. «A esa hora, teníamos el *bicho* dentro y comenzaba a dar la cara», declara el cabo Luis Alfaro Rovira desde la base de Retamares, en Madrid, donde ejerce como experimentado administrador del sistema operativo Windows destinado en el Mando Conjunto del Ciberespacio (MCCE). «*Malware*, *backdoors*, *defacement web*, *phising*…». El comandante Manuel Gutiérrez de la Mata, destinado en el Grupo de Defensa de la Fuerza de Operaciones del MCCE, pone nombre a los vectores cibernéticos que miden el potencial destructivo del *bicho* al que se refiere en tono coloquial el cabo Rovira. El día 18, uno antes del inicio de las hostilidades y del comienzo propiamente dicho del ejercicio *Locked Shields 23*, los agentes maliciosos comenzaron a ser lanzados por un grupo de *hackers* desde Tallín, sede del Centro de Excelencia de Defensa Cibernética Cooperativa de la OTAN, organizador del evento. El objetivo de los intrusos era reconocer, atacar, comprometer y degradar el funcionamiento de las infraestructuras críticas y los sistemas de telecomunicaciones de un ficticio país aliado. Durante las siguientes 48 horas, hasta el 20 de abril, especialistas civiles y militares respondieron a estas amenazas en el ciberespacio, considerado el quinto dominio del enfrentamiento militar, junto al terrestre, naval, aéreo y espacial.

El ejercicio *Locked Shields* representa el nivel de adiestramiento más complejo, realista y demandante del mundo por la magnitud del incidente cibernético simulado a gran escala que recrea. Es un ejercicio diseñado para poner en jaque prácticamente a todos los servicios esenciales de los ciudadanos de un país: su energía, economía, comunicaciones, seguridad, salud, transporte y un largo etcétera.

En la edición de este año han participado más de 3.000 militares y civiles de 38 países, procedentes tanto del sector público como del privado y del ámbito empresarial y universitario. La mayoría lo hicieron distribuidos en 24 equipos de respuesta rápida, denominados *blue teams* por la organización del evento. Estos grupos de especialistas en ciberdefensa hicieron frente, cada uno desde su país de origen, a más de 7.000 ataques

Se lanzaron más de 7.000 ataques simulados para degradar las infraestructuras y los sistemas de comunicación

programados de manera global. «Aproximadamente, 300 incidentes por equipo», especifica el comandante de la Mata, jefe del *blue team* español. «Los *hackers* encuadrados en el *red team* intentaron, y en ocasiones lo consiguieron, penetrar en nuestras máquinas: alrededor de 330 sistemas informáticos como ordenadores, servidores o web. Lo hicieron de manera ilegítima, tras encontrar sus puertas traseras [los puntos vulnerables] introduciendo virus y códigos maliciosos a la espera de ser detonados», añade el comandante de la Mata.

Los objetivos de los atacantes eran dañar las estaciones de trabajo o los servidores, extraer información, suplantar identidades de dominio, secuestrar los protocolos de comunicación en redes o interrumpir el normal funcionamiento de las estaciones de trabajo. En función de este escenario técnico se formó un equipo mixto compuesto por alrededor de 172 profesionales. Entre ellos, militares del Ejército de Tierra, de la Armada y del Ejército del Aire y del Espacio, del Estado Mayor de la Defensa y el Órgano Central, agentes de la Policía Nacional y de la Guardia Civil y personal civil del Instituto Nacional de Ciberseguridad (INCIBE), de Ingeniería de Sistemas para la Defensa de España (ISDEFE), del Departamento de Seguridad Nacional, de la Oficina de Coordinación de Ciberseguridad del Ministerio del Interior y del Banco de España. Todos ellos trabajaron coordinados con ingenieros y técnicos de empresas del sector privado, como Telefónica, Siemens, Indra, o Iberdrola, de diversas entidades bancarias, firmas que prestan servicios de monitorización en el ámbito de la ciberseguridad, otras dedicadas a la comunicación y los asuntos públicos y, por último, docentes y alumnos de diferentes universidades españolas.

Sin despliegue de contingentes militares sobre el terreno y sin disparar un solo tiro, la batalla silenciosa en la que participa el *blue team* español tenía lugar a golpe de ratón y teclado en una enorme sala de operaciones bunquerizada y computarizada en la base de Retamares, a casi 4.000 kilómetros del supuesto país agredido. Los combates eran una suerte de fuego cruzado entre virus, gusanos, troyanos, *spyware*, *rookit*, *adware*, *ransomware* y otros muchos códigos y programas maliciosos frente a «nuestras contramedidas», como define el comandante de la Mata al conjunto de herramientas empleadas por el *blue team* bajo su mando. Se trata de antivirus y *scripts* o fragmentos de códigos que incluyen instrucciones para ejecutar diferentes funciones en un programa, en este caso, defensivas y contraofensivas.

En la sala de operaciones la vestimenta civil se entremezclaba con la uniformidad militar en cada una de las trece células diseñadas según las capacidades que aportaban para la defensa de los sistemas de control industrial —los que gestionan la planta generadora de gas—, del banco central, de la red 5G y de comunicaciones por voz IP, los sistemas operativos Windows y Linux y web. También se diseñó una célula de Redes o *Networking* y *Firewalls* y otra de monitorización de los sistemas informáticos. Además, se constituyó una unidad de Inteligencia y *Reporting*, donde se registraban, analizaban y podían consultarse todos los incidentes y las soluciones a los mismos.

Militares del Ejército de Tierra, de la Armada y del Ejército del Aire y del Espacio monitorizan la red tras una incidencia.

OTRAS INCIDENCIAS

Desde Tallín, también se plantearon incidencias, como los volcados o copias de discos duros de ordenadores y servidores para su análisis por parte del equipo de forenses del *blue team* para comprobar si habían sido manipulados. Además, se cubrieron los aspectos legales que conllevan las acciones ciber, para lo que se contó con miembros de la Fiscalía de Madrid y del Cuerpo Jurídico Militar del MCCE y delmundo universditario. Y, por último, un equipo de comunicación estratégica analizó el falso relato ofrecido por el enemigo, y otro de especialistas en medios de comunicación de masas se encargó de trasmitir la verdad de los hechos a los ciudadanos intoxicados por las *face news*.

Una pantalla gigante refleja en la sala, a modo de semáforo, el estado operativo de los sistemas informáticos comprometidos en el combate cibernético, el único aspecto visible que ofrece la *zona gris*, gentileza de los organizadores del *Locked Shields* para que los *cyberwarriors* dispongan de una visión en tiempo real de los resultados de la monitorización del escenario virtualizado en el que navegan. El color verde indica que los equipos están disponibles; en amarillo, que presentan algún problema y en rojo, no funcionan. «En este ejercicio lo importante es comprobar cómo actúan, reaccionan y colaboran entre sí los sistemas sometidos a un enorme estrés», señala Jesús Cámara, técnico de Telefónica I+D integrado en la célula 5G. «Parar todos los ataques, según está planteado el ejercicio, es muy complicado».

J.L. Expósito
Fotos: Pepe Díaz