1. LAS MÚLTIPLES ARISTAS DE LOS CIBERATAQUES, ANTESALA DE LA GUERRA HÍBRIDA

EN LA REUNIÓN DEL G20 CELEBRADA EN julio en Hamburgo, el presidente de EEUU Donald Trump coincidió con su homólogo ruso Vladimir Putin en un clima de máxima expectación tras reconocer el mandatario estadounidense la posible incidencia rusa en las elecciones de noviembre. La presunta incidencia consistió en el robo de información de correos electrónicos del Partido Demócrata y su publicación a través de Wikileaks, lo que pudo ayudar a que Trump ganara las elecciones. Tras su reunión con Putin, el mandatario americano desveló, vía Twitter, la voluntad de ambos de crear una unidad de ciberinteligencia para hacer frente a futuros *hackeos* electorales.

Se trata de un extraño clima diplomático en el que un agresor es, a su vez, un potencial socio y colaborador. Por si fuera poco, un ataque informático con robo de información termina teniendo un impacto electoral en la mayor potencia mundial. El ambiente enrarecido se amplifica en el momento en el que un *software* malicioso con la apariencia de *ransomware* —bloqueo de equipo y solicitud de una cantidad de dinero como rescate para su desencriptación— como el caso del virus *NotPetya*, que se propagó el 27 de junio, parece esconder detrás un sabotaje al sector económico de un país como Ucrania. Sin embargo todos estos factores responden a un único *modus operandi*: la guerra híbrida.

Este concepto fue acuñado por la OTAN en 2014 para denominar la actuación de Rusia en el conflicto con Ucrania. Javier Candau, jefe del departamento de Ciberseguridad del Centro Criptológico Nacional (CCN), servicio dependiente del Centro Nacional de Inteligencia (CNI), describe la guerra híbrida como la "operación dirigida por un Estado que utiliza tácticas abiertas y encubiertas con el objetivo de desestabilizar otros estados y polarizar a la población civil. Incluye una gran variedad de herramientas como la diplomacia, las acciones de inteligencia tradicionales, actos subversivos y de sabotaje, influencia política y económica, instrumentalización del crimen organizado, operaciones psicológicas, propaganda, desinformación y ciberataques".

En 2015, el CNI contabilizó 430 incidentes calificados como de peligrosidad muy alta y crítica. El año pasado la cifra se incrementó un 44%

EN ESTE ECOSISTEMA 'HÍBRIDO', LOS los ciberataques se están convirtiendo en un vector con cada vez más peso en los conflictos entre países y amenazas en auge para el sector empresarial. Adolfo Hernández es subdirector y cofundador de Thiber, *think tank* creado en 2013 especializado en el estudio y el fomento de la ciberprotección y que elabora los boletines mensuales de Ciber Elcano. Hernández calcula que tres cuartas partes de los ataques informáticos tienen una motivación económica. "Esta vertiente criminal focaliza los ataques en un tipo de víctima y de incidente. Cuando se puede descartar la motivación económica y se trata de una motivación política, ideológica o religiosa entramos en otra vertiente que da más miedo", valora Hernández. El CNI a través del CCN-CERT gestiona los cibe-

La OTAN acuñó hace tres años el término guerra híbrida a un tipo de conflicto larvado en el que unas potencias tratan de desestabilizar a otros estados a través de todo tipo de estrategias de influencia. Uno de los principales ejes de estas nuevas operaciones son los ciberataques, ya sean a través de robo de información de partidos políticos y su publicación con el fin de influir en el voto de los electores, o por medio de sabotajes cibernéticos a infraestructuras críticas. En España, de hecho, este último tipo de incidentes no deja de crecer. Los virus 'ransomware' que, en principio, parecen tener un móvil económico no se escapan de la sospecha de que detrás puede haber una motivación política, algo que ha quedado patente con el virus NotPetya. A pesar de que, de momento, el terrorismo no parece disponer de la infraestructura técnica necesaria para llevar a cabo un cibersabotaje, lo cierto es que los yihadistas han mostrado ser expertos en el cuestionable arte de la captación, radicalización y financiación a través de las redes sociales. Mientras, el cibercrimen, considerado el negocio ilícito más rentable, por delante del tráfico de drogas, representa el 75% de los ataques. POR LUIS ALBERTO ÁLVAREZ

rincidentes que tienen que ver con las instituciones públicas (Administración central, comunidades autónomas y ayuntamientos) así como en el sector de las empresas públicas. En 2016 gestionó 20.940 ciberincidentes.

El responsable del departamento de Ciberseguridad del CCN estima que para 2017 se alcanzarán los 24.000 incidentes gestionados, en torno a un 15% más. "Es un crecimiento alto aunque también hemos mejorado los sistemas de detección. Lo que más nos preocupa son los ataques tipificados como de peligrosidad muy alta y críticos".

SE CONTABILIZARON 430 INCIDENTES EN estas dos categorías en 2015, mientras que el año pasado se incrementó la cifra un 44%, hasta los 620. "Los incidentes críticos son los que han hecho mucho daño y no han transcendido. Nuestra principal preocupación son los ataques esponsorizados por estados, lo que llamamos ciberespionaje. Su cometido es robar información e intentar pasar desapercibidos. También hemos sufrido alguna denegación de servicio [DoS, en sus siglas en inglés] importante", reconoce Javier Candau.

"WannaCry pudo ser una prueba de fuego que pretendía camuflarse bajo una máscara de chapuza extrema", asegura un experto en seguridad informática

La herramienta preferida por los atacantes en materia de ciberespionaje son las Amenazas Persistentes Avanzadas (APT, en sus siglas en inglés). "Son procesos silenciosos que se introducen en equipos y redes de víctimas para tener acceso durante un periodo largo de tiempo a sus recursos y datos", explica Jorge SoydelBierzo, pseudónimo de un experto en seguridad informática (soydelbierzo.com).

Para responder a los incidentes que sufren las administraciones y el sector público, el CCN-CERT cuenta con tres niveles. El primero es el que se conoce como Sistema de Alerta Temprana, que consiste en una serie de sensores instalados en las máquinas de los organismos. El segundo, formado por una veintena de expertos en ciberseguridad, es el que forma el Grupo de Ataques Complejos. El equipo forense y de ingeniería inversa compone el tercer nivel: se dedica a analizar equipos infectados.

A las pocas horas de descubrirse el virus *WannaCry* el pasado 12 de mayo, el CCN desarrolló una vacuna, bautizada como *NoMoreCry,* que permitía que los equipos conectados a una red en la que alguna máquina ya estuviera infectada engañaban al *malware* haciéndolo creer que éstos ya lo estaban. Gobiernos como el belga lo implementaron para prevenir la propagación entre los organismos públicos de aquel país.

Otras acciones alarmantes que se pueden llevar a cabo son los cibersabotajes, especialmente si van dirigidos a infraestructuras críticas. Uno de los más conocidos fue el ataque por parte de Rusia al oleoducto georgiano Baku-Tbilisi-Ceyhan en 2008 a través de un DoS.

UN CASO SONADO FUE EL 'MALWARE' denominado Stuxnet, un virus a modo de gusano que infectó la central nuclear de Natanz, en Irán, en 2010. *The New York Times* atribuyó su auto-

1 LAS MÚLTIPLES ARISTAS DE LOS CIBERATAQUES, ANTESALA DE LA GUERRA HÍBRIDA

Terminales infectados por 'NotPetya' en un supermercado de Ucrania.

ría a un ataque coordinado por los servicios secretos de EEUU e Israel. En diciembre de 2014 el virus BlackEnergy dejó sin luz a 80.000 hogares ucranianos en un sabotaje informático a centrales eléctricas del país. Todas las sospechas apuntaron a Rusia.

"¿QUIÉNES TIENEN CAPACIDAD PARA LANZA-zar un ataque de estas características? Las tres potencias de *Champions* [Candau prefiere no dar nombres]. Los demás países, no. Por ejemplo, no creo que Corea del Norte tenga capacidad para colapsar Internet", comenta el jefe de Ciberseguridad del CCN.

En España, el número de incidentes en infraestructuras críticas se ha multiplicado exponencialmente, pasando de 63 en 2014 a 134 en 2015, 479 en 2016 y 432 solo en el primer semestre de este año. "Hay una tendencia a doblar cada año el número de incidentes que gestionamos, lo cual nos da una idea de la velocidad a la que avanza la amenaza", destaca Fernando Sánchez, director del Centro Nacional de Protección de Infraestructuras Críticas (Cnpic). El catálogo que componen las infraestructuras críticas está compuesto por más de 3.500 instalaciones dentro de áreas estratégicas como energía, transporte, agua, salud o el sistema financiero, entre otros.

"Debemos prestar más atención a los sistemas de control industrial, dado que es en este tipo de entornos donde un ciberataque podría provocar afectaciones en el ámbito físico de una forma directa", comenta Sánchez. Los operadores que se encuentren en el catálogo de infraestructuras críticas tienen una serie de obligaciones que pasan por desarrollar un plan que contemple la política de seguridad integral de la organización, así como otro de protección específico para cada una de las instalaciones del catálogo bajo su responsabilidad.

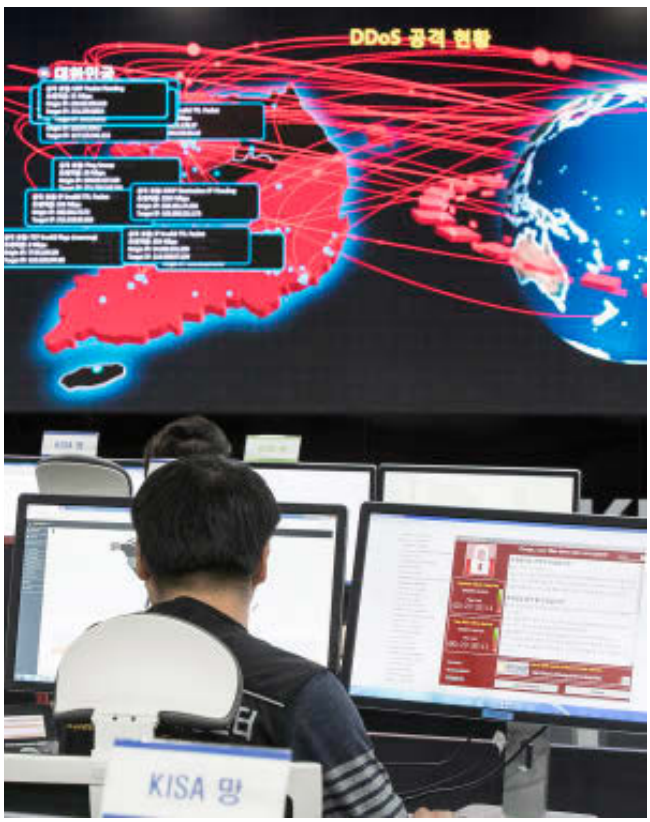
EL CIBERTERRORISMO ES UNA DE LAS mayores preocupaciones en lo que a infraestructuras críticas se refiere. Se trata de una amenaza real, hasta el punto de que tanto Europol como las Fuerzas y Cuerpos de Seguridad del Estado cuentan con unidades específicas para combatirlo. Ahora bien, hasta el momento el terrorismo internacional no ha realizado ninguna acción de cibersabotaje, salvo un apagón aislado en la televisión francesa TV5Monde en 2015 y algún *hackeo* en webs institucionales. "Se han centrado, sobre todo el ISIS, en el uso de las redes sociales para la captación, radicalización y financiación del terrorismo. ¿Es eso ciberterrorismo? Para mí, sí", considera Adolfo Hernández.

Pero si hay una palabra que hace estremecer hoy a la opinión pública esa es *ransomware*, popularizado recientemente por los ataques *WannaCry* o *NotPetya*. A pesar de ser un viejo conocido —muchos lectores recordarán los virus de la Policía, de Correos o, más recientemente, el de la factura de Endesa, el salto cualitativo de nuevos ataques es que no se basan en lo que se conoce por ingeniería social. Este concepto suele consistir en que el usuario recibe un correo electrónico, lo abre y se descarga un archivo adjunto que propaga el virus en el terminal. En cambio, *WannaCry* y *NotPetya* se distribuían sin modificar la voluntad del usuario. "Estos dos últimos ataques se hacen especialmente virulentos por el uso de Eternalblue, una vulnerabilidad en SMBv1 [protocolo de red de los equipos que permite compartir archivos e impresoras] por la cual puede distribuirse en red e infectar lo máximo posible. Por lo tanto, no son sólo *ransomware* sino también gusanos",

1 LAS MÚLTIPLES ARISTAS DE LOS CIBERATAQUES, ANTESALA DE LA GUERRA HÍBRIDA

explica Fernando Díaz, *malware analyst* de Hispasec.

La hibridez de los nuevos ataques se constata por el hecho de que tanto *WannaCry* como *NotPetya* incluían código sustraído por el grupo de *hackers* The Shadow Brokers nada menos que a la Agencia de Seguridad Nacional de EEUU (NSA) el pasado año. La secuencia de los hechos es la siguiente: la NSA conoce la vulnerabilidad en los equipos Windows desde 2013. El *hackeo* a la NSA ocurre en 2016. La NSA tarda meses desde la sustracción de datos hasta comunicar a Microsoft la vulnerabilidad y la multinacional americana anuncia en marzo de este año una actualización que parchea dicha vulnerabilidad. Un mes después The Shadow Broker hace pública la brecha de seguridad. Y 30 días después aparece el ataque de *WannaCry*.



Operarios de la Agencia de Internet y Seguridad de Corea del Sur (KISA) realizan un seguimiento en tiempo real de la propagación de 'WannaCry'.

Todo esto lleva a pensar a expertos como Jorge SoydelBierzo que tal como estaba hecho *WannaCry* "o era un test de laboratorio que se le fue de las manos a quien lo estuviese haciendo o realmente era una prueba de fuego que pretendía camuflarse bajo una máscara de chapuza extrema". El resultado es que el virus, que pedía un rescate de 300 dólares en bitcoins, infectó a más de 250.000 equipos de todo el mundo, afectando a multinacionales españolas como Telefónica, así como a los servicios de urgencias de varios hospitales del servicio público de salud británico.

DETRÁS DE LA 'MUTACIÓN' DE ESTOS *malware* puede incluso haber algo más allá de un acto cibercriminal, remitiendo de nuevo a la guerra híbrida. Algo que suscribe el propio director del Cnpic. "En la mayoría de los casos es difícil dilucidar cuál es el objetivo final de un incidente de ciberseguridad. Incluso en aquellos en los que aparentemente se busca un móvil económico es difícil determinar que no sea sólo un punto de partida para un ataque más complejo. Los atacantes podrían utilizar otro tipo de vulnerabilidades para expandirse por la red de la organización, mantenerse ocultos y llevar a cabo acciones diferenciadas, como el robo o manipulación de la información", dice Sánchez.

En el caso de *NotPetya*, el hecho de que el paciente cero fuera una empresa ucraniana que desarrolla un *software* para el pago de impuestos, que utilizan muchas compañías de aquel país, deja entrever que el móvil no era económico. Cuanto más, por el hecho de que el objetivo de *NotPetya* era más bien borrar los archivos del terminal infectado (*wiper*, en el *argot* técnico) más que la solicitud de un rescate (*ransomware*). De hecho, la OTAN se planteó este ciberataque como un posible acto de guerra.

El cibercrimen representa el 75% de los incidentes globales. En España el Instituto Nacional de Ciberseguridad (Incibe) contabilizó 115.237 ataques de este tipo dirigidos tanto a empresas como a particulares. "Las situaciones más frecuentes están relacionadas con intentos de acceso a los sistemas, en especial a través de *ransomware*; sistemas comprometidos por *botnets*, es decir, *malware* que se utiliza para robar información e infectar a otros equipos hasta que son descubiertos; e incidentes relacionados con el fraude, como por ejemplo intentos de robo de cuentas de correo y credenciales para el acceso a redes sociales, con el fin de obtener dinero ilícitamente", comenta José María Lassalle, secretario de Estado para la Sociedad de la Información y la Agenda Digital. Para hacer frente a este desafío el Incibe cuenta con un presupuesto de 23,2 millones de euros, 2,7 millones más que en 2016.

EN LA ÚLTIMA MEMORIA DE LA Fiscalía del Estado en 2015 se contabilizaron 22.575 procedimientos judiciales incoados como delitos informáticos. El 76% se tipificó como estafa. Los delitos de daños informáticos sólo representaron 295 casos. "El *ransomware* se califica como estafa pero tiene más que ver con daños informáticos", asegura David Maeztu, socio en Abanlex.

Según la policía, los principales vectores de ataque hacia los particulares son el correo electrónico con archivos infectados, así como la visita a páginas web con mucha publicidad, especialmente de descargas y pornográficas, que pueden contener lo que se denomina *malvertising*, cuya finalidad es infectar un terminal sin necesidad de hacer clic en su enlace.

"Los delincuentes se sirven de la ingeniería social para atacar a la ciudadanía, por ello el principal consejo que daría sería usar el sentido común. En cuanto a las empresas, las aconsejaría que cuenten con soluciones profesionales en ciberseguridad y que inviertan en recursos e información", comenta un inspector del Grupo de Seguridad Lógica de la Unidad de Investigación Tecnológica de la Policía Nacional.

Un ataque tan mediático como el de *WannaCry* o *NotPetya* se hubiera evitado o, al menos, mitigado con una política de actualizaciones y de copias de seguridad (*backup*) periódicas. Jorge SoydelBierzo recomienda al sector empresarial que realicen al menos un *backup* diario.