EL LUGAR MÁS PELIGROSO DEL CIBERESPACIO

Enrique CUBEIRO CABELLO
Jefe de Operaciones del Mando Conjunto de Ciberdefensa

Introducción

CIBERESPACIO, ciberdefensa, ciberseguridad, ciberconflicto, ciberguerra, cibersoldados, *i-war*… son términos que cada vez con más frecuencia aparecen relacionados con el ámbito militar. Muchos analistas expresan su convencimiento de que los conflictos del futuro se iniciarán y acabarán en el ciberespacio. Y es que la amenaza «cíber» ya no es algo de ciencia-ficción, sino del propio pasado. Valgan como ejemplos el masivo ciberataque sufrido por Estonia en el año 2007, el conflicto entre Georgia y Rusia en Osetia del Sur (2008) o el asunto Stuxnet (2010).

Con la sensación de abordar el problema con mucho retraso, prácticamente todas las organizaciones militares del mundo están tratando de buscar cómo encajar el denominado «quinto dominio» (*the fith warfare domain*) en sus estrategias nacionales de defensa, en su orgánica y, lo más difícil de todo, en su proceso de planeamiento operativo. En paralelo, sesudos juristas discuten sobre la forma de extender el derecho de la guerra al nuevo dominio, buscando la forma de trasladar conceptos tales como «acto hostil», «autodefensa», «respuesta proporcionada» o «uso de la fuerza» al ciberespacio o de acomodar el famoso artículo 5 del Tratado del Atlántico Norte a este ambiguo territorio (1).

---

(1) Art. 5.°: Las Partes convienen en que un ataque armado contra una o varias de ellas, ocurrido en Europa o en América del Norte, será considerado como un ataque dirigido contra todas, y, en consecuencia, convienen en que si tal ataque se produce, cada una de ellas, en el ejercicio del derecho de legítima defensa, individual o colectiva, reconocido por el art. 51 de la Carta de las Naciones Unidas, asistirá a la Parte o Partes atacadas tomando individualmente, y de acuerdo con las otras, las medidas que juzgue necesarias, comprendido el empleo de las fuerzas armadas para restablecer la seguridad en la región del Atlántico Norte.

Emblema del Mando Conjunto de Ciberdefensa (MCCD).

En lo que se refiere a la respuesta orgánica, España ha dado ya un primer y decidido paso con la reciente creación del Mando Conjunto de Ciberdefensa (MCCD), ubicado en la madrileña base de Retamares y que alcanzó su IOC (*Initial Operational Capability*) en septiembre de 2013.

Entre los cometidos del MCCD, que se detallan en la O. M. 10/2013, están el de garantizar el libre acceso al ciberespacio y la disponibilidad, integridad y confidencialidad de la información y de las redes y sistemas de su responsabilidad; el de obtener, analizar y explotar la información sobre ciberataques e incidentes en esas mismas redes y sistemas; el de ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional; el de ejercer la representación del Ministerio de Defensa en materia de ciberdefensa militar en el ámbito nacional e internacional, y el de definir, dirigir y coordinar la concienciación, la formación y el adiestramiento especializado en materia de ciberdefensa.

Cualquier lector, incluso aquel sin demasiados conocimientos en la materia, se habrá dado cuenta tanto de la importancia como de la dificultad de las tareas que esta nueva unidad, relativamente pequeña y aún casi en pañales, tiene que afrontar.

Y todo ello en un ámbito en el que las cosas giran a enorme velocidad y donde cualquier documento, plan o procedimiento que tenga más de doce meses adquiere una apariencia tan obsoleta como si estuviera escrito con tinta y pluma sobre un raído pergamino.

En este contexto, quizás lo que voy a afirmar resulte sorprendente para muchos lectores, dada la aparente complejidad y trascendencia de la gran mayoría de los cometidos mencionados. Pues bien, en mi opinión, de todos ellos, ninguno resultará tan decisivo para potenciar nuestra capacidad de ciberdefensa como *la concienciación*. Concienciación que, en el fondo, no supone otra cosa que inculcar, profundamente y en cada miembro de la organización, el convencimiento de que *ciberdefensa somos todos*.

Cartel del Ejercicio de Ciberdefensa 2013, dirigido por el MCCD.

Para apoyar esta aseveración (y, quizás de paso, modificar algún mal hábito y, en consecuencia, reducir algún «ciberriesgo» potencial) he preparado algunos ejemplos ilustrativos. Ejemplos que van avanzando en complejidad, que protagonizan desde usuarios de lo más corrientes hasta autoridades con elevadas responsabilidades, y que, aunque inventados expresamente para este artículo (2), creo que presentan situaciones que pueden ocurrir perfectamente en cualquier momento, o que hasta puede que hayan ocurrido ya en un formato similar. Y no debemos olvidar que la realidad casi siempre acaba por superar a la ficción.

Ciberdefensa somos todos

Caso 1: «el doc se abre con el nombre de tu perro»

Comentario introductorio: a nadie escapa que la progresiva aceleración de los acontecimientos está llevando a una forma de trabajo cada vez más reactiva. Si esto es aplicable a cualquier organización, alcanza su máxima expresión

(2) Tarea en la que he contado con el inestimable apoyo de mis muy competentes compañeros del Mando Conjunto de Ciberdefensa.

en los estados mayores militares. Planes, informes, mociones, solicitudes y oficios se elaboran casi siempre con premura y son tareas en las que, en muchas ocasiones, han de intervenir diversos organismos, a través de sus correspondientes POC o representantes. Tampoco a nadie escapa que urgencia y seguridad chocan en infinidad de ocasiones. Por otra parte, y esto es extensivo a la mayoría de casos planteados en este artículo, nunca como ahora se dieron unas condiciones tan favorables para explotar lo que se denomina «ingeniería social» (3).

(Correo electrónico remitido a través de la Red de Propósito General por el capitán de fragata Incauto, de la División de Planes del E. M. Conjunto de Sildavia al teniente coronel Asfixiado de la División de Planes del E. M. del Ejército de Sildavia).

ASTO: MUY URGENTE.
ARCHIVOS ADJUNTOS:
EstrategiaNacionaldeCiberdefensa_draft_v02.docx
TEXTO: Querido Juan, necesito que me remitas ASAP vuestras observaciones al borrador adjunto. Mi Jefe lo tiene que presentar mañana y aún tenemos que preparar el power point. *Te lo paso por esta vía porque tenemos pegas con el Sistema Seguro de Mensajería. He protegido el doc. Para abrirlo, introduce el nombre de tu perro en minúsculas. Haz lo mismo con lo que me devuelvas, porque se supone que es reservado. Recuerdos a Carmen. Un fuerte abrazo. Paco.*

A mil doscientos kilómetros de allí, el capitán Malvado, del Servicio Militar de Inteligencia de Borduria, interceptaba el correo, aprovechando el implante *stealth* que una empleada (de origen bordurio y perteneciente a la subcontrata encargada de la limpieza de los despachos del Cuartel General del E. M. Conjunto de Sildavia) había insertado dos meses antes en la CPU del capitán de fragata Incauto, tras ser instruida por un agente bordurio y recibir un primer pago de 5.000 *slotzs* en billetes pequeños. Tras introducir en *Google* «Juan Asfixiado», localizó un perfil de *Facebook*, en el que penetró con mucha facilidad. A los pocos minutos, encontró una fotografía en la que aparecía la hija del teniente coronel Asfixiado con un cachorro. La foto estaba etiquetada «Marta con Toby». Tras hacer doble *click* en el icono del archivo

(3) En seguridad informática, se denomina ingeniería social a la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos y, en general, a toda técnica utilizada para obtener información, acceso o privilegios en sistemas informáticos que permitan realizar algún acto que perjudique o exponga a la persona u organismo comprometido a riesgo o abusos. El principio que sustenta la ingeniería social es el de que en cualquier sistema los usuarios son el eslabón más débil.

EstrategiaNacionaldeCiberdefensa_draft_v02.docx, introdujo «toby» cuando el programa le pidió la contraseña.

Caso 2: la contraseña en el postit

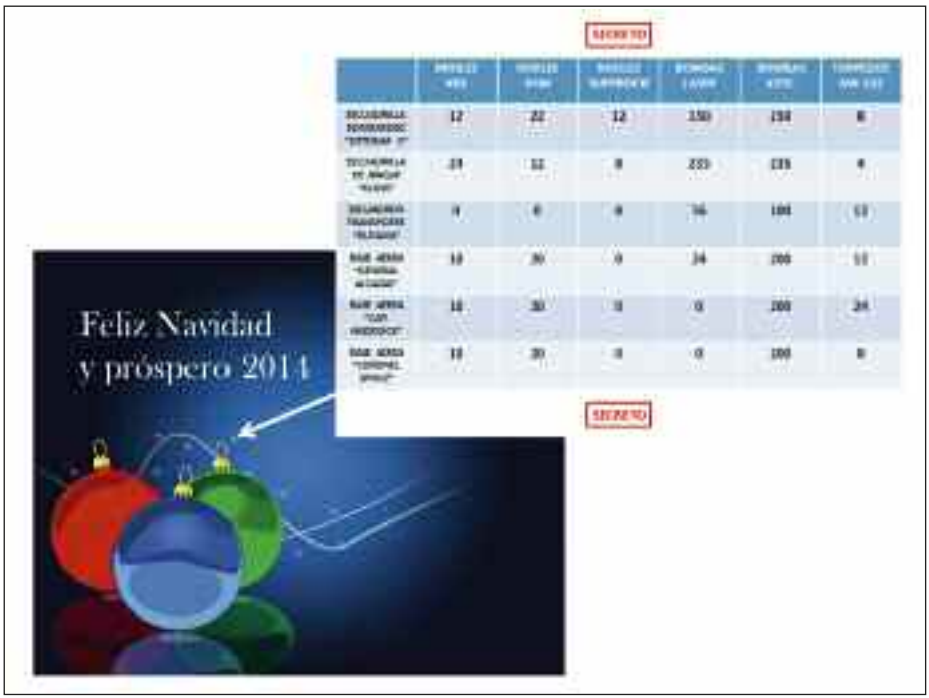
Comentario previo: Las contraseñas de acceso son una necesidad incómoda. Por desgracia, un muy elevado porcentaje de usuarios las considera únicamente una molestia. El hecho de que necesitemos varias, que cada una requiera un elevado número de caracteres (combinando letras, números y signos especiales) y el que haya que cambiarlas cada cierto tiempo complica aún más las cosas.

El sargento Confiado, destinado en la Sección de Logística del Cuartel General de la Fuerza Aérea, ubicado en la base de Klow (Sildavia), arrancó su ordenador, esperó pacientemente a que las ventanitas emergentes (que informaban de cosas, para él incomprensibles, acerca de *pluggins* y *addins*) dejaran de aparecer e introdujo su código de «usuario» en la ventana de inicio de sesión en *Windows*. A continuación, tecleó *Password_005* y vio con desagrado cómo aparecía un mensaje de «contraseña incorrecta», invitándole a probar de nuevo. Sacudió la cabeza y tecleó esta vez *Password_006*. La sesión se inició normalmente. Se disponía a revisar su correo electrónico, cuando apareció

otra ventana emergente: «Su contraseña caduca en 15 días. Haga *click* aquí para cambiarla». Pocas cosas irritaban tanto al sargento Confiado como ese anuncio. «Pero si la he cambiado hace nada —pensó— y justo ahora que empezaba a saberme la nueva de memoria». Muy molesto hizo *click* en «descartar» y repitió la misma operación en las mañanas siguientes, hasta que llegó el día en que la ventana emergente indicó que la contraseña actual caducaba al día siguiente. Con un suspiro de resignación, el sargento fue siguiendo los pasos hasta establecer la nueva contraseña: *Password_007*.

Como de costumbre, incorporó la nueva clave al documento de *Word* cuyo icono ocupaba la esquina superior izquierda del escritorio, archivado con el nombre «claves.docx». Por si acaso, también como de costumbre, escribió la nueva clave en un *postit* amarillo, lo enrolló como un canuto y lo depositó en la jarra con el escudo de la escuadrilla «Ottokar V» que utilizaba para los lápices y los bolígrafos, no sin antes extraer el *postit* con la clave anterior, hacer con él una pelotilla y tirarlo a la papelera.

A las 1807, cerca de una hora después de que el sargento Confiado cerrara la puerta de su despacho para irse a su casa, penetraba en él el soldado Avispado, que se encontraba de guardia, usando la llave maestra. Hacía cerca de tres



Ocultación de un archivo clasificado en una fotografía mediante técnicas de esteganografía.

años que Avispado había sido reclutado por un agente bordurio (que le ofreció, como primer pago por sus futuros servicios, liquidar las importantes deudas de juego que el soldado había contraído con una casa de apuestas *on line*). Desde entonces, Avispado llevaba 33 meses consecutivos montando guardia de seguridad en el Cuartel General los días 5 o 6 de cada mes, sin que nadie se hubiese percatado de aquella extrañísima coincidencia. Una vez dentro, el soldado cerró la puerta del despacho y, tratando de hacer el menor ruido posible, pulsó el botón de *on* de la CPU.

Apenas cinco minutos más tarde (dos más de lo habitual, que fue lo que tardó en advertir el cambio de clave de *Password_006* a *Password_007)*, copiaba en un *pendrive* las tablas de *Excel* archivadas en C:/LOGISTICA/EXISTENCIAS_MUNICION/2013/SEP que el sargento Ingenuo había elaborado a partir de los datos recibidos de todas las unidades de la Fuerza Aérea y que, como todos los meses, no más tarde del día 5, tenía que volcar en la aplicación LOGMUN, a fin de actualizar las bases de datos que gestionaba la División de Logística del Estado Mayor del Ejército del Aire de Sildavia, que ocupaba el ala norte del cuarto sótano del Cuartel General Aéreo.

A la mañana siguiente, nada más salir de guardia, el soldado Avispado remitía los archivos desde un cibercafé a una cuenta de correo electrónico de la Inteligencia borduria, enmascarándolos en unas fotografías, aparentemente anodinas, empleando técnicas de esteganografía (4).

Caso 3: el pendrive *regalado*

Comentario introductorio: no es nada raro que las delegaciones militares reciban algún tipo de obsequio con motivo de visitas oficiales a otros países. Pues bien, cada vez es más frecuente que esos obsequios sean algún tipo de dispositivo electrónico; son muy comunes los *pendrives* (son muy baratos, prácticos y se pueden personalizar fácilmente con emblemas o logos), pero cuando el visitante es de alto rango también pueden llegar a ser cosas más caras y atractivas, como PDA, tabletas o móviles. A pesar del conocido riesgo que eso entraña, está demostrado que lo primero que uno hace al recibir un *pendrive*, venga de donde venga, es introducirlo en el puerto USB de su ordenador personal. Recientemente, ha habido alguna noticia llamativa al respecto (por ejemplo, los *pendrives*

(4) La esteganografía (del griego *στεγανος* (*steganos*): cubierto u oculto, y *γραφος* (*graphos*): escritura) es la parte de la criptología en la que se estudian y aplican técnicas que permiten el ocultamiento de mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia. Es decir, se trata de ocultar mensajes dentro de otros y de esta forma establecer un canal encubierto de comunicación, de modo que el propio acto de la comunicación pase inadvertido para observadores que tienen acceso a ese canal.

regalados por el presidente Putin a los mandatarios en la cumbre del G-20), que demuestra claramente la validez de ese principio inmutable que dice: «en Inteligencia no hay países amigos o enemigos; únicamente, otros países».

El capitán de navío Ingenuo encendió el ordenador de su despacho, introdujo la clave «1111» para acceder a su sesión y sacó de su bolsillo el bonito *pendrive* con forma de llavero, forrado en piel, con el escudo del Estado Mayor de la Defensa en relieve, que le habían regalado en su reciente visita oficial a Borduria. El antivirus no saltó. El capitán de navío no creía que los bordurios fueran tan audaces como para introducir un virus en un *pendrive* y regalárselo a continuación al jefe de la Sección CIS del E. M. de la Flota de Sildavia. Clicó sobre el icono de «Mi PC», accedió a la unidad F y, con el botón derecho del ratón, marcó «Propiedades». Observó con alborozo que el *pendrive* era de 16 gigas; más exactamente, 15.988.654.988 *bytes*. Como no se fiaba del todo, su siguiente paso fue formatear el *pendrive*. En ningún momento observó que en la unidad existía una partición oculta de apenas un centenar de *Kbytes*.

Durante los días siguientes, utilizó habitualmente el *pendrive* para trabajar en el borrador del Plan de Operaciones de la Flota, documento clasificado que tenía que estar listo antes del 10 de octubre para su posterior aprobación por el almirante. Tenía apenas una semana, por lo que cada día se lo llevaba a casa para seguir avanzando.

A las 1200 del día 7 de octubre, jueves, Día Nacional de Borduria, el fichero autoejecutable, contenido en la partición oculta del *pendrive*, insertó un troyano en el disco duro del ordenador del capitán de navío, aprovechando una vulnerabilidad «día 0» en el sistema operativo *Doors XP Service Pack 4*. Desde ese día, desde el Centro de Inteligencia Naval de Borduria, ubicado en Szohôd, se tuvo acceso al disco duro, unidades extraíbles y cuentas de correo electrónico del ordenador infectado, hasta que una actualización del antivirus de la red corporativa detectó la existencia del troyano, 456 días después.

Algo más tardó en producirse la detección en el ordenador particular del capitán de navío, pues la compañía fabricante del antivirus que tenía instalado en los tres ordenadores de casa (el más barato de los habilitados para tres licencias que encontró en el centro comercial) incorporó el troyano a su base de datos cerca de un año después, permitiendo a la Inteligencia Naval borduria obtener profusa información acerca de algunos aspectos bastante oscuros de la vida del capitán de navío Ingenuo que podían ser explotados en el futuro, mediante la vieja, pero siempre efectiva, técnica del chantaje.

Caso 4: el hardware *«de riesgo»*

Comentario previo: la incorporación de elementos COTS al mundo militar es algo cada vez más habitual en todos los ámbitos, pero es en los campos de

la electrónica y la informática donde su proliferación alcanza unas proporciones más altas. La rapidísima evolución y los costes que llevaría aparejado su minucioso estudio obligan a adquirir productos comerciales sin las debidas garantías de seguridad. Esto no solo afecta al *software*, sino también —y esto es menos sabido— al *hardware*, y muy en particular a aquel que incluye componentes fabricados en determinados países.

El general Receloso, jefe del Apoyo Logístico del Ejército de Sildavia, había adquirido cierta «ciberparanoia» tras asistir a un seminario sobre ciberseguridad, impartido para altos mandos de las Fuerzas Armadas.

Desde entonces, había adoptado algunos hábitos, como revisar cada mañana los puertos de su equipo informático en busca de posibles *keyloggers* (5), analizar con el antivirus todos los documentos anexos recibidos por el correo electrónico corporativo, independientemente de su origen, y apagar el *smartphone* antes de entrar en un local reservado.

Una mañana, durante el *briefing* diario con los jefes de los diferentes departamentos de la jefatura, la conversación derivó hacia los controles de calidad a los que eran sometidos los diferentes repuestos y suministros para las Fuerzas Armadas. Su sorpresa fue notable cuando se enteró de que el proceso de control de calidad de los equipos informáticos y de infraestructura de red empleados en las redes clasificadas y de mando y control no contemplaba el *tampering* (6).

Uno de sus subordinados, que procedía de la División CIS del Estado Mayor Conjunto, señaló que, cuando desde la División se propuso incluir ese requisito en la contratación de suministros electrónicos, cuya adquisición para la totalidad de las Fuerzas Armadas sildavas se había centralizado en la Dirección General de Infraestructuras, la propuesta fue rechazada. Al parecer, el grupo de trabajo que se creó para su valoración (grupo con perfil «contable», en el que no había ningún representante con conocimientos de ciberseguridad) la consideró innecesaria, además de inviable por falta de recurso económico.

Muy preocupado, pues era bien conocido que la práctica totalidad del equipamiento informático era fabricado en la vecina Borduria (donde, por razones de economía de coste, se ubicaban la mayor parte de las plantas de producción de las grandes multinacionales de la electrónica de consumo), el general Receloso ordenó al subdirector de Ingeniería llevar a cabo, con la mayor urgencia, un análisis técnico para identificar posibles vulnerabilidades *hardware* en equipos y sistemas.

---

(5) Los *keyloggers* son dispositivos o aplicaciones que registran las pulsaciones del teclado con el fin de obtener información de la víctima: contraseñas, códigos de acceso a cuentas bancarias, documentos en redacción, etcétera.

(6) Modificación intencionada de un producto de forma que este puede resultar dañino para el usuario.

La tarea fue finalmente asignada al comandante Ingeniero Capaz, auténtica institución en las Fuerzas Armadas sildavas, cuya sobrada competencia en asuntos de informática forense era bien conocida.

El resultado de la exhaustiva y meticulosa investigación que, durante dieciséis semanas, llevó a cabo su equipo de analistas no dejó lugar a dudas: un elevado porcentaje del *hardware* instalado en las redes, tanto clasificadas como de propósito general, disponían de puertas traseras que permitían su administración remota e incluso la captura sistemática del tráfico. Aunque no había forma de demostrarlo, había fundadas sospechas de que, a través de esas vulnerabilidades, agentes del gobierno bordurio podían estar llevando a cabo, de manera sistemática, la exfiltración de información, y que podían tener, incluso, la capacidad potencial de interrumpir el servicio de las redes de comunicaciones sildavas en un momento dado. En resumen, se podía decir que el conjunto de redes y sistemas de mando y control sildavo era, muy probablemente, un conglomerado de *botnets* en manos de los bordurios.

Caso 5: el responsable CIS saturado y el usuario irresponsable

Comentario previo: la continua ampliación de cometidos de las secciones CIS no siempre va aparejada del correspondiente refuerzo de sus plantillas. Como en tantos otros ámbitos, muy poca gente tiene que hacer demasiadas cosas. Esto lleva a que, en muchas ocasiones, la prioridad de las tareas no se asigne en función de su importancia, sino de su urgencia, lo que repercute negativamente en la seguridad.

El capitán de corbeta Agobiado llevaba seis meses destinado en la sección CIS del Cuartel General de la Marina sildava en Klow y nunca en su vida profesional se había sentido tan superado por los acontecimientos. Su carpeta de «Asuntos Pendientes» engrosaba cada mañana, y desde el primer día tenía la sensación de no tener control alguno sobre su jornada laboral. Aquella mañana pretendía, una vez más, llevar a cabo la inspección del nodo de la Red de Propósito General del Cuartel General, que llevaba semanas teniendo que posponer. Pero, sin haber acomodado aún sus posaderas en el sillón de su despacho, el teléfono comenzó a sonar:

—Capitán de corbeta Agobiado, sección CIS. Buenos días.

—Buenos días, Carlos. Soy el coronel Correveidile. Necesito que mandes a alguien urgentemente al despacho del almirante de Estrategia porque tiene algún tipo de problema con su ordenador.

—Enterado, mi coronel. Me pongo a ello.

Con un suspiro de impotencia, Agobiado volvió a arrepentirse de haber permitido a su único suboficial en plantilla inscribirse en el Curso Avanzado

de Gestión STIC, con cuatro semanas de fase presencial. Cuando no eran los «problemillas» de los almirantes y capitanes de navío con sus ordenadores; eran las altas, bajas y renovaciones de las acreditaciones de usuarios, los cortes de suministro eléctrico o los inventarios de material CIS. La inspección del nodo tendría que esperar un poco más. Y, en algún momento, tenía que encontrar un hueco para instalar los parches del sistema operativo y actualizar el antivirus corporativo, operaciones que normalmente ejecutaba su suboficial y que hacía ya tres semanas que no se llevaban a cabo. Se levantó, cerró la puerta con llave y salió por el pasillo, con andar cansino, hacia el despacho del almirante.

Siete plantas más abajo, en el cuarto sótano, el alférez de navío Despreocupado conectaba, como hacía cada día desde que lo compró, su *smartphone* de última generación a uno de los puertos USB de su ordenador personal, lo que le evitaba tener que llevar consigo al trabajo el único cargador de que disponía y que compartía con su compañero de piso. Estaba muy orgulloso de su móvil, que tenía repleto de aplicaciones gratuitas descargadas de *Play Store,* que se actualizaban automáticamente, y para el que había contratado una tarifa *Premium* sin límite de descargas.

El dispositivo se había convertido en algo imprescindible en su vida diaria, hasta el punto que no concebía cómo había podido subsistir sin él en el pasado. Lo utilizaba como GPS, como despertador, para hacer gestiones bancarias, para intercambiar correo electrónico, para chatear, para hacer fotos y vídeos, para navegar por Internet, para escuchar música, como agenda, como libro electrónico, para jugar a todo tipo de juegos, para hacer la compra *on line*, como linterna… y, a veces, hasta como teléfono.

Era totalmente ignorante de las muchas vulnerabilidades que había ido introduciendo en el dispositivo; es más, lo consideraba completamente a salvo tras incorporar a su panoplia de aplicaciones un antivirus gratuito, específicamente diseñado para dispositivos *Androide*, que estaba valorado con cinco estrellas en *Play Store*. En ningún momento se percató de que, a través de una de las actualizaciones automáticas de una de las aplicaciones gratuitas, el teléfono había sido infectado por un *malware* tipo *botnet,* cuya existencia acababa de ser descubierta por la empresa responsable del antivirus corporativo e incorporada a la última actualización. Este *software* malicioso, diseñado por una organización criminal con el objetivo de obtener información susceptible de ser vendida en el mercado negro, infectaba dispositivos móviles que trabajaban con el sistema operativo *Androide 3.0* y de ahí podía propagarse a sistemas con sistema operativo *Doors* que no estuvieran actualizados con los últimos parches.

Nada más conectar el *smartphone* al puerto USB de su ordenador, el *malware* empezó a actuar. Encontrando terreno abonado, dado que el sistema operativo estaba sin parchear y el antivirus sin actualizar, el *malware* comenzó a propagarse de forma sigilosa en el sistema, accediendo a las carpetas de

documentación en red y a las diferentes bases de datos que se iba encontrando. Una vez localizada la documentación, esta era fraccionada y enviada en diferentes intervalos de tiempo a través del protocolo *http* a una dirección IP de una famosa ONG situada en otro continente. Esta comunicación requería un salto satélite, por lo que la información no solo la recibía la dirección IP de destino, sino que cualquiera que se encontrara en la huella del satélite se convertía en un receptor potencial.

Al día siguiente, y sin que fuera detectado por los responsables de seguridad de la información de la Marina sildava, cuantiosa información sensible de la organización estaba a la venta al mejor postor en la *deep web*.

Examen de comprobación

Con todo lo visto, creo que cualquier lector está ya en condiciones de contestar a la pregunta a la que lleva directamente el título de este artículo: ¿dónde se ubica el lugar más peligroso del ciberespacio? Y estas son las opciones de respuesta que les planteo:

— En Borduria.
— En el Mando Conjunto de Ciberdefensa.
— Entre el teclado y la silla.
— Todas las anteriores son ciertas.

En efecto, la respuesta es la tercera.

BIBLIOGRAFÍA

Tratado del Atlántico Norte.
VV. AA.: *Ciberespacio, nuevo escenario de confrontación*. Monografías CESEDEN. Núm. 126. Febrero 2012.
VV. AA.: *Ciberseguridad. Retos y Amenazas de la Seguridad Nacional en el Ciberespacio*. Instituto Español de Estudios Estratégicos. Diciembre 2010.
HOOD, Andrew; ANDRESS, Jason, y WINTERFELD, Steve: *Cyber Warfare*. Syngress, 2011.
KLIMBURG, Alexander (Ed.): *National Cyber Security Framework Manual*. NATO CCD COE Publication. Tallinn 2012.
GUERRA SOTO, Mario (teniente de navío): *Ciberconflicto, una amenaza real,* 2012.
Mandiant Report. APT1. Exposing One of China's Cyber Espionage Units, 2013.
GÓMEZ LÓPEZ, Julio: *Guía de Campo de Hackers*.
PICOUTO RAMOS, Fernando: *Hacking y Seguridad en Internet*.
BEAVER, Kevin, y DAVIS, Peter: *T. Hacking wireless networks*.
Angelucho. X1red+segura, 2013.
Wikipedia. Varios artículos.