CAPÍTULO TERCERO

EL CIBERESPACIO Y EL CRIMEN ORGANIZADO

EL CIBERESPACIO Y EL CRIMEN ORGANIZADO

JUAN SALOM CLOTET

RESUMEN

El increíble auge de las nuevas tecnologías ha supuesto un cambio en las relaciones e interacciones de la sociedad actual, donde usuarios, legisladores y gobiernos no acaban de vislumbrar la forma de ordenar la pacífica y libre existencia.

Por el contrario, el delincuente sí se ha amoldado rápidamente a ese nuevo escenario, aprovechando las ventajas de las deficiencias legislativas y del nuevo espacio jurídico. Su adaptación ha sido tal que se ha procurado un espacio de impunidad, que ha supuesto un efecto llamada para la delincuencia. Han desembarcado, de la mano de los expertos informáticos o hackers, con toda su fuerza, abriéndose paso las formas más avanzadas de la delincuencia, las bandas organizadas.

Palabras clave: Cibercrimen, ciberespacio, ciberpolicía, delito informático, incultura digital, paraíso informático, hacker, hacking, cracker, script kiddie, lammers, pirata informático, troyanos, caballo de troya, rootkit, código dañino, phishing, phisher, carding, skimming, scrow, pharming, vishing, smishing, CaaS, mulas, scam 419.

CYBERSPACE AND ORGANIZED CRIME

ABSTRACT

The incredible rise of new technologies has brought about changes in the relationships and interactions of today´s society, where users, le-

gislators and governments are not able to envision how to manage the peaceful and free existence.

On the other hand, offenders have quickly adapted themselves to this new situation, taking advantage of the weaknesses of the new legislation and legal framework. Their adaptation has been such that it has raised a space of impunity, which has been a knock-on effect for the crime. Organized gangs, the most evolved form of crime, have landed with all their force, and with the help of computer experts and hackers have pushed through the Internet.

Key words: Cybercrimen, cyberspace, ciberpolice, cibercrime, digital illiteracy, data haven, hacker, hacking, cracker, script kiddie, lammers, trojan, trojan horse, rootkit, malware, phishing, phisher, carding, skimming, scrow, pharming, vishing, smishing, CaaS, mules, scam 419.

INTRODUCCIÓN

El enorme desarrollo de las Nuevas Tecnologías, la informática y las telecomunicaciones, y especialmente el efecto sinérgico entre ambas, está suponiendo un cambio trascendental en la sociedad. Trabajo, economía, administración y ocio son algunos de los aspectos que están variando a pasos agigantados, dirigiéndonos hacia esa sociedad cada vez más global, en la que la esfera de influencia supera nuestro entorno mediato, y lo que ocurre en nuestras antípodas ya forma parte de nuestras circunstancias. En este nuevo modelo social, al que hemos bautizado como Sociedad de la Información, juega un papel determinante Internet como vehículo de transmisión e intercambio de todo tipo de información (1), produciéndose una sinécdoque entre la parte y el todo, Internet por Sociedad de la Información.

Internet, la red de redes, es factor determinante de la globalización cultural y, en especial, de los mercados, diseñando nuevos escenarios socioeconómicos. Sin ir más lejos, el comercio electrónico (*e-commerce*), abre un escenario de potenciales mercados internacionales, inima-

(1) Ver introducción de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).

ginables para los actuales modelos de pequeñas empresas, que traerán consigo el desarrollo de servicios complementarios de transporte y precisarán de un esfuerzo imaginativo por parte de la administración para el control de la actividad fiscal.

La implantación de esta sociedad, que parece no conocer otro límite que la imaginación humana, puede incluso hacer tambalear los propios fundamentos del Estado y de la concepción actual del sistema democrático, dando paso quizá a una democracia electrónica (2) con la ya probada experiencia del voto electrónico, en la que cabría una participación que superara la simple elección de representantes para llegar a la toma de decisiones de forma cotidiana y directa por parte del ciudadano.

Estas situaciones reflejadas no son más que simples conjeturas de lo que esta Sociedad de la Información puede traer consigo, además del ya indiscutido incremento de la calidad de vida, apoyado en el desarrollo tecnológico.

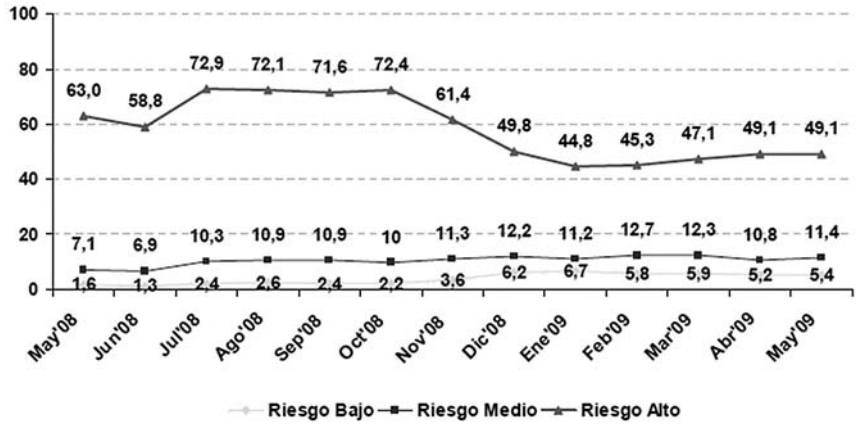
Por otro lado, Internet está vivo, está en un proceso de crecimiento imparable, tanto en servicios como en usuarios, afectando cada vez más a nuestra forma de vida. En la red proyectamos nuestro trabajo, es nuestro escenario de ocio, de comunicación, de negocio, en ella nos movemos, compramos, buscamos información y depositamos nuestra intimidad y privacidad, nuestra vida laboral y económica. Es un espacio común, al que denominamos «ciberespacio», que sirve a fines legítimos y positivos, pero que también ha traído nuevas situaciones sobre las que resulta precisa la intervención del Derecho. La protección de la información, de nuestra privacidad, regular las relaciones comerciales, o los derechos de propiedad intelectual no pueden quedar al arbitrio de los usuarios. Resulta preciso adecuar las normas al nuevo escenario, para evitar crear espacios de impunidad, que pueden ser aprovechados por unos pocos para hacer prevalecer sus intereses.

Ese mundo virtual basado en la tecnología digital, se ha convertido en un reto intelectual para unos y una barrera para otros. La complejidad técnica de los sistemas informáticos y del diseño de las redes, y los protocolos de comunicaciones que se utilizan, generan indudablemente diferencias de conocimiento entre los usuarios de la Red, que sin duda

(2) En este sentido ver informe del GOL (Goverment On Line) del G8, de 6 de diciembre de 2001, en el que se realiza un estudio de la adaptación de los Estados a una futura pero posible democracia electrónica.

son aprovechados por unos pocos para hacer prevalecer sus intereses. En este sentido cabe destacar los resultados de los estudios que realiza INTECO (3) sobre la seguridad de la información y la e-confianza de los hogares y de las PYMES españolas, en los que de forma reiterada, se obtienen valores de riesgo de los equipos informáticos que rondan el 50%.

Gráfico 15: Evolución del nivel de riesgo de los equipos (%)



Fuente: INTECO

Esa dificultad para comprender y conocer el mundo digital, de la que no es ajeno el legislador, también afecta al proceso legislativo sobre las nuevas tecnologías, amén de que la dinámica de éstas, sometidas a un vertiginoso y contante avance, sobrepasa la dinámica legislativa. El resultado es una inadecuación o vacío legal en torno a los aspectos de la Red, que afectan a todos los órdenes del Derecho, incluido el penal.

A ello hay que añadir la complejidad del escenario global, donde los tradicionales límites geográficos quedan desdibujados por la realidad del tráfico internacional de información y la interacción entre sujetos sometidos a distintas jurisdicciones con marcos legislativos distintos, lo que sin duda da lugar a espacios de impunidad o *paraísos informáticos,* en los

(3) INTECO (Instituto Nacional sobre Tecnologías de la Comunicación) Realiza periódicamente estudios sobre los niveles de confianza de los usuarios domésticos y PYMES, que se pueden descargar en http://www.inteco.es/Seguridad/Observatorio.

que el control normativo, por intereses superiores o por nivel de desarrollo de la sociedad, no existe o es muy permisivo.

Por último, Internet se revela como un mundo virtual donde no existen los mismos patrones sociales del mundo real, un mundo al que nos asomamos ocultos tras la pantalla, creyendo ser anónimos y asumiendo nuevos roles. Donde la protección que ofrece la facilidad de crear identidades ficticias, supone un acicate o desinhibidor de nuestros temores frente a las barreras sociales, impulsándonos a veces a superar la legalidad establecida.

A la incultura digital, al escaso rechazo social de las conductas desviadas en la red, al vacío legal y al anonimato de la red, que ya de por sí son estímulos para el delincuente, se suma el rechazo social a cualquier medida restrictiva orientada a la seguridad. La idea romántica de una red como máximo exponente de la libertad de expresión está muy arraigada. Cualquier medida de control es interpretada como una potencial amenaza a la intimidad de las personas como derecho fundamental, lo que lleva a una defensa cada vez más férrea de ésta, incluso frente al intervencionismo de los Estados para la protección de sus ciudadanos, interpretado como un intento de crear una «*sociedad orweliana*» (4).

Este conjunto de circunstancias nos ha llevado a una sociedad de la información, a un ciberespacio, inseguro, donde las alarmas van creciendo día a día y la inseguridad es cada vez mayor.

La expresión más representativa de esa inseguridad, de ese lado oscuro de la red, es lo que socialmente entendemos como el cibercrimen.

EL DELITO INFORMÁTICO

El Ciberdelito, cibercrimen o delito informático es un concepto que manejamos socialmente para referirnos a un conjunto de conductas que vulneran los derechos de terceros y se producen en un escenario o medio tecnológico, provocando un rechazo social y sobre las que media el derecho penal.

Pero la idea es muy amplia. Las nuevas tecnologías están presentes en muchas facetas de nuestra vida. Qué duda cabe que el enraiza-

(4) George Orwell, en su novela «1984», imaginó una sociedad controlada por el Estado, el «Gran Hermano» que todo lo ve. La novela fue publicada en 1949.

miento de los medios tecnológicos es tan grande que están en todas partes. Por ello, casi no podemos imaginar la realización de cualquier delito sin que éstos aparezcan. El desvío de dinero a paraísos fiscales a través de transacciones electrónicas para evadir impuestos o blanquear dinero, la falsificación de moneda a través de medios tecnológicos, la apología de diversos tipos penales, la coordinación entre terroristas o bandas organizadas, las amenazas, la extorsión, etc. Prácticamente todo cabe. Y por ello, la idea de ciberdelito es cada vez más amplia o global.

Sin embargo, jurídicamente, el debate es más amplio y no hay consenso al respecto. Existen incluso los que niegan la existencia de estos delitos alegando que son delitos tradicionales que tienen encaje en los tipos penales actuales. Otros, por el contrario, defienden la necesidad de definir nuevos tipos.

El proyecto legislativo de mayor trascendencia, quizá el esfuerzo más serio y más ambicioso, el más consensuado a la hora de acotar el delito informático, ha sido el del Consejo de Europa. Su Consejo de Ministros nombró, en 1997, un Comité de Expertos del Ciberespacio, integrado por policías, juristas e informáticos, y al que se invitó a su participación a países no europeos pero con un peso especial en la sociedad de la información global (EE.UU, Canadá, Japón y Australia), para debatir los problemas que generaba una incipiente delincuencia en Internet. Tras cerca de cuatro años y veinticinco borradores con distintas revisiones, logró poner de acuerdo a la comunidad internacional con su Convenio sobre Ciberdelincuencia, aprobado y abierto a la firma por el Plenario del Consejo de Ministros en Budapest, el 23 de noviembre de 2001.

Este Convenio pretende armonizar la legislación de los diversos países que lo ratifiquen, no sólo en materia de derecho penal sustantivo, sino también de derecho procesal para hacer frente a ese tipo de delincuencia.

El Convenio define los delitos informáticos agrupándolos en cuatro grupos:

a) Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos.
   Engloba las conductas de acceso ilícito, interceptación ilícita, interferencia de datos, interferencia de sistemas y el abuso de dispositivos.

b) Delitos por su contenido.
   Comprende las conductas que se engloban en los delitos relacionados con la tenencia y distribución de contenidos de pornografía infantil en la Red.
c) Delitos relacionados con la informática.
   Se definen dos tipos penales, la falsificación informática y el fraude informático.
d) Delitos relacionados con las infracciones de la propiedad intelectual y de los derechos afines.
   En este grupo el Convenio hace una remisión normativa a los tratados y convenios internacionales sobre propiedad Intelectual.

En un Protocolo adicional al Convenio, de enero de 2003, se incluyeron las conductas de apología del racismo y la xenofobia a través de Internet, como delitos de contenido.

El Convenio y su Protocolo adicional, se hicieron eco de las realidades sociales de algunos delitos, especialmente de los delitos de contenido, dándoles el estatus de delito informático. Conductas que hasta entonces existían en el mundo real, pasan a ser conductas prácticamente exclusivas del mundo virtual, es decir, delitos informáticos, puesto que ya no existe en otro medio que no sea el tecnológico. Incluso ha sido el medio tecnológico lo que ha fomentado el delito, pasando de ser una conducta esporádica en el mundo real, a un delito muy repetido en el mundo virtual.

Las mismas circunstancias de la pornografía infantil, se reproducen en otras conductas que en el momento de discusión del Convenio, no tenían cabida o no se llevaban a cabo en la red. Tal es el caso del acoso a menores a través de la red, conducta conocido en el argot de internet como *grooming*, las injurias y calumnias, las amenazas, el robo de identidad, el intrusismo laboral, conductas que la red está fagocitando. Por ello, podemos decir, sin temor a equivocarnos, que hay una pluralidad de conductas que, día tras día, van adquiriendo mayor incidencia social y que entonces, cuando se aprobó el Convenio, tenían nula o escasa incidencia, y por ello, la catalogación de delitos informáticos que hace el Convenio empieza a necesitar una revisión.

Es éste quizá, el único pero que se puede achacar al Convenio, el no haber previsto el dinamismo y crecimiento de la red. Sin embargo, supone un gran acierto el buscar la uniformidad de las normas penales y procesales de los países firmantes, para facilitar la persecución de un delito global, que no entiende de fronteras terrestres.

El Convenio, hasta la fecha, sólo ha sido firmado por 46 países y ratificado por 30 estados firmantes (5). España lo ratificó el pasado 3 de junio de 2010, y acaba de entrar en vigor el día 1 de octubre.

La importancia del Convenio no está tanto en el número de países que lo han firmado y ratificado sino en que se ha constituido en el referente internacional a la hora de hablar de la delincuencia informática, y de aproximarnos a una legislación global. Gran número de países, sobre todo latinoamericanos, que ha redactado leyes especiales para la delincuencia informática, como es el caso de Venezuela, Chile o Argentina, han tenido una clara inspiración en el Convenio.

DEL *HACKER* ROMÁNTICO AL PIRATA INFORMÁTICO

De los cuatro grupos de delitos que el Convenio de Ciberdelincuencia acota como informáticos, quizá el más informático de todos sea el conjunto de delitos contra integridad, confidencialidad y disponibilidad de datos y sistemas informáticos.

Tenemos la tendencia a definir Internet como la gran red de redes, otorgándole así, indirectamente, mayor valor a la red en sí que a la información que se almacena en ella, al mallado de cables que componen la red que a los datos que por ellos circulan. Son pues la información que circula por la red y la funcionalidad de ésta, su poder de tratamiento de información y de comunicación, el objeto de la protección penal. Que esa información se almacene y fluya en la red con garantías de integridad, confidencialidad y disponibilidad.

El funcionamiento de la red se basa en unos protocolos que permiten el envío de información, independientemente del tipo de información que sea y del sistema que la remite. Estos protocolos fueron ideados hace ya muchos años para un proyecto militar, Arpanet, en el que por su uso y naturaleza, no se contemplaba que pudieran ser interceptados. De igual forma, la información se almacena en sistemas gestionados por programas y sistemas operativos, que como toda obra humana, está sujeta a errores desde el punto de vista de la seguridad. Vemos pues que el medio es vulnerable y ello llevó a muchos usuarios, apasionados por

(5) Se puede ver la lista actualizada de los países firmantes y los que lo han ratificado en http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=29/06/2010&CL=ENG.

la tecnología, a buscar y detectar cualquier vulnerabilidad de las redes y sistemas. Sus pretensiones no eran dañinas, su afán de descubrir los fallos del sistema a veces les llevaba a superar barreras de confidencialidad, pero el marco legislativo, con su indefinición, les protegía. Eran los primeros *hackers*.

Aunque el termino *hacker* tiene sus orígenes en la vulneración de las redes telefónicas para efectuar llamadas gratuitas, accediendo a centrales o interceptando llamadas, con la extensión de la red para uso de la comunidad universitaria y científica, rápidamente se transmutó el significado, y socialmente se identificó al *hacker* con el experto informático que era capaz de detectar los fallos de programación y entrar en los sistemas informáticos vulnerando las medidas de seguridad. Eran los inicios de la socialización de la informática, donde ésta todavía era muy «árida» y poco usable, muy distinta a la informática de hoy en día. Para algunos se convirtió incluso en un estilo de vida, en un reto intelectual y personal. La red era su pasión y su vida. Eran los románticos de la red.

Socialmente no se les reprobaba. Más al contrario, se les consideraba mentes privilegiadas que causaban admiración. Se estaba creando el mito social del *hacker*, apoyándose en novelas (6), películas (7) y con estereotipos de comportamiento. Se estaba alimentando la cultura del «*hacking*», que lejos de verse como una conducta negativa y perjudicial para los derechos colectivos de los usuarios de internet, sigue hoy manteniendo esa connotación romántica y positiva.

Qué duda cabe que no todos aquellos *hackers* tenían una visión tan romántica de la red, ni todos respetaban por igual la confidencialidad ajena, pero en líneas generales, sí se podía hablar de *hackers* «no lesivos». Incluso entre ellos distinguían los que tenían pretensiones filantrópicas, de mejorar la red, y aquellos otros que les movía la ambición y los intereses delictivos, a los que llamaron crackers.

Con el crecimiento de la red y el triunfo de jóvenes *hackers* emprendedores que fundaron las principales empresas del sector, se consolidó el mito y la meta para el *hacker*, lograr alcanzar notoriedad con sus acciones en la red, para aspirar a destacados puestos profesionales, rodeados de todo tipo de prebendas económicas y sociales. El *hacker* que es contratado por una multinacional con sueldos astronómicos.

---

(6) STOLL Clifford, *The Cuckoo's Egg*, EE.UU, Doubleday, 1989, 326.
(7) Película Juegos de Guerra, EE.UU. año 1983.

Esta idea romántica del *hackers*, guardián o «Robin Hood» de la red, ha permanecido hasta nuestros días y, aún hoy, en la juventud, atraída por el escenario de la red y enmarcado en la rebeldía juvenil, se autoidentifican muchos como *hackers*.

Pero con la socialización de la red y su enorme crecimiento, las circunstancias han cambiado mucho. Los sistemas son cada vez más seguros pues la demanda social así lo exige y las empresas de desarrollo de software dedican más recursos a ello. Por el contrario, los conocimientos técnicos para detectar las vulnerabilidades han de ser muy altos y por ello, al alcance de muy pocos. El afán de comunicación y de divulgación de conocimientos que impera en la red, arrastra a todos, incluidos los *hackers*, que darán a conocer los fallos o errores de programación que descubran, quizá por ese afán de notoriedad que rodea a la personalidad del *hacker*. Otros, incapaces de detectarlos, los harán suyos, los utilizarán e incluso los adaptarán mediante programas automáticos, para que sean utilizables por terceros que, ni siquiera serán capaces de entender la vulnerabilidad o fallo de seguridad que están aprovechando. Así nacen los *script kiddies* o *lammers*, usuarios con conocimientos un poco superiores a la media, que se autodenominan *hackers* y dispuestos a vulnerar la legalidad para buscar protagonismo.

Dado el gran número de usuarios que se identifican con esta cultura del hacking, y que practican sin reparos acciones con menosprecio de los derechos de terceros, el concepto de *hacker* ha mutado semánticamente, pasando a identificar al *hacker* como el usuario de la red, que haciendo uso de conocimiento, técnicas y herramientas informáticas, actúa contra sistemas informáticos de terceros, aprovechando las vulnerabilidades y errores de configuración de los sistemas, vulnerando la legalidad.

Tal es la carga peyorativa del *hacker* que, aquellos que poseen los conocimientos técnicos adecuados, utilizando las mismas técnicas de los *hackers*, para prevenir la acción de éstos, prestan servicios de auditoría y seguridad de sistemas informáticos para detectar vulnerabilidades, debiendo calificar sus actuaciones, siempre legales, de hacking «ético» o «blanco».

Pero pese a esa transformación del *hacker*, parte de la sociedad todavía ve con buenos ojos al *hacker*, un joven travieso e inquieto, no identificándolo con el delito, para el que busca otros conceptos como «pirata informático».

El objetivo del *hacker* es encontrar fallos de seguridad en el software del equipo. En su sistema operativo o en las aplicaciones que tiene instaladas. Estos fallos de seguridad se conocen como *bugs* o agujeros de seguridad. Desde su descubrimiento hasta que se hace público entre los técnicos de seguridad y logran encontrar la corrección o *parche de seguridad*, es explotado por los delincuentes que desarrollan pequeños programas (*exploits*) que aprovechan esa vulnerabilidad permitiendo entrar en los sistemas y adquirir *privilegios de administrador*, es decir, acceder al sistema para gestionarlo y/o controlar la información. Normalmente, una vez dentro, el atacante se asegura poder entrar en el sistema cuantas veces quiera, dejando una vía de entrada oculta, a la que llaman *puertas traseras*.

Las primeras acciones de los *hackers*, buscando notoriedad, fueron la creación de los temidos virus o gusanos, programas maliciosos que se introducían en el ordenador y que causaban un daño más o menos leve. La diferencia entre los virus y los gusanos estaba en la capacidad de autorreplicación, es decir, en la capacidad de que un ordenador infectara a otros. La vía primera de distribución de esos virus era a través del intercambio de disquetes o CD.

Posteriormente los virus se empezaron a ocultar en otro programa o documento que al ejecutarse por el usuario, infectaba el sistema. Eran los *troyanos*, en alusión al Caballo de Troya que ocultaba en su interior soldados griegos para asaltar la inexpugnable ciudad de Troya. Para infectarse, la víctima debía aceptar el caballo, el atractivo regalo aparentemente inocuo, el programa gratuito que buscamos, la presentación con atractivas imágenes, el vídeo de moda, etc. El *vector de infección* más utilizado para hacernos llegar el atractivo regalo, que contiene oculto el programa malicioso, fue el correo electrónico. Hoy, los vectores de infección son muy diversos: las redes P2P que enmascaran los troyanos en videos musicales o películas; las descargas de software gratuito; los servidores web con contenidos dinámicos, que al visitarlos el usuario se descarga, sin saberlo, el programa malicioso, etc...

La solución contra los virus eran los antivirus, y frente a ellos, los *hackers* desarrollaban cada vez más virus y más complejos, algunos prácticamente indetectables, como los *rootkits*. Así, podemos afirmar que se ha entrado en una dinámica o espiral de acción reacción entre los *hackers* y las empresas de desarrollo de software y de seguridad de la información.

¿HACKING BY DOLLAR?

La Red evoluciona y día a día se hace más «usable», más intuitiva y fácil de manejar, pasando del modo comando, al alcance de unos pocos y en el que había que conocer complejas instrucciones alejadas del lenguaje humano, a sistemas mediante ventanas, muy intuitivos y fáciles de usar hasta para el usuario menos avezado. Esta evolución también se proyecta en el volumen de información que en ella se deposita. La red se ha convertido en un repositorio de datos personales, información que pertenece al ámbito de la privacidad de las personas. Nuestra intimidad circula por la red, nuestras relaciones sentimentales, orientaciones sexuales, conflictos personales con terceros, son habitualmente compartidos con amigos, parejas, compañeros, o simplemente almacenados en nuestros equipos informáticos. Pero no sólo se almacena o comparte información personal, también se comparte información empresarial y económica. Las estrategias de empresa, los planes de negocio, los secretos de empresa, los datos económicos, etc. Y esa información, tiene un valor, un valor económico.

Los *hackers* se dan cuenta de que el mito del contrato millonario en la empresa *punto com* ya no existe. Que frente al experto informático la empresa prefiere al titulado académico. Que sus actuaciones con afán de notoriedad, no le reportan beneficio. Que la capacidad de entrar en los sistemas ajenos, por sí sola no tienen valor. Que el valor está en la información que almacenan los sistemas. El objetivo final cambia, ya no es descubrir la vulnerabilidad de las redes o sistemas. Ese es un objetivo táctico. El objetivo estratégico es acceder a los sistemas para obtener la información.

La primera información objeto de su interés, es la que más relación directa guarda con el valor económico, la información financiera. Sus principales acciones se dirigen a obtener datos económicos. Información de tarjetas de crédito, cuentas bancarias, etc. Información que puedan convertir fácilmente en dinero o bienes. Para ello, se centrarán en el comercio electrónico, con las compras, utilizando tarjetas de crédito de terceros, conducta conocida como *carding*.

A partir del año 2002, con el incipiente servicio de banca electrónica, empiezan a buscar rentabilidad a sus acciones mediante la usurpación de las identidades online de banca electrónica para transferencias de dinero no consentidas. Sus técnicas de hacking se orientan al apode-

ramiento de las claves de acceso a banca electrónica, mediante la conjugación del engaño y la suplantación de portales de la banca. Nace el *phishing*.

Pero no todos los *hackers* buscan la rentabilidad económica de sus acciones. Siguen existiendo los *hackers* movidos por las banalidades y veleidades humanas, los conflictos personales. El robo de información a parejas por rencores anclados a la rotura de la relación; de información empresarial, para dañar la imagen, fama y honor de directivos intransigentes contra los que existe un enfrentamiento; o de la privacidad de terceros por buscar diversión o satisfacer las inclinaciones *voyeristas*.

Incluso, algunos persisten en su idea de ganar notoriedad en la red, realizando ataques a sistemas con resultados visibles para el resto de usuarios, que puedan firmar o autoimputarse. Estamos refiriéndonos a los ataques de *defacement* o modificaciones de páginas web, y a los ataques de denegación de servicio contra sistemas informáticos (8).

LA DELINCUENCIA ORGANIZADA

Pero las posibilidades de ganar dinero en la red, vulnerando la legalidad, no pasan desapercibidas para las mafias de la delincuencia organizada, que, advirtiendo que el escenario es nuevo y con deficiencias legislativas que juegan a su favor, decide irrumpir en este terreno. Éstas, aportan su experiencia y estructura organizativa para el crimen, pero necesitan de los conocimientos de expertos *hackers*. Así nace el maridaje entre la delincuencia organizada y el cibercrimen.

Los primeros escenarios de la delincuencia organizada se focalizan en el fraude en el comercio electrónico y en la banca electrónica, como instrumentos más rápidos para obtener beneficios. Por ello conviene conocer los distintos modus operandi de ambos fraudes, para entender el papel de la delincuencia organizada y su evolución, especialmente del segundo, del que derivan otras formas de delincuencia organizada, consecuencia de la especialización de determinadas actividades o etapas del delito, que se ofrecen como servicio al resto de organizaciones de-

(8) Una denegación de servicio o ataques DoS (Denial of Service), consiste en atacar la disponibilidad de los sistemas de información, evitando que puedan prestar el servicio para el que han sido concebidos. Es uno de los ataques más temidos por los administradores de sistemas, por su relativa facilidad de comisión y el peligro que supone para la imagen continuidad del negocio de las empresas afectadas.

lictivas. Tal es el caso de la llamada industria del malware y del comercio de información personal.

Por último, no hay que obviar otro tipo de delincuencia organizada, menos estructurada y técnica, pero también vinculada a la red, concretamente a los timos en la red.

Fraude en comercio electrónico

El comercio electrónico o la adquisición y venta de productos a través de la red, se realiza sin la mediación del comercial, lo que permite reducir costes. Su dinámica es muy sencilla, ofrecer productos a través de comercios electrónicos, abonarlos mediante el clásico sistema de tarjetas de crédito, utilizando sistemas de envío de dinero o mediante pago electrónico seguro (PayPal, MoneyBookers,…), y remitirlo por empresas de transporte.

Como podemos ver, el sistema es sencillo a la vez que frágil. La confianza que ofrece el vendedor se basa en la apariencia y el nombre de un comercio, y de unos productos que únicamente conocemos por lo que se ve en la web. Y como quiera que el comercio electrónico se está orientando hacia la venta entre particulares, la confianza queda muy mermada por desconocer al vendedor.

La fortaleza del sistema de pago reside en la robustez de las tarjetas de crédito o débito, sistema que ya de por si es frágil y que tiene un alto índice de fraude, pero que, en Internet, se acrecienta por la imposibilidad de acreditar la tenencia de la tarjeta y la identidad del titular de la misma. Una vez que se dispone de la numeración de una tarjeta de crédito/débito y su fecha de caducidad, se puede utilizar contra cualquier comercio electrónico utilizando una filiación falsa y un punto de entrega del producto «comprometido», bajo control del defraudador. Está técnica de pago con tarjetas fraudulentas se conoce como *carding*. El terminal de venta virtual del comercio electrónico establece comunicación con su entidad financiera y la única verificación que establecen para validar la compra es la validez de la tarjeta. Hoy en día, algunos comercios y entidades financieras, están exigiendo el Código de Seguridad de la Tarjeta (Card Security Code - CSC) o también llamado CVV (Card Verification Value - CVV o CV2), un nuevo valor numérico presente en el soporte físico de la tarjeta y que, teóricamente, acredita que el usuario de la misma la tiene físicamente en su poder.

Por último, el sistema de entrega del objeto de la compra es vulnerable toda vez que no existe un sistema de acreditación del titular destinatario del producto. Normalmente las empresas de mensajería y transporte, ante la ausencia de respuesta en un domicilio, dejan una notificación para acudir a la central de la empresa a recoger el porte, donde con la simple notificación ya es garantía para recibirlo. Si se dispone de un domicilio desocupado y el control del buzón, un defraudador ya tiene domicilio para direccionar la entrega.

Con este escenario, cabe imaginar que el fraude ha de existir. Si a ello añadimos el ingenio del defraudador para inducir a engaño a las víctimas, el resultado está garantizado.

Por último mencionar que el fenómeno del comercio electrónico ha evolucionado de los portales de venta hacia los portales de subastas o clasificados, donde el vendedor no es un comercial, sino particulares que compran y venden. El fraude, por la exigencia de previo pago, prácticamente solo cabe del vendedor hacia el comprador, es decir, simular una venta para cobrar y no entregar nada a cambio.

Veamos las formas más habituales del fraude en el comercio electrónico, en las que la delincuencia organizada ha focalizado su actuación.

El carding

Inicialmente, el fraude en el comercio electrónico se centró en duplicar portales de venta que inducían a engaño a las víctimas que abonaban dinero por productos que no recibían. La vida útil de las falsas web era muy escasa. Lo justo para engañar a unas pocas víctimas que denunciaban el fraude. La incidencia del fraude fue escasa e imputable a delincuentes esporádicos que actuaban de forma independiente.

Posteriormente, se pasó al *carding*, la compra de productos abonándolos con tarjetas de crédito falsas. Los defraudadores posteriormente revendían los objetos del fraude, a precios muy bajos, para obtener beneficios. La gran mayoría de estos fraudes se dirigieron contra comercios de productos informáticos, de telefonía móvil, con gran salida en el mercado, y billetes de transportes (tren, avión, barco). Esta dinámica de fraude exigía una estructura capaz de obtener tarjetas para las compras, infraestructura para la recepción de los productos y canales de venta posteriores de objetos procedentes del fraude, es decir, una mínima estructura organizativa, grupos organizados para delinquir.

En España estas organizaciones estaban y están formadas mayoritariamente por grupos de inmigrantes subsaharianos, y los canales de recepción y venta se centran sobre los propios miembros de la etnia, que les dan salida a través de la venta ambulante. Aunque mayoritariamente toda la operativa del fraude se realiza desde España, ocasionalmente se ha detectado que la fase de compra vía internet se realiza desde los países subsaharianos, si bien la entrega del producto se hace en España.

Conscientes de la vulnerabilidad que representa la entrega del producto objeto del fraude, los defraudadores utilizan lugares de entrega en los que se logre desvincular al receptor, del fraude, como por ejemplo bares donde la recogida la efectúa el camarero en nombre de un cliente habitual, o *casas pateras* frecuentados por miembros de la etnia, donde están los encargados de recibir los envíos.

La obtención de los datos de las tarjetas para la realización del fraude, ha sufrido también una evolución importante. Inicialmente se obtenían tarjetas mediante técnicas de *skimming* o copiado de la información de la tarjeta con dispositivos técnicos. Incluso en la red se podían encontrar listados de numeraciones de tarjetas con sus datos de caducidad y titular, aunque la fiabilidad era muy baja porque las entidades bancarias también las observaban en la red y las catalogaban rápidamente de fraudulentas. A día de hoy, los datos de tarjetas se compran en la red a grupos organizados, cuya actividad se centra en la obtención de información financiera de los usuarios, y que más adelante comentaremos.

Las ventas en portales de anuncios clasificados

A medida que la red se ha hecho más participativa, los usuarios han aprovechado las ventajas que ésta les ofrece, y el mundo de las subastas y ventas entre particulares ha experimentado un gran auge. Como no puede ser de otra forma, los delincuentes se han trasladado al nuevo escenario de ventas entre particulares, donde la entrega del producto casi siempre está supeditada a un previo pago, y el fraude se centra sobre las estafas del vendedor hacia el comprador.

Los usuarios ofertan y compran a través de portales web dedicados a ofrecer a los usuarios esta posibilidad. El negocio de los portales está en las pequeñas comisiones que puedan llevarse de cada operación y el derivado de la publicidad. Cuantas más ventas, más rentabilidad para su negocio, por ello, son los primeros interesados en minimizar el impacto

del fraude. Algunos ofrecen sistemas de pago más confiables, como es el caso de eBay con su sistema PayPal, o sistemas de valoración de fiabilidad de vendedores.

El defraudador busca generar el suficiente engaño en la víctima para obligarle a realizar un acto de disposición patrimonial en beneficio del defraudador, es decir, engañarle para que la víctima pague sin haber recibido el producto. El engaño se basa en ofrecer productos estrella con gran demanda, a precios realmente interesantes, y articular un sistema de pago confiable para el pagador.

Los productos estrella en este tipo de fraude son los vehículos de alta gama, las viviendas y el equipamiento informático. Siendo real la venta de coches de segunda mano y de alta gama a precios muy competitivos, los defraudadores se han centrado en ese tipo de ventas. Para ello, aprenden de los anuncios de ventas legales y llegan a copiarlos, para lo que mantienen fluidas comunicaciones con los vendedores y obtienen toda la información necesaria para montar anuncios paralelos de venta del mismo producto, ya sea un vehículo o la venta o alquiler de una vivienda. Los anuncios fraudulentos tienen las mismas fotos, los mismos datos técnicos y las mismas circunstancias del vehículo o la vivienda, incluso copian la identidad del legítimo vendedor, en otra web de anuncios. El engaño se acompaña de situaciones creíbles, como la adjudicación de vehículo de empresa o el desplazamiento por motivos laborales a un tercer país.

Huelga decir que el defraudador se adapta al medio y varía su estrategia conforme ésta es o no rentable y según la tendencia del mercado. Si hoy son coches y casas, ayer eran quads, motos o robots de cocina thermomix, pero siempre acompañan el engaño con suplantación de identidades personales o comerciales.

Un caso particular de tipo de comercio es la venta de productos ilegales o delictivos. Estamos en el caso de venta de titulaciones académicas falsas, licencias de conducir fraudulentas, servicios profesionales de extorsión, amenazas, sicarios, etc. Por supuesto, la mayoría de los servicios y productos ilegales esconden engaños y fraudes al comprador que, por la naturaleza delictiva del producto o servicio, no denunciará.

Los sistemas de pago son los clásicos en el comercio electrónico, la transferencia bancaria o el envío de dinero a través de empre-

sas de transferencia de dinero, tipo Western Union o MoneyGram. En ocasiones, para generar confianza en el comprador, se apoyan en la utilización de falsas empresas intermediarias, que simulen realizar la función de intermediar entre comprador y vendedor para evitar el fraude. Reciben el producto del vendedor y el dinero del comprador, y validan la operación entregando a cada uno lo suyo. Son las empresas llamadas *escrow*. Estas empresas ficticias son creadas virtualmente por los propios estafadores, es decir, son falsas webs que simulan su existencia.

Otra fórmula de engaño es la utilización de falsas empresas de transporte que simulan ser receptoras de la mercancía comprada para obligar a la víctima a abonar su importe. En este caso tampoco son empresas reales, sino websites que simulan su existencia.

Como se ha comentado, alguno de los portales de ventas entre particulares utiliza el sistema de pago por PayPal, que básicamente consiste en cuentas virtuales vinculadas a tarjetas de crédito reales.

La utilización de cuentas bancarias o de tarjetas de crédito vinculadas a cuentas de Paypal, para recibir los pagos, suponen un punto vulnerable para los defraudadores, que quedarían identificados como titulares de las cuentas o tarjetas de crédito. Para ello cuentan con colaboradores financieros, conocidos por el nombre de *mulas*, para recaudar las ganancias, y cuyo único cometido es ofrecer sus cuentas para recibir el dinero y retirarlo inmediatamente para transferirlo a su destinatario final mediante las empresas de transferencia de dinero.

La estructura recaudatoria basada en colaboradores financieros ofrece muchas variantes, y como quiera que se utiliza en otras modalidades de fraude, se desarrollará más adelante.

Un elemento común de estos fraudes es la transnacionalidad de las operaciones. Las operaciones fraudulentas más importantes se realizan entre clientes y vendedores de distintos países, y el dinero circula también entre distintos países, lo que dificulta la persecución.

Vemos pues que hay un desarrollo informático más o menos complejo, con creación de empresas ficticias, que hay una fase de preparación de los fraudes con la recogida de información para copiarla, que hay un estudio de los escenarios más rentables, que hay una técnica y modus operandi que van repitiendo en distintos escenarios o portales de anuncios clasificados, que operan a nivel internacional y que disponen

de red de colaboradores y de un sistema estudiado de recaudación. La utilización de estas técnicas, como es de suponer, evidencia una mayor complejidad, propia de bandas organizadas.

Es difícil precisar cuántas bandas organizadas se dedican a esta actividad, puesto que las actuaciones policiales han sido pocas, y, por la naturaleza del fraude, con una pluralidad de afectados inicialmente desconexos entre sí. Pero casi todas las investigaciones apuntan a unos elementos comunes. La tipología de fraude está liderada por bandas organizadas de rumanos. Estas bandas tienen sus raíces en comunidades o localidades de Rumanía, donde se encuentra la cabeza de la organización delictiva y donde hacen gran ostentación de su poderío económico. En ocasiones, esta ostentación, la divulgan por internet, difundiendo imágenes de sus fiestas, que más parecen orgías en hoteles de gran lujo, y con el uso de vehículos de alta gama. La red de recaudación basada en colaboradores financieros se nutre de inmigrantes de Rumanía, captados normalmente por contactos personales entre los miembros de la comunidad inmigrante. Se profesionalizan para estos cometidos, subsistiendo de esa actividad y abandonando toda actividad laboral legal. Utilizan documentaciones falsas que facilitan la apertura de varias cuentas bancarias para recibir los pagos de las ventas fraudulentas, dificultando su identificación y localización en el terreno.

Una peculiaridad de estos grupos, probablemente debida a la presión de la policía rumana en el control de las transacciones a través de Western Union, es que utilizan mensajeros para la recaudación y control de sus *mulas*, en lugar de remitir el dinero por la empresa de transferencia de fondos.

Por último, señalar una variante, también explotada por las mismas bandas organizadas, en las ventas en portales de anuncios clasificados, dirigido del comprador hacia el vendedor, el de los *honorarios adelantados*. El defraudador compra un producto abonándolo con un talón bancario de importe superior a la compra, con la exigencia de compromiso para el vendedor de abonar la diferencia, a través de empresas de transferencia de dinero. Cuando el vendedor recibe el talón, lo ingresa en su cuenta figurando el abono y sin fijarse que se encuentra retenido a la espera de validación del talón, operativa que lleva varios días. En este periodo, el vendedor remite el producto y la cantidad sobrante del talón, que posteriormente le será descontado de su cuenta por no tener fondos.

Fraude en banca electrónica

El servicio de banca electrónica que ofrecen las entidades bancarias a sus clientes, supone comodidad e inmediatez en las gestiones para los usuarios que hacen uso de él, pero presenta una vulnerabilidad importante, la autenticación del usuario. Inicialmente, los usuarios se identificaban con un sistema de autenticación primario, es decir, con algo que se sabe, un login y un password, un nombre de usuario y una contraseña. Si ésta es conocida por terceros, pueden usurpar nuestra identidad y realizar toda aquella operativa que el banco ofrezca. Ese fue el inicio del fraude bancario.

Los estafadores enviaron correos electrónicos a multitud de usuarios, simulando proceder de la entidad bancaria y requiriendo la conexión al banco para actualizar las contraseñas. Se alegaban motivos técnicos, motivos de seguridad, o actualizaciones de sistemas, y los mensajes incluían enlaces a la supuesta web bancaria. Activando esos enlaces se acudía a una web idéntica a la del banco pero fraudulenta, donde el usuario consignaba sus datos identificativos, su identidad online, que pasaban a poder de los defraudadores, quienes posteriormente accedían a la página original del banco, usurpaban la identidad de la víctima y ordenaban transferencias de dinero a cuentas bancarias bajo su control. Este engaño para hacerse con los datos de identidad online de la banca electrónica se bautizó como *phishing*. El origen del término no está claro. Parece ser que podría provenir del término inglés *fishing*, alusivo a la «pesca» de contraseñas. Otros barajan como origen del término el acrónimo de *password harvesting fishing* (cosecha y pesca de contraseñas). Por extensión, el defraudador que practica el *phishing*, será el *phisher*.

Un error bastante extendido es confundir una parte con el todo. *Phishing* es únicamente la técnica para obtener las contraseñas que nos permiten autenticarnos, y otra es utilizarlas contra el sistema de banca electrónica, usurpando la identidad de su legítimo titular para disponer de su dinero. Y es conveniente recalcarlo porque el *phishing* ya no sólo se practica para obtener las contraseñas de banca electrónica, sino para obtener todo tipo de contraseñas y datos personales, con finalidad defraudatoria o no.

Este fraude, al igual que ocurre en algunas de las modalidades del fraude en el comercio electrónico, precisa la colaboración necesaria de los llamados colaboradores financieros o usuarios que ponen sus cuen-

tas a disposición de los defraudadores para recibir el dinero e inmediatamente retirarlo y entregarlo al estafador, antes de que la víctima se aperciba de la estafa y ordene su devolución. A estos colaboradores financieros se les conoce como *mulas*, nombre también utilizado en otras figuras delictivas como el blanqueo de capitales. El nombre hace alusión al animal de carga necesario para el porte de mercancías, sin más responsabilidad que la carga y fácilmente reemplazable.

Así, el *phisher* que suplanta la identidad de una víctima, ordena transferencias de dinero a la cuenta bancaria de la *mula*, quien recibe aviso inmediato y ha de acudir a la oficina o sucursal bancaria para hacer efectivo el dinero y remitirlo por una empresa de transferencia de dinero al *phisher*.

Este fraude inicialmente tuvo una incidencia muy alta, quizá porque pilló desprevenidos a los bancos, que finalmente reaccionaron, incrementando las medidas de seguridad, y a las policías, que vieron cómo desde cualquier rincón del mundo se suplantaban identidades, generando múltiples víctimas que diversificaban la acción judicial, y a las que se les quitaba el dinero de sus cuentas y, con un sistema rápido, se dirigía el dinero hacia países del este, donde la colaboración policial era más precaria.

En torno a esta actividad se detectaron numerosos grupos que actuaban internacionalmente, remitiendo los mensajes desde ordenadores comprometidos e inseguros que los *hackers* se encargan de localizar, controlar y utilizar para sus fines delictivos, y creando redes de colaboradores financieros, recolectores de dinero o *mulas* cuya misión era remitir el dinero hacia los países del este. Prácticamente en todos los países europeos de la ex república soviética se remitía dinero, lo que permite intuir el volumen de fraude que hubo. El número de fraudes era tan alto y tanta la dispersión de hechos que no se era capaz de vincular las acciones a un mismo grupo, toda vez que actuaban sobre usuarios de distintas entidades bancarias y distintos países.

Otro problema que se detectó en torno a este fraude es el tráfico de datos personales. Hasta la fecha, los usuarios sufrían el spam o correo masivo no deseado con fines comerciales, algo que preocupaba más a las operadoras de internet, por el consumo de red que suponía, que al usuario, que no veía amenazada su intimidad con ello. Pero esos mismos datos que se vendían para el spam, se venden para convertirnos en destinatarios del *phishing*.

Ante el alarmante crecimiento del fraude en banca electrónica, desde la prensa, la banca y la policía se alertó, con profusión, a los ciudadanos, lográndose minimizar su impacto. El ciudadano estaba más atento a los engaños de suplantación de identidad de las entidades bancarias para robarle los datos de identificación del servicio de banca electrónica. Y, como se ha dicho, la banca reforzó el sistema de autenticación con un segundo nivel de seguridad, algo que se tiene. Ya no sólo se identificaba al usuario con algo que sabía, un login y un password, sino que se le efectuaba una pregunta cuya respuesta venía en algo que el usuario debía tener, una tarjeta con coordenadas numéricas o un *token* o testigo que entrega el banco al cliente.

Pero siguiendo la espiral de acción reacción, los *phishers* idearon nuevos métodos para hacerse con las contraseñas o identidad online de sus víctimas. La experiencia de los *hackers* fue vital para esta etapa. De la creación de los virus y gusanos que buscaban causar daño en los sistemas se pasa a diseñar otro tipo de programas que pretenden acceder al sistema y robar información, sin que el usuario sea consciente de ellos. Empieza la industria del malware o software malicioso.

Primero fueron los troyanos bancarios tipo *keylogger*, programas que permiten la captura de pulsaciones de teclado del usuario. Se instalaban en los ordenadores de las víctimas y cuando tecleaban la palabra banco o similar empezaba a capturar las pulsaciones de teclado, sabedores de que entre ellas estaban los identificadores del usuario. La contramedida bancaria fue el diseño de teclados virtuales en pantalla, donde el usuario no pulsaba teclas sino pulsaba clics de ratón en un teclado que aparecía en pantalla. Los *phishers* diseñaron troyanos que capturaban las secuencias de pantalla.

A medida que las entidades bancarias adoptaban medidas preventivas y de seguridad, los phishers ideaban y mejoraban el software malicioso, logrando la sofisticación de los troyanos con técnicas mucho más complejas, que permitían, una vez autenticado el usuario con su banco, establecer una comunicación entre el banco y *phisher* oculta para la víctima. Y así se continúa en una escalada de medidas y contramedidas, combinándolo con la «ingeniería social» o capacidad de engaños que atesoran los estafadores en general.

Esta escalada ha dado lugar a variantes del *phishing* que han adquirido nombre propio:

- *Pharming*, técnica de *phishing* que consiste en derivar las conexiones a banca electrónica actuando sobre los servidores de resolu-

ción de nombres de dominio o DNS. En esencia consiste en que cuando al navegador web se le indica una dirección web de un banco concreto, en vez de acudir al banco adecuado acude a la que el *pharmer* le ha indicado. Esta resolución falsa de nombres de dominio, que lleva a la víctima a la página web falsa, se puede hacer en «local», actuando sobre el propio ordenador de la víctima a través de un programa malicioso, o en «red», actuando sobre los servidores de DNS, ordenadores que están en la red con la función de indicar el «camino» adecuado para acceder a las páginas web solicitadas.

- *Vishing*, técnica basada en la tecnología de *Voz sobre IP* (VoIP) que permite hablar por teléfono a través de la red de Internet. Se manipulan ordenadores para que actúen como auténticas centralitas telefónicas, dando una respuesta similar a una central de banco, a través de la cual solicitan al usuario víctima los datos de identidad bancaria o datos de tarjetas de crédito. La forma de inducir al usuario a que efectúe llamada al número de telefonía por VoIP es mediante el envío de mensajes SMS en los que alerta de gastos no realizados, incluyendo en el mensaje el supuesto número para reclamaciones, que no es otro que el de la centralita de VoIP.
- *Smishing*, o *phishing* a través de mensajes SMS de telefonía móvil. Se realiza un spam de SMS supuestamente remitidos desde la entidad bancaria reclamando respuesta por esa misma vía de datos bancarios.
- *Whaling* o *whale phishing* (*phishing* de ballenas). Es una variante de *phishing* mucho más preparada y dirigida a altos ejecutivos, políticos o empresarios a los que se supone que tienen disponibilidad de cantidades más altas de dinero o manejan información más sensible, y por ellos son objetivos más rentables.
- *Hishing* o *hardware phishing*. Es el *phishing* a través de productos hardware que se comercializan con una vulnerabilidad que permite el acceso fácil al equipo de la víctima o que el propio hardware lleva incorporado en su *firmware* el programa malicioso que permite el robo de información bancaria y su remisión a un servidor bajo control de *phisher*.

Como se puede observar, las variantes son muchas y conjugadas con el ingenio y la capacidad de engaño, con la ingeniería social, las posibilidades de sufrir engaño son muy altas. A modo de ejemplo, por su originalidad, citar dos originales casos de *phishing*. Uno mediante el

envío de un mensaje de correo electrónico presuntamente procedente de la policía de Brasil en que se le indica que está siendo requerido en una investigación policial, para lo que se solicita que acceda a la página web de la policía y conteste a un formulario requerido, estando el enlace en el propio mensaje. Al acceder al mensaje y rellenar el formulario uno es infectado por un troyano bancario. Y el segundo mediante el envío de un SMS informando que ha sido dado de alta en un chat erótico pornográfico, informando que si desea darse de baja debe conectarse a una URL que figura en el mensaje. Al conectarse y solicitar la baja, también se infecta con un troyano bancario.

Qué duda cabe que cuanto más sofisticadas sean las medidas y contramedidas, menor incidencia tiene el fraude, y que siempre serán más vulnerables aquellos que menos medidas de seguridad implementen. Hoy nos movemos en niveles de fraude en banca electrónica altos, y por desgracia no declarados. Prácticamente es una política común de las entidades bancarias asumir el fraude por la propia entidad, descargando a sus clientes de culpa. Esto les lleva, por norma general, a ocultar los datos reales para no perjudicar la imagen institucional. Y si los consumados no son declarados, las tentativas, que son muchísimas más, tampoco lo son. Los sistemas bancarios, en la espiral de acción reacción que mantienen con los delincuentes, han desarrollado sistema de detección de operativas fraudulenta como mejor sistema para evitar el fraude, alcanzándose niveles de eficacia altos.

Un elemento a tener en cuenta en la práctica totalidad de la amplia casuística del *phishing* es la existencia de sistemas informáticos donde se recoge la información de las víctimas. Quien cae en el engaño del enlace a una web fraudulenta, al igual que la víctima del troyano, remite la información personal a un sistema informático ubicado en la red y controlado por el *phisher*. Esto ha obligado a los *phishers* a crear una red de máquinas u ordenadores comprometidos para uso propio, y dispersos por todo el mundo. Nos podemos encontrar que un día la información se manda a un equipo alojado en EE.UU y mañana, a otro distinto situado en Rusia. Los informes hablan que el país con mayor número de páginas alojadas es Estados Unidos, seguido de Rusia. La existencia de estos servidores y de las páginas fraudulentas o *fakes* de bancos es uno de los indicadores del nivel de fraude que hay en torno al *phishing*. Las entidades bancarias contratan servicios informáticos de empresas dedicadas a neutralizar, en el menor tiempo posible, las páginas que afectan a su entidad. Por otro lado, la acción policial contra este tipo de fraude,

dista mucho de ser eficaz, toda vez que como se ha podido intuir, por la complejidad de su realización y la diversidad de actores que participan, está monopolizada por bandas organizadas, que operan a nivel transnacional, haciendo muy difícil su persecución.

Si a la escasa eficacia de las actuaciones policiales se suma la pasividad de las entidades bancarias a denunciar tanto los hechos consumados como el enorme volumen de tentativas de fraude existentes, por temor a consecuencias negativas a la imagen institucional o del servicio de banca electrónica, se está creando un espacio de impunidad para el delincuente que favorece el crecimiento de este tipo de delitos.

Vemos pues que es un modelo delictivo muy estructurado en el que hay desarrolladores con altos conocimientos técnicos, utilización de recursos de red, estructuras de blanqueo de dinero a través de *mulas*, y los organizadores del fraude. Y además, creciente por la escasa presión que sufren. Por ello, y en base a estimaciones de volumen de fraude, se comenta que la industria del crimen que rodea al fraude en banca electrónica está creciendo a pasos agigantados, llegando a ser más rentable que otras actividades clásicas de la delincuencia organizada, como el tráfico de drogas. Lo que sí se ha observado es que el crecimiento está trayendo consigo la especialización de las funciones, creándose grupos dedicados a sólo alguna de las etapas o pasos del fraude en banca electrónica y ofreciendo su especialización como servicio para otras bandas delictivas. Es el crimen como servicio, *crime as a service*.

Crime as a service

El crecimiento del *phishing*, derivado de la rentabilidad del delito, tanto en criterios económicos como de impunidad, hace proliferar los grupos organizados que aterrizan en este escenario delictivo. Un escenario que precisa de desarrollos informáticos para el diseño de falsas páginas web de entidades financieras, de malware para infectar las máquinas y controlarlas, y para obtener información de éstas.

El incremento de grupos en torno al *phishing* les obliga a buscar, entre los ambientes *hackers*, gente capaz de cubrir sus necesidades. Qué duda cabe que la demanda trae consigo el incremento de la oferta, y ésta deriva en un abaratamiento de los costes de los productos o desarrollos informáticos. En el entorno del mundo *hacker*, a través de foros o canales temáticos de fraude se empieza a comercializar las herramientas de *phishing*, los troyanos que roban información de las víctimas.

Por otro lado, debido a la permanente respuesta del mundo de la seguridad informática y bancaria, el *hacker* está obligado a una constante innovación. Todo el malware que desarrolla tiene una vida limitada hasta que es descubierto. Pero no sólo el malware, sino las técnicas de hacking para detectar agujeros de seguridad o bugs en los sistemas o programas, que permiten acceder sin ser detectados, tienen una vigencia hasta que el desarrollador del software corrige el error. Esta actividad creativa ha alcanzado cotas insospechadas, llegándose a una producción de malware sin precedentes, donde las empresas de seguridad antimalware, no son capaces de dar una respuesta eficiente.

Dentro de este mundo del malware, fruto de los análisis que llevan a cabo las empresas antivirus y otras del sector, se pueden definir dos corrientes o escuelas. La de los países del este y la de los brasileños. La primera tiene su influencia o campo de acción sobre los usuarios europeos y norteamericanos, y la segunda sobre los latinoamericanos. Pero el efecto globalizador de la red también se deja notar en ambas escuelas, donde se empieza a detectar que unas copian de otras. Tras los recientes incidentes de Google con *hackers* chinos, se empieza a hablar también de la escuela china, no tan orientada al fraude de banca electrónica sino al robo de información.

Consecuencia de esta amplia actividad de desarrollo de malware, las bandas organizadas empiezan a dejar de tener *hackers* a su servicio, para empezar a contratar servicios que éstos venden. Y el *hacker*, de esta forma, se desvincula del hecho delictivo concreto y sólo ofrece el instrumento. El más claro ejemplo de esto es la venta de kits de *phishing* en la que un usuario cualquiera, sin conocimientos avanzados de informática puede adquirir en el mercado del malware, un kit que sólo ha de configurar y poner en funcionamiento, para empezar a infectar equipos y obtener información de sus usuarios. Incluso en los acuerdos de servicio por el kit, informan que el desarrollador no se hace responsable del mal uso del programa.

Lamentablemente la cultura de seguridad informática es muy escasa, tanto a nivel doméstico como a nivel empresarial. La informática es concebida como un servicio y no como un activo que requiere de una inversión en seguridad. Consecuencia de esto es la ausencia o insuficiente dedicación de esfuerzos a la seguridad de los equipos y sistemas, y el gran número de máquinas y servidores susceptibles de ser comprometidos.

Existen numerosos estudios, la mayoría de ellos realizados por las empresas del sector de la seguridad informática, que arrojan cifras escalofriantes. En España, el Instituto Nacional de Tecnologías de la Comunicación (INTECO), ha realizado diversos estudios del estado de la sociedad de la información en el escenario español. Muchos de los resultados son extrapolables a la sociedad global. Por ello, es de recomendada lectura el *Estudio sobre la seguridad de la información y eConfianza de los hogares españoles* y el *Estudio sobre incidencias y necesidades de seguridad en las pequeñas y medianas empresas españolas,* al que ya se ha hecho mención al inicio del presente capítulo. En el último estudio publicado se habla de que, prácticamente dos de cada tres equipos domésticos, está infectado con malware.

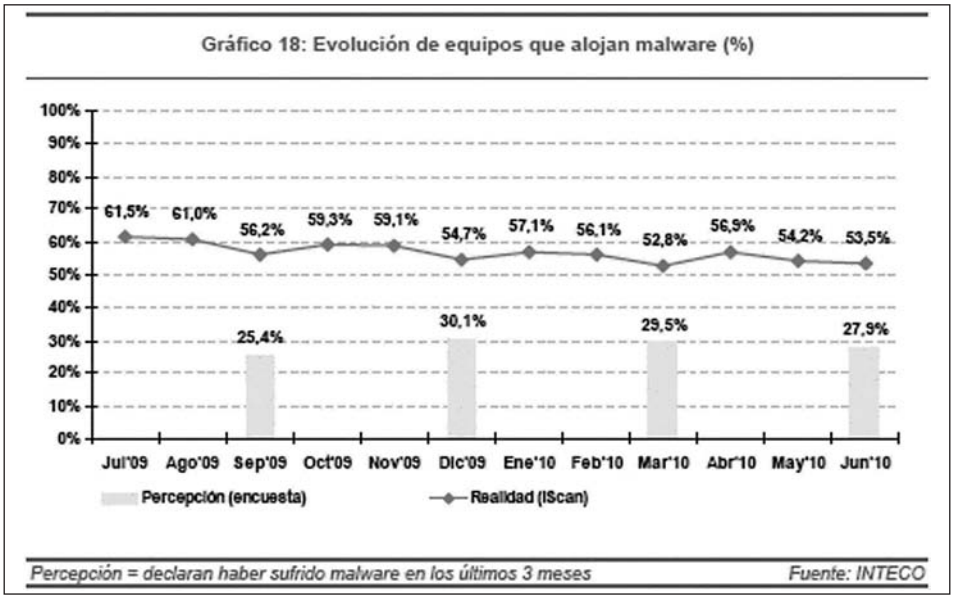


Figura 1. Gráfico de evolución de equipos que alojan malware. Fuente: INTECO.

Los *hackers* son conscientes de esta realidad y de las posibilidades que ello supone. El valor de los sistemas no está en el sistema en sí, sino en la información que almacenan. Si se es capaz de entrar en un sistema ajeno, aprovechando vulnerabilidades o deficiencias de configuración, y controlarlo remotamente, o se es capaz de infectar un ordenador con un troyano para robar la información bancaria, también se puede infectar para entrar y robar cualquier tipo de información o espiar la actividad y comunicaciones del usuario.

Así, el malware que diseña sirve para más funciones. Ya no sólo es troyano bancario para espiar los datos de conexión a banca electrónica, sino que permite el control del ordenador, roba las contraseñas de los accesos a los distintos servicios que tenga el usuario, ya sea su webmail, su cuenta de PayPal, la cuenta del casino virtual o las contraseñas de banca electrónica.

De esta forma el *hacker*, va conformando una legión de ordenadores infectados, bajo su control, a los que les puede robar la información y ordenarles que realicen cualquier acción, ya sea conectarse a una web determinada, mandar un mail o borrar su propio disco duro, es decir, crear su propia red de ordenadores zombis, red de robots o *botnet*, como se le conoce en el argot *hacker*.

Siguiendo la política de disminuir riesgos y responsabilidades, algunos *hackers* capaces de desarrollar este software, en lugar de utilizarlo, lo ponen a la venta, comercializándolo como un servicio personalizable. Otros, sin embargo, lo explotan y lo que comercializan es la información que obtiene.

Así, se ha creado un mercado negro de información personal de todo tipo, pero especialmente de datos financieros. Podemos encontrar que se están vendiendo filiaciones de personas completas, con números de tarjetas de identidad, seguro médico, y todo lo necesario para fingir en la red ser otro; y podemos también encontrar listado de tarjetas de crédito con todos los datos necesarios, ordenados por entidades bancarias y por saldo disponible, con todos los datos necesarios para su operativa. En fin toda la información que guardemos en nuestros sistemas y que puede ser robada, puede ser vendida. Es el comercio de los datos personales.

Pero una red de ordenadores bajo control de un *hacker* tiene más posibilidades. Pueden utilizarlos para realizar ataques contra terceros; pueden convertir los equipos en repositorios de malware, de música, de películas, e incluso de pornografía infantil; pueden utilizarlos para enviar *spam*, pueden causar daños en los equipos, borrando cualquier tipo de información o programa, y pueden utilizar los equipos para cualquier actividad de fraude.

Dentro de los ataques a terceros cabe mención especial los ataques a la disponibilidad de la información o bloqueo de los sistemas. Si cuando el usuario requiere el uso del sistema o de la información, no está disponible por la acción de terceros, nos enfrentamos a una denegación

de servicio (DoS del inglés Denial of service). Muchas empresas, tienen como única línea de negocio, la prestación de un servicio a través de la red. Otras, sin ser la única línea de negocio, su funcionalidad es parte de la imagen empresarial. Imaginemos las consecuencias para un banco que no pudiera prestar el servicio de banca electrónica por la acción de terceros sobre los sistemas informáticos del banco.

Relacionado con los ataques DoS, hay que mencionar el *black mail*. Las bandas organizadas ya se han hecho eco del riesgo que supone para algunas empresas la disponibilidad de sus sistemas y han actuado al más puro estilo mafioso, exigiendo sumas de dinero, extorsionando, para que sus sistemas no sufran ataques de «denegación de servicio».

Y nuevamente esta potencialidad de las *botnes*, frente a la demanda del mundo del crimen, se empieza a ofrecer como servicio. Se alquilan las *botnets*.

Otro elemento imprescindible para la ejecución del fraude en banca electrónica es la existencia de equipos u ordenadores deslocalizados por la red, donde almacenar la información y las *fakes* de los supuestos bancos. Para ello se desarrollan herramientas que exploren la red en busca de servidores mal configurados o vulnerables a determinados fallos de seguridad, que permitan la instalación de sistemas de control remoto. También se buscan servidores que garanticen el anonimato de sus usuarios gracias a legislaciones que no obligan a guardar los datos de registro de sucesos de los sistemas, es decir, servidores en paraísos informáticos.

En torno a esta necesidad se han creado auténticas infraestructuras de servidores e incluso de proveedores de servicio de internet (ISP), que conscientes de que sus clientes hacen un uso delictivo de él, y amparados en una normativa inexistente o deficiente, prefieren mantener una estructura de red que les genera beneficios. Fue especialmente famosa la RBN (Russian Business Network) constituida por un conjunto de ISP que ampararon en un momento determinado la gran mayoría del fraude de banca electrónica que existía.

La infraestructura de mulas

A lo largo de las distintas estructuras organizativas de la delincuencia que se ha creado en torno al cibercrimen, se ha comentado la necesidad del blanqueo de las ganancias procedentes del delito, utilizando

colaboradores financieros o *mulas*. El tema se ha descrito de forma muy generalista y como indicio determinante del carácter organizado de la delincuencia que recurre a este sistema de blanqueo y recaudación de las ganancias del delito. Y se ha dicho que como elemento común de varios tipos de delitos se describirá con más detalle. Vistos los fraudes y la industria del malware, llega su turno.

La tipología de *mulas* es muy diversa y ha sufrido una evolución significativa. En los inicios, las bandas organizadas enviaban a los distintos países donde operaban personal de la banda con varias identidades falsas y con cada una de ellas y en distintas entidades y sucursales abrían cuentas bancarias para recibir el dinero de las víctimas.

Posteriormente, trasladaron a miembros de la banda como captadores de *mulas* entre colectivos de inmigrantes naturales de los países donde se ubicaba la cabeza de la banda organizada. Buscaban el apoyo de sus paisanos, sabedores de que éstos eran conscientes de los riesgos que corrían si eludían o intentaban apoderarse de las ganancias que debían trasladar. Dada la escasez de recursos económicos de los inmigrantes y el escaso reproche penal que sufrían si eran objeto de la acción policial y judicial, les era fácil encontrar personas dispuestas a hacer de *muleros*. Los captadores se dedicaban a ofrecer pingües ganancias a quienes están dispuestos a colaborar, dándoles las instrucciones oportunas incluso para hacer frente a la acción policial, con coartadas creíbles, como la recepción de ingresos procedentes de herencias de amigos de su país remitidas para evitar la acción fiscal de su gobierno, o ingresos procedentes de separaciones matrimoniales de amigos para evitar el control del cónyuge.

También se captaban *mulas* vinculadas al mundo de la droga que estaban dispuestas a ofrecer sus cuentas por las escasas ganancias que les permitirán adquirir nuevas dosis de droga. Hasta mujeres de países del este, víctimas del tráfico de seres humanos para la prostitución, traídas bajo engaño a nuestro país y obligadas a la prostitución para pagar su presunta deuda, retirándoles su identidad con la que abrían cuentas corrientes para recibir los ingresos de victimas de *phishing*.

El endurecimiento de la acción judicial, con sentencias calificando la acción de las *mulas* de cooperación necesaria, obligó a las bandas organizadas a agudizar el ingenio para captar nuevas *mulas*, toda vez que la vida útil de éstas, en la inmensa mayoría de los casos es de una sola recepción de dinero procedente del fraude.

Sin dejar de coexistir los anteriores procedimientos de captación de *mulas*, a día de hoy, el sistema de captación de *mulas* ha migrado hacia el engaño, siendo éste el más utilizado. Remiten mensajes de correo electrónico a multitud de usuarios proponiendo una colaboración financiera para una empresa que va a empezar a operar en el país. Las ganancias son porcentuales en función de lo que reciba en su cuenta, y aseguran que se puede llegar a ganar cantidades de hasta 3.000 €con dedicación exclusiva. La cobertura de las empresas es muy diversa y muchas de ellas creíbles, como el caso de la agencia matrimonial de mujeres de países del este, que se desplazan al país de la «*mula*» y cuando contraen matrimonio, el supuesto cónyuge abona los servicios a través de ingresos al colaborador financiero o *mula*. Es de suponer que, según el grado cultural de la *mula*, hay consciencia o no de su vinculación al mundo del delito. Pero lo cierto es que los delincuentes agudizan el ingenio y crean historias que pueden llevar al engaño a cualquiera. Actualmente y con la crisis económica que atenaza a prácticamente a todos los países, son técnicas habituales el reclutar *mulas* con distintos engaños entre los usuarios de portales de empleo.

A ello hay que sumar la reciente normativa europea de creación de la Zona Única de Pagos en Euros, conocida bajo el acrónico de SEPA (de la terminología inglesa Single Euro Payments Area), que establece la liberación de las transferencias internacionales electrónicas, con lo que el dinero objeto del fraude, ya sean de banca electrónica o de comercio electrónico, se transfiere libremente de un país a otro, dificultando aún más la acción policial y judicial. Las *mulas* españolas empiezan a recibir el dinero procedente de fraudes cuyas víctimas se hallan en terceros países europeos, y viceversa.

Tal es la actividad de captación de *mulas* mediante las técnicas de engaño, que se ha creado en torno a él redes de delincuentes especializados en el tema, capaces de diseñar engaños, acompañados de la infraestructura tecnológica necesaria, como son páginas web simulando empresas o negocios legales, capaces de obtener listados de usuarios que concurren, aportando sus currículos, a portales de trabajo, y capaces de lanzar campañas dirigidas a estos usuarios seleccionados para el engaño, que la función de captación de *mulas*, también se empieza a ofrecer como servicio para el mundo del crimen organizado.

Por último, hay que tener presente que la función de la *mula* no es otra que recibir el dinero, procedente del fraude, en su cuenta corriente

y remitirlo, previa comunicación, vía empresa de transferencia de dinero, a un tercer destinatario. Como ya se ha comentado en anteriores apartados, el fraude en la red que se sufre en el espacio europeo proviene mayoritariamente de organizaciones delictivas afincadas y naturales de países del este. Algunas de ellas, especialmente desde que se compartimenta las fases del fraude ofreciéndose como servicio, se afincan en Reino Unido. Por tanto, el dinero debe dirigirse hacia esos destinos. Esto nos obliga a tener en cuenta dos aspectos, que el responsable de las *mulas* ha de ponerse en contacto con la *mula* para indicarle donde ha de enviar el dinero y que el dinero transferido deja un rastro en los operadores de transferencia de fondos.

Las comunicaciones de los responsables con sus *mulas* siempre es telemática. Para ello se utilizan redes que permiten anonimizar las comunicaciones, servidores comprometidos donde se instalan servidores de correo y las clásicas cuentas de servidores webmail anónimos, como Hotmail, Yahoo o Gmail. Esta es otra de las funciones que los grupos organizados dedicados a la captación de *mulas* asumen en su portfolio de servicios.

Para evitar la trazabilidad del rastro del dinero, el sistema de *mulas* también se utiliza en destino. Es decir, la remisión del dinero por las empresas de envío internacional de fondos no es directa al *phisher*, sino que en destino también lo reciben *mulas* que, posteriormente, directamente o a través de un recaudador, lo entregan al *phisher*. Esta diversificación dificulta sobremanera la acción policial incluso contando con la excelente colaboración de las empresas de envío de dinero, sistema legal y muy útil especialmente para los numerosos colectivos que sufren el fenómeno de la inmigración.

Los timos en la red

No podemos finalizar este documento sin hacer referencia a la pequeña delincuencia organizada que se genera en torno a los timos. El concepto de timo, engaño mediante promesa de ganancias fáciles de dinero, ha existido desde siempre en la vida real. Pero para ser víctima de esos engaños, resultaba preciso cruzarse en el camino del timador. Ahora, Internet, nos ha acercado a todos a los timadores. Servicios tan populares como el correo electrónico, utilizados por todos, nos convierten en potenciales víctimas de los timadores que remiten de forma masiva, a modo de *spam*, mensajes con supuestos de importantes ganancias fáciles, que no son otra cosa que burdos engaños para estafarnos.

Quizá el más popular de todos los timos en la red sean las cartas nigerianas. En ellas se alude a supuestas fortunas de ciudadanos africanos que por razones políticas de exilio o de accidentes inesperados, han fallecido dejando su dinero sin un legítimo sucesor o con trabas administrativas para que éstos puedan disponer del dinero. La participación de la víctima se reduce al pago de una pequeña cantidad de dinero en concepto de impuestos, sueldos para comprar a empleados bancarios corruptos o a funcionarios que falsificarán documentos oficiales, convirtiéndole en legítimo destinatario de fortunas que siempre rondan cifras millonarias de dólares. A cambio de esta colaboración los beneficios que se pueden obtener rondan los 10 ó 15 millones de dólares.

En ocasiones los mensajes recibidos con este tipo de fraudes son burdas traducciones del inglés, en las que se evidencia el engaño por todas partes. En otras, tienen una perfecta redacción e incluso son acompañadas de enlaces a webs en los que se hace referencia al fallecimiento o exilio del millonario africano. Lógicamente, estas páginas son falsas, creadas por los propios timadores.

El segundo timo más popular es el de las loterías internacionales, en las que se avisa de la ganancia de un premio millonario. Suelen vincularse a servicios de apuestas existentes, tipo Bonoloto española o europea. La participación del agraciado (timado) está originada por supuestas empresas que, para promocionarse, asocian cuentas de correo electrónico a números que participan en el sorteo. La ganancia siempre está en torno a fortunas de 50 millones de euros y la obligación del premiado es adelantar el pago de tasas o comisiones para la empresa encargada de gestionar los números ganadores. Igual que en el anterior timo, las comunicaciones se adornan con copias de páginas oficiales de los organismos de loterías.

Este tipo de timos están liderados por bandas organizadas de ciudadanos nigerianos, que fueron quienes empezaron con esta actividad con las famosas cartas nigerianas. Por eso, a estos timos también se les conoce como los fraudes del *Scam del 419*, en alusión al número del artículo del código penal nigeriano en que se tipifican los fraudes. Su estructura organizativa está a caballo entre Nigeria, de donde se envían muchos de los mensajes cebo, y Reino Unido y España, donde está el aparato encargado del cobro y de buscar los reclamos necesarios para orquestar los timos.

La incidencia de esta estafa es pequeña y las víctimas se sitúan mayoritariamente entre los ciudadanos americanos y asiáticos, y al igual que con las bandas de subsaharianos, el beneficio es pequeño. Permite

a pequeños grupos organizados subsistir, lo que les lleva a hacer de esta actividad su estilo de vida.

BIBLIOGRAFÍA

FERNÁNDEZ TERUELO Javier Gustavo, *Cibercrimen, los delitos cometidos a través de Internet*, Oviedo, Constitutio Criminalis Carolina, 2007,181.

HERNÁNDEZ GONZÁLEZ Claudio, *Hackers, piratas tecnológicos*, Madrid, Coelma, 1998, 410.

MATA Y MARTIN Ricardo M. «Criminalidad Informática: una introducción al cibercrimen», *Actualidad Penal*, nº 37, 2003, 127.

PANDA SECURITY, *Datos bancarios al descubierto*, publicado en julio de 2009, disponible en [www.pandasecurity.com/img/enc/Boletines%20PandaLabs4.pdf]

PANDA SECURITY, *El Negocio de los Falsos Antivirus*, publicado en julio de 2009, [disponible en

www.pandasecurity.com/img/enc/El%20Negocio%20de%20los%20falsos%20antivirus.pdf]

PANDA SECURITY, *Informe anual año 2009*, publicado en Enero 2010, [disponible en www.pandasecurity.com/img/enc/Informe_Anual_Pandalabs_2009.pdf]

PANDA SECURITY, *Informe trimestral Abril-Junio 2010*, [disponible en www.pandasecurity.com/img/enc/Informe_Trimestral_PandaLabs_T2_2010.pdf]

SANZ MULAS Nieves, *El desafío de la Criminalidad organizada*, Granada, Comares S.L. 2006, 280.

S21sec, *Informe análisis: Apuestas y fraude en Internet 2009, p*ublicado en febrero de 2010, [disponible en www.s21sec.com/descargas/Apuestas_fraude_S21sec.pdf]

S21sec, *Informe especial: Carding y Skimming,* publicado en febrero de 2010

S21sec, *Informe de Fraude Online y Cibercrimen 2005-2009,* [disponible en www.s21sec.com/servicios.aspx?sec=157&apr=202]

SYMANTEC, informe Norton Online Family report 2010

SYMANTEC, Informe Norton Online living report 2009