ANEXO III TEMA 33

GLOSARIO DE TERMINOS DE DELITOS TECNOLÓGICOS.

CONCEPTOS RELACIONADOS CON EL CIBERCRIMEN

- **Vulnerabilidad**: Aquello que es susceptible de ser utilizado para comprometer la seguridad. Puede deberse a errores en la programación, fallos en el diseño del *software* o la interacción entre distintos sistemas, así como a usuarios poco formados y a malas políticas de seguridad.

- ***Hacker* o *white hat*.** Experto informático que se dedica a demostrar vulnerabilidades en los sistemas de seguridad informática y demostrar lo que es capaz de hacer. Los *hackers* que basan su actuación en teléfonos móviles se conocen comúnmente como ***phreakers*.**

- ***Cracker* o *black hat***. Del inglés *to crack*, que significa 'romper' o 'quebrar'. Experto informático que se vale de su habilidad por objetivos destructivos o delictivos.

- ***Lamer***. Persona con ganas de hacer *hacking*, que presume de tener unos conocimientos o habilidades que realmente no posee ni tiene intención de aprender, a pesar de llevar suficiente tiempo dedicado a ello.

- ***Defacer*.** Persona que se dedica a explotar fallos en sitios web con ayuda de programas (tendencia de convertirse en *lamer*) o bien, a través de conocimientos propios (puede llegar a *cracker* o *hacker*). Lo hacen por diversión o por manifestar su inconformidad antes ciertas páginas, aunque algunos intentan retar o intimidar a los administradores.

- ***Copyhackers***. Conocidos en el terreno del *crackeo* de *hardware*, del sector de tarjetas inteligentes empleadas en sistemas de televisión de pago. Fines lucrativos.

- ***Newbie*.** Es un novato. Aquel que, navegando por Internet, descubre un área de descarga de buenos programas de *hackeo* y se los baja para trabajar con ellos. Al contrario que los *lamers*, los *newbies* aprenden el *hacking* siguiendo todos los cautos pasos para lograrlo y no se mofan de sus logros.

- ***Script kiddies* o *skiddies***. Similar al *lamer*, se trata de un individuo no cualificado que utiliza *scripts* o programas desarrollados por otros para atacar sistemas informáticos y redes y defectos de sitios web. Generalmente son niños que carecen de la capacidad de escribir programas sofisticados o *exploits* y que su objetivo es intentar impresionar a sus amigos. Sin embargo, el término no se relaciona con la edad real del participante.

- ***Exploits***: Son piezas de *software* específicas para un *software* y vulnerabilidad concretos que permiten obtener resultados no deseados por los propietarios del *software*, como conseguir acceso a un sistema informático de forma ilegítima.

- **Vulnerabilidades *zero-day***: Son vulnerabilidades desconocidas para los responsables del *software* al que afecta. El conocimiento de estas vulnerabilidades, y de los *exploits* que se pueden utilizar para aprovecharlas, es recompensado por los fabricantes y otras empresas, y puede obtenerse mucho dinero por su venta en mercados *underground*.

- **Ingeniería social:** Permite comprometer la seguridad a través de engaño de los usuarios del sistema informático. El objeto es que revelen información que permita vulnerar su seguridad, como convencer a través del teléfono a un empleado de que le está llamando el servicio técnico de la empresa y que necesita que le suministre las claves del ordenador para instalar *software*, o bien que abra una herramienta de control remoto.

- ***Psicohacking* o *hacking* psicológico**: Es uno de los pilares fundamentales sobre los que se sustenta la ingeniería social.
  Psicohacking es la disciplina que engloba los principios de psicología, sociología y antropología que explota la ingeniería social aprovechando la repercusión en nuestras vidas del uso de las nuevas tecnologías (correo electrónico, mensajería instantánea, *Smartphone* o redes sociales).
  Los *psicohackers* realizan experimentos y análisis de la conducta humana valiéndose de programas informáticos con los que observan tendencias y, de esta manera, intentan engañar a la víctima para obtener un beneficio (infectar su dispositivo al abrir un archivo u obtener información personal con el fin de acceder a sus cuentas bancarias).

- **Ataque por fuerza bruta**: Probar combinaciones de contraseñas hasta que se da con el resultado correcto que permite el acceso al sistema con una seguridad.

- ***Man in the Middle***: Su nombre significa literalmente «hombre en el medio» y esa es la idea: conseguir que las comunicaciones entre el sistema víctima y el otro sistema con el que este se está comunicando pasen por el atacante, con lo que el atacante actúa de intermediario de la comunicación de forma inadvertida para los interlocutores víctima.

- ***Defacements***: Consisten en modificar o desconfigurar el aspecto de una web para que esta muestre lo que al atacante desee en vez de su contenido original. Normalmente, la intención de los atacantes no es más que mostrar un mensaje reivindicativo o propagandístico, lo que abarca desde el típico *hackedby* de *hackers* que solo busca notoriedad a los mensajes proyihadistas.

  Ataques de denegación de servicio, (DoS: *denial of service*), son el arquetipo de ataque contra la disponibilidad. Pueden afectar a páginas web, aplicaciones o servidores completos. El método más habitual se basa en la saturación de los recursos del servidor, bien porque la cantidad de conexiones limite sus capacidades computacionales, bien porque la cantidad de información que reciba sature su conexión, de forma que no pueda atender a los usuarios legítimos.

- ***Phishing*:** Viene de la palabra inglesa *fishing*, literalmente «pescando», y es un ataque de ingeniería social que consiste en suplantar la plataforma de una entidad que al usuario de servicios informáticos y/o telemáticos le genera, en apariencia, confianza (usando su logotipo, colores, diseños, lenguaje, etc.) para sustraer o robar información personal y/o financiera, a la que el usuario llega por medio de un correo o redirección de un sitio web. Normalmente los datos robados consisten en su usuario y contraseña.
  Posteriormente, el sujeto fraudulento hace uso de dichos datos en perjuicio de su legítimo usuario haciendo transferencias de cantidades económicas, utilizando los datos de las tarjetas de débito para efectuar pagos no deseados por su legítimo propietario, etc.

  El término *phishing* encuentra su origen en la analogía entre este delito y el concepto de

pesca (del término inglés *fish* «pescado»), según el Anti-Phishing Working Group, referente en la investigación y lucha contra esta dinámica delictiva (se entiende dada la «pesca virtual» de todo tipo de información sensible del usuario).

En el phising bancario de forma previa o simultánea a la captura de las credenciales bancarias de las víctimas de este fraude, se efectúa la apertura de cuentas puente o intermediarias. Las cuentas intermediarias pueden estar abiertas por miembros de la organización o bien por personas ajenas a ella. Estas últimas son captadas a través de supuestas ofertas de trabajo y desempeñan el papel de las denominadas ***moneymules*** **o «mulas de dinero»**.

- ***Spearphishing*:** Consiste en enviar el correo electrónico de *phishing* bien personalizado según la víctima y su situación actual. Son ataques dirigidos a victimas concretas.

- ***Phishing unicode***. Nuevo tipo de phishing que consiste en crear una página fraudulenta en la que la URL en lugar de ser letras del código ASCII contiene caracteres de tipo cirílicos, que a simple vista tienen el mismo aspecto, pero sin embargo tiene diferente representación Unicode. A este tipo de ataque se le conoce como *phishing homográfico* o ataque de *phishing* mediante el uso de caracteres Unicode.

  Por otro lado, para dotar de mayor credibilidad al fraude, se puede utilizar una autoridad certificadora que expide certificados gratuitos (Let's Encrypt). De esta forma, el usuario ve el candado verde y el https en la URL.

- ***Vishing*.** Similar al *phishing* pero con teléfonos. El *vishing* consiste en el uso de técnicas de ingeniería social junto con VoIP (voz sobre IP) para engañar a la víctima mediante una llamada telefónica, por medio de una voz computerizada, y conseguir que esta facilite información sensible (datos personales y/o información bancaria). El término es una combinación del inglés *voice* (voz) y *phishing*.

- ***SMiShing*.** Tipo de delito o actividad criminal utilizando técnicas de ingeniería social por medio del empleo de mensajes de texto (**SMS**) dirigidos a los usuarios de telefonía móvil, a los que se solicitan datos, que se llame a un número o se pide que se entre a una determinada web. El *SMiShing* es una variante del *phishing*.

  Mediante reclamos atractivos con alertas urgentes, ofertas interesantes o suculentos premios, tratan de engañar al usuario aprovechando las funcionalidades de navegación web que incorporan los dispositivos móviles actuales.

  El objetivo es redirigir al usuario a una página web fraudulenta con el propósito de obtener información personal, apropiarse de datos bancarios o infectar el dispositivo móvil. En otras ocasiones tratan de convencer al usuario para que llame a un número de tarificación especial, se suscriba a un servicio SMS *premium* de forma ilícita o simplemente tratar de vender algún servicio o producto inexistente pagando cierta cantidad por ello.

- ***Spoofing***. Uso de técnicas a través de las cuales un atacante, generalmente con usos maliciosos o de investigación, se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación.

- ***Pharming*.** Consiste en introducir en el ordenador un código malicioso que modifique el sistema de resolución de nombres en Internet (cuando un usuario introduce una dirección en su navegador de Internet, esta es convertida en una dirección IP numérica, de lo que se encargan los servidores DNS), de modo que, a pesar de que el usuario esté introduciendo la dirección de la página web de su entidad bancaria o de otro servicio correctamente en el explorador de Internet, este código modifica la conversión haciendo que el usuario acceda realmente a la dirección IP de la página web falsa.
  Normalmente el *hacker* realiza un ataque al servidor DNS, puede modificar el llamado archivo *hosts* o directamente al *router*.

  Un servidor DNS (*domain name system* o «sistema de nombres de dominio») es un servidor que traduce nombres de dominio a IP y viceversa. En las redes TCP/IP, cada PC dispone de una dirección IP para poder comunicarse con el resto de PC. Es equivalente a las redes de telefonía en las que cada teléfono dispone de un número de teléfono que le identifica y le permite comunicarse con el resto de teléfonos.

  Lo que diferencia principalmente el *phishing* del *pharming* es que este último el *hacker* realiza un ataque redireccionando los servidores DNS, modificando el archivo *host* o directamente el *router* o el *firewall*.

  El archivo *host* de un ordenador es usado por el sistema operativo para guardar en el PC la correspondencia entre dominios de Internet y direcciones IP.

- **Fraude del CEO**: Requiere averiguar qué empleados tienen capacidad de hacer transferencias en nombre de la empresa. Una vez averiguado esto, se suplanta a un alto cargo de la empresa y mediante ingeniería social, imitando los correos de este alto cargo, se solicitan trasferencias cuantiosas hacia las mulas de la organización criminal, con la excusa de una situación de emergencia en la empresa que impide realizar el trabajo por los cauces habituales o comprobar lo que se pide.

- ***Sniffer*.** Es una clase de *software* que permite capturar el tráfico de una red informática, tanto si esta red está basada en *ethernet* (por cable) como si es wifi (inalámbrica).

- ***Typosquatting*.** Es un tipo de amenaza cibernética que puede poner en serio riesgo a nuestro equipo, a partir de que erremos en una letra de la escritura de una dirección URL. Es por eso que este tipo de ciberataque también se le llama URL *hijacking* (secuestro de URL). Los cibercriminales que lo utilizan se encargan de registrar direcciones derivadas del nombre de algún sitio famoso en internet, pero que contiene evidentes errores de ortografía o tipeo. Los *ciberquatters* cargan en los sitios malintencionados material peligroso para el PC, usualmente *ransomware*.

- ***PIN Logger***. Muchas aplicaciones reclaman permisos excesivos y extraen valores de los sensores integrados. Es posible utilizar esto de forma maliciosa con un nuevo ataque llamado *PINLogger*, el cual interpreta datos de los sensores y calcula el número pin.
  Al contrario de otros ataques, *PINLogger* no requiere la instalación de software en el *smartphone*. Todo lo que necesita es que un navegador con el código malicioso en una página web «quede abierto» mientras el usuario ingresa el pin.

- ***Cibersquatting*** (ciberocupación). Acto de comprar un dominio con un nombre comercial que ya existe en el mundo o muy parecido, pero sin estar registrado, para posteriormente

venderlo por una suma generosa a la empresa en cuestión.

- ***Domainer***. Persona que especula con la compra y venta de nombres de dominios.

- ***Trashing***. Consiste en rastrear en las papeleras de reciclaje de nuestro ordenador en busca de información, contraseñas o directorios.

- ***Skimming***. Robo de información por clonación (copiar banda magnética) de tarjetas de crédito/débito en cajeros automáticos en el momento de la transacción.

- ***Carding***. adquisición de productos o servicios en comercios virtuales con tarjetas de crédito/débito válidas sin conocimiento ni autorización de sus titulares, obtenidas ilegalmente o siendo generadas por programas.

- **Bomba lógica**. Piezas de un código o de una aplicación que permanecen inactivas hasta que se cumple una determinada condición que las hace activarse.

- ***Spam*** (Comunicaciones comerciales no solicitadas). Envío masivo de correos electrónicos a un número indiscriminado de personas, supuestamente en nombre de entidades bancarias reconocidas que imitan el diseño de sus webs. En los correos se solicita a los usuarios que, por motivos de seguridad, mantenimiento, mejora del servicio, confirmación de identidad o cualquier otro pretexto, actualicen sus datos personales (nombres de usuario, claves y contraseñas de cuentas bancarias, número de tarjetas de crédito, etc.).

- ***Hoax***. En términos de delitos informáticos son sinónimos de las cadenas formadas por envíos y reenvíos de correos electrónicos (*emails*) que, generalmente, difunden noticias falsas o rumores con el objetivo de obtener direcciones de correo para generar correo basura.
  Los ***hoaxes*** (broma o engaño) son mensajes con falsas alarmas de virus o de cualquier otro tipo de alerta o de cadena (incluso solidaria o que involucra la salud) o de algún tipo de denuncia distribuida por correo electrónico, cuyo común denominador es pedirles a los usuarios que los distribuya a la mayor cantidad de personas posibles. Su único objetivo es engañar y/o molestar.
  No se deben confundir con las publicaciones *spam* (publicidad) o con las publicaciones con enlaces maliciosos (que llevan a webs infectadas).

- ***Gossipping.*** Consiste en la creación de foros y salas de chat anónimas donde se comentan rumores que pueden derivar posteriormente en algún tipo de delito.

- ***Bluejacking***. Se hace uso de teléfonos móviles haciendo uso de la tecnología *bluetooth* con la intención de enviar mensajes anónimos a otros teléfonos.

- ***Bluesnarfing***. Acceso no autorizado a la información guardada en teléfonos móviles, ordenadores y tablets haciendo uso de una conexión de *bluetooth*.

  Un sujeto se puede introducir en un teléfono móvil y copiar, ver o incluso modificar ciertas partes. El acceso tiene lugar desde un dispositivo cercano sin que ello cause alerta, en ningún caso, al propietario.

- ***Flaming*.** Discusión que se lleva a cabo en línea (por medio de correos electrónicos, redes, blogs o foros) que toma un tono insultante o desagradable hacia una de las personas con el

objetivo de crisparla y/o imponer los puntos de vista de la otra.

Un *flame* (a veces traducido al español como *desahogo*, *puñal* o *flamazos*) consiste en un mensaje deliberadamente hostil o insultante enviado sin ningún propósito constructivo, en consecuencia, *flaming* (en ocasiones castellanizado como *flamear*) es el acto de publicar usualmente en el contexto social de un foro o una lista de correo electrónico, y aquel que los envía recibe el nombre de *flamer*. A veces se publican como respuesta a un cebo (en inglés *flamebait*), un mensaje provocativo, pensado especialmente para generar respuestas insultantes.

- **Trol.** En la jerga de Internet, un trol o *troll* describe a una persona que publica mensajes provocadores, irrelevantes o fuera de tema en una comunidad en línea, como ser un foro de discusión, sala de chat, comentarios de blog, o similar, con la principal intención de molestar o provocar una respuesta emocional negativa en los usuarios y lectores, con fines diversos (incluso por diversión) o, de otra manera, alterar la conversación normal en un tema de discusión, logrando que los mismos usuarios se enfaden y se enfrenten entre sí.

- ***Fake*.** *Fake* («falso» en inglés y en el mundo de Internet) se refiere en general a una falsificación de cualquier tipo de contenido, se utiliza para describir un montaje fotográfico, un anuncio falso, etc.

- ***Malware* o «programa maligno»:** *programa informático o virus específicamente diseñado para perturbar o dañar un sistema*. Los términos «programa maligno» y «programa malicioso» no son sinónimos, ya que «programa malicioso» hace referencia al que se introduce en un sistema operativo con mala intención, pero sin dañar el equipo.

- **VIRUS**. Es un programa informático diseñado para dañar de alguna forma el equipo o dispositivo al que ataca y que cuenta con dos características principales: actúa de forma transparente al usuario y tiene la capacidad de autorreplicarse.

La principal característica de los virus informáticos es que inyectan su código malicioso en otros programas, como si de su ADN/ARN se tratara, para así replicarse y abstraerse de los sistemas de seguridad (el «sistema inmunológico») del sistema al que infecta. Lo que se infecta son los ficheros mediante código maligno, aunque para ejecutarse requieren que el programa infectado sea ejecutado, por lo que suelen necesitar interacción humana.

El primer virus informático fue **Creeper**, diseñado por **Bob Thomas en 1971**, aunque su objetivo no era causar daño a los equipos infectados, sino que se trataba de un experimento para comprobar si se podía crear un programa que se moviera entre ordenadores como había propuesto en 1939 el científico matemático John Louis Von Neumann.

El término *virus informático* no fue acuñado hasta la década de los ochenta, cuando aparecieron los primeros virus que se propagaron masivamente entre ordenadores, como Elk Cloner, programado por un estudiante de 15 años para los Apple II.

Tipos de virus más comunes:

1. **Virus de acción directa**. No permanece en la memoria, pues actúa según se ejecuta, al venir camuflado dentro de archivos .exe. Es preciso que el usuario los ejecute para funcionar y, una vez lo haga, se expanden con facilidad en busca de archivos similares. Aunque está considerado como uno de los más fáciles de eliminar, puede llegar a inutilizar ciertos archivos o programas.

2. **Virus residente**. Se instala en el equipo oculto en la memoria RAM, y pueden llegar a afectar a programas y archivos una vez se ejecutan. Es el más contagioso y el que infecta con mayor facilidad. Se distinguen dentro de estos dos subtipos, aquellos que desaparecen una vez que el ordenador se apaga debido al vaciado de la memoria RAM, y los que permanecen en el equipo reinstalándose cada vez que se inicia este. Son difíciles de eliminar.

3. **Virus del sector de arranque**. Reside en la memoria e infecta al sector de arranque. Es el más clásico y el más peligroso. Podemos encontrarlo en discos duros, memorias extraíbles o a través de archivos maliciosos en correos electrónicos.

4. **Virus de sobreescritura**. Su función es sobreescribir o destruir la información que encuentra a su paso. No es uno de los más peligrosos, pero sí molesto. La única forma de eliminar el virus es eliminar el archivo afectado con la consiguiente pérdida de los datos.

- **Gusanos**. Son un tipo de *malware* cuya principal característica es la capacidad de autopropagación. Tiene la habilidad de autorreplicarse, aunque su único objetivo es el de aumentar su población y transferirse a otros ordenadores a través de Internet o dispositivos de almacenamiento.
  A diferencia de los virus, los gusanos se pueden propagar de ordenador a ordenador sin la necesidad de interacción humana, ya que trabajan en secreto de espaldas al usuario.
  En principio no realizan ningún daño sobre el equipo, aunque por su naturaleza normalmente consumen espacio en el disco duro y, como consecuencia, pueden llegar a ralentizar la velocidad del ordenador si lo hacen a gran escala.
  Otra de las diferencias entre el gusano y el virus informático es que el primero no necesita infectar los archivos de los programas, sino que entra directamente en la memoria para duplicarse a sí mismo.

  El **gusano Morris** ha pasado a los libros de historia como el primer *malware* de este tipo.
  Hoy en día los gusanos informáticos se utilizan para crear **redes de *bots*** gigantescas que controlan a ordenadores en todo el mundo, denominados ***zombies***, que se utilizan para enviar *spam*, lanzar ataques de denegación de servicio (DoS) o descargar todo tipo de *malware*.

- **Troyanos**: Los troyanos no son virus, sino un tipo de *malware* que no se autopropaga y que, aparentando ser un programa legítimo, tiene por objetivo proporcionar una puerta trasera de cara a otros programas maliciosos o ciberdelincuentes, para que puedan instalar funcionalidades indeseadas por el usuario, sin su consentimiento ni su conocimiento, habitualmente anulando sistemas de seguridad.

  A diferencia de los gusanos informáticos, los troyanos no son capaces de propagarse por sí

solos. Su nombre proviene, evidentemente, de la historia del caballo de Troya mencionada en la Odisea de Homero.

Los más peligrosos pueden actuar como ***keyloggers* o *sniffers*** de teclado que transmiten las pulsaciones realizadas sobre el teclado de la víctima.

Existen mil maneras de infectarse con un troyano, desde la descarga de programas de redes P2P, páginas web que contienen contenido ejecutable, *exploits* en aplicaciones no actualizadas o archivos adjuntos en correos electrónicos.

Los síntomas pueden ser imperceptibles para gran parte de los usuarios, aunque algunas acciones como la aparición de pantallas poco habituales, modificaciones del escritorio, lentitud en el sistema operativo o el acceso a páginas de Internet sin consentimiento del usuario son señales de un posible troyano.

- ***Keyloggers* o *sniffer*** de teclado (registradores de teclas). *Software* o *hardware* cuya funcionalidad básica es interceptar y guardar las pulsaciones que se teclean en el sistema que haya sido infectado para poder transmitirlas posteriormente al ciberatacante. De esta forma, se puede tener acceso a los datos personales, nombres de usuario, contraseñas, números de tarjeta de crédito, etcétera.

  Este *malware* se sitúa entre el teclado y el sistema operativo para interceptar y registrar la información sin que el usuario lo note. Un *keylogger* o *sniffer* de teclado almacena los datos de forma local en el ordenador infectado y, en caso de que forme parte de un ataque mayor, permite que el atacante tenga acceso remoto al equipo de la víctima y registre la información en otro equipo.

- **Puerta trasera o *backdoor*:** Su papel es crear la posibilidad de acceso remoto al sistema infectado. Normalmente solo el que ha instalado esta puerta trasera tiene la posibilidad de utilizarlo, ya que el acceso está oculto y requiere algún tipo de contraseña o autenticación para usarse. A veces lo utilizan los fabricantes para tener control sobre sus productos con distintas finalidades.

- ***Dropper*:** Es un *malware* cuya única función es ser el contenedor de otro, llamado *payload*. Lo habitual es que ofusque el código del *malware* que contiene para evitar ser detectado antes de su ejecución. Puede tener funcionalidades para anular sistemas de seguridad del sistema atacado y asegurar el éxito de la infección de su *payload*. También es habitual que detecte si está siendo analizado para inhibir su funcionamiento y dificultar su análisis.

- ***Downloader*:** Es similar al *dropper*, pero, en vez de contener su *payload* dentro del propio *malware*, lo descarga desde un servidor controlado por el atacante. Frente al *dropper*, tiene la ventaja de permitir cambiar fácilmente el *payload* sin tener que reconfigurar el *downloader* (simplemente hay que cambiar en el servidor el *payload* que se quiera descargar). También puede estar configurado para descargarse un *payload* u otro en función de los datos del sistema infectado, o bien para informar de estos al servidor malicioso con el objetivo de que le suministre el *payload* adecuado.

- ***Spyware*:** Un programa espía o *spyware* es un *malware* que se puede instalar por sí solo o ejecutarse en el equipo a través de otro programa sin consentimiento ni conocimiento del usuario. Los programas espía suelen trabajar a escondidas, a diferencia del *adware*,

intentando ocultar cualquier rastro o síntoma al usuario, aunque a menudo afectan al rendimiento del equipo.

Su funcionalidad principal es recopilar datos del sistema infectado y de sus dispositivos de memoria para enviarlos remotamente al atacante. A diferencia de los virus y de los gusanos informáticos no tiene la habilidad de autorreplicarse, por lo que su funcionamiento habitualmente se compara al de un parásito.

- ***Adware*:** El *adware* en realidad no es más que una clase de *spyware*. Además, los programas *adwares* no tienen intención alguna de dañar el ordenador infectado, así que tampoco se ajustan del todo a la definición de *malware*.

  Su función es mostrar publicidad en ventanas en las que deberían aparecer páginas web o bien, durante la instalación o la ejecución de un programa, habitualmente los gratuitos, ya que esta fórmula se articula como su única fuente de ingresos. Suele cambiar páginas de inicio de navegadores y alterar las búsquedas del usuario para mostrar enlaces a más anuncios. Puede tener funcionalidades *spyware* con el objeto de decidir qué anuncios se ajustan mejor a las preferencias del usuario y así tener más visitas.
- ***Ransomware*:** Las formas *programa de secuestro* o *secuestrador* y *programa de chantaje* o *chantajista* son posibles alternativas en español a ese anglicismo.

  En sus comienzos, la funcionalidad específica de este *malware* era bloquear de alguna forma el equipo y solicitar un rescate (de *ransom*, «rescate») a cambio de su liberación, mostrando un mensaje que alertaba de la presencia de un potente virus basándose en que el usuario había cometido diferentes delitos relacionados con las descargas y pornografía. Para ello, hacía uso de imágenes y logotipos de las fuerzas y cuerpos de seguridad del Estado, lo que añadía una dosis de credibilidad al fraude. Para desbloquear el equipo, la víctima debía pagar una cantidad a través de servicios de envío de efectivo, como Ukash o Paysafecard.

  Pertenece a este apartado el famoso «virus de la Policía», que, en sus diversas variantes (desde el FBI a Correos o la Guardia Civil) y dispositivos infectados, consistía básicamente en desplegar una pantalla que impedía usar con normalidad el sistema y en la que, simulando ser la Policía, se acusaba al usuario de haber consumido pornografía infantil, programas o música pirateada o haber cometido otro tipo de acto ilícito. De esta manera, se solicitaba el pago de una multa por estos hechos para no iniciar un procedimiento penal. El virus de la Policía se propagó especialmente a través de los anuncios de las webs pornográficas, lo que facilitaba que las víctimas cayeran en el engaño de la pornografía infantil. Su posterior evolución llegó a infectar también a los *smartphones*.

  Cuando las campañas comenzaron a no ser tan rentables para los ciberdelincuentes, el *ransomware* evolucionó. Su objetivo ya no era únicamente bloquear el dispositivo, sino que también se fijó en la información que este alojaba, ya que el sistema operativo es fácilmente reemplazable pero la información contenida en su disco duro, en muchas ocasiones, no. Esta variante del *ransomware* basaba su funcionamiento en cifrar los archivos personales de la víctima impidiendo su acceso, y en caso de querer recuperarlos, debía pagar el rescate solicitado, generalmente en *bitcoins*, que es una moneda virtual difícilmente rastreable.

  La variante anteriormente descrita sigue siendo muy efectiva en la actualidad, pero el objetivo de los ciberdelincuentes se ha diversificado, no fijándose únicamente en los archivos personales. Motivados por la existencia de gran cantidad de dispositivos cotidianos

con acceso a Internet, conocidos como el *Internet de las cosas* o IoT (*Internet of things*), los ciberdelincuentes han encontrado un filón que ya han comenzado a explotar.

Hay que tener en cuenta, que cualquier dispositivo conectado a Internet, como los televisores inteligentes o *smartTV*, son susceptibles de ser víctimas del *ransomware*. A esta práctica se la conoce como *ransomware of things* o *RoT*. Ya se han dado casos de televisores inteligentes infectados con un *ransomware* similar al anteriormente mencionado «virus de la Policía».

El método de infección más común en cualquier dispositivo inteligente procede de la instalación de aplicaciones que no provienen de la tienda oficial.

- ***Scareware*** (aplicaciones milagro y falsos optimizadores para tu *smartphone*). Aplicaciones que prometen funcionalidades milagrosas y optimizadores para nuestro móvil.

  Cuando navegamos por Internet a través de nuestro móvil, es bastante frecuente encontrarnos con ventanas que nos informan de situaciones como que nuestro dispositivo no está funcionando de manera óptima, que está infectado por *malware*, que tiene problemas en la batería o cualquier otro mensaje alarmante cuyo objetivo es confundir al usuario.

  No se trata de un engaño nuevo, ya que los usuarios de los ordenadores se han visto afectados por estas prácticas durante años, pero con el auge de los dispositivos móviles el *scareware* ha evolucionado y sus mensajes alarmantes se han ido adaptando. Se utilizan técnicas de ingeniería social como un contador de tiempo, mostrar la marca y modelo del dispositivo que estamos utilizando o hacer que vibre el *smartphone*. Todo esto, unido a que algunas veces nuestro dispositivo móvil no funciona con la misma fluidez que cuando lo compramos, podría llevarnos a equívocos.

  Este tipo de aplicación milagrosa generalmente es de pago, con lo que sus desarrolladores ya habrán obtenido rédito económico. Pero este beneficio no se queda ahí, sino que la aplicación además puede:

  - Generar mayores ganancias económicas con publicidad.
  - Recolectar información personal del usuario en función de los permisos solicitados por la aplicación, que suelen ser excesivos. Esta información posteriormente la podrán utilizar en su propio beneficio o venderla.
  - Solicitar la instalación de aplicaciones alternativas, que lo más probable es que también sean de pago, para completar los servicios prometidos.
  - Solicitar el número para suscribirte a servicios de tarificación especial (SMS Premium).
  - Instalar *malware* en el dispositivo capaz de realizar tareas como descargar e instalar aplicaciones de forma transparente para el usuario (sin su conocimiento).

  ***Rootkit*:** Es un *malware* dedicado específicamente a ocultar que un sistema ha sido infectado, lo que logra ocultando procesos, archivos, conexiones de red, llaves de registro, etc., al usuario o a los programas antivirus. La diferencia del funcionamiento de un *rootkit* frente al de otro tipo de medidas que sobrepasan las medidas de seguridad del sistema infectado es que el *rootkit* afecta a las funciones del sistema operativo: estas trabajan normalmente hasta el momento en que son usadas para detectar el *malware*, y devuelven información falsa en este momento. Para entendernos, es como si pusiéramos al sistema operativo unas gafas que son transparentes, salvo cuando se mira el lugar donde está el *malware*, momento en el que muestran una imagen irreal para evitar que lo veamos.

- ***Botnet*:** Existe *malware* que busca convertir a los sistemas víctima en los llamados *bots*, conocidos como zombis o robots: sistemas que conjuntamente, en lo que se denomina una *botnet* (red de *bots*) o red zombi, responden a órdenes en remoto de un computador maestro o controlador (*botmaster* o «dueño de los *bots*»). Este control se lleva a través de los conocidos como *Command and Control* o centros de mando y control (C&C, C²), que son servidores a los que los sistemas infectados se conectan para recibir órdenes. Sus propietarios pueden no ser conscientes de ello.

  Un *bot* es una pieza de *software* que puede, de manera autónoma, ejecutar una tarea «en nombre de» una persona o entidad. Es decir, actúa «en representación» de un tercero, el cual puede no estar presente. Esta pieza de *software* tiene alguna variante de *trigger* o disparador incluido, el cual, cuando es ejecutado, hace que el agente desarrolle su actividad sin intervención futura.

  El uso de las *botnets* es muy variado y es muy habitual en ataques DoS, pero estas también pueden utilizarse para realizar transmisiones (las cuales pueden incluir código malicioso, *spam* que probablemente contenga *malware*, virus, etc.) hacia otros ordenadores conectados también a la red y para otros usos maliciosos.

Fraudes

Son muchas y muy variadas las tipologías delictivas que se desarrollan a través de la fenomenología de los fraudes en Internet. Las más comunes, por cuanto a su rentabilidad y casuística se refiere, son las que afectan a la banca *online* y al comercio electrónico. El delito tipo investigado fundamentalmente es la estafa a través de Internet, sea a particulares, empresas o entidades varias. Con el fin último de la estafa, en muchas ocasiones se hace necesario investigar otros delitos que complementan a aquella: la falsificación documental, el blanqueo de capitales, etc.

No obstante, una visión generalista de los fraudes en Internet hace referencia a las siguientes tipologías delictivas:

- **Transferencias electrónicas fraudulentas** (TEF). En líneas generales, esta actividad delictiva engloba otras tantas complejas e individualmente consideradas, como el *phishing*, el *pharming*, el *CEO FRAUD* / *SPEARPHISHING* / *BUSINESS EMAIL COMPROMISE*, la utilización de programas maliciosos conocidos como *malware* o la aplicación de diferentes técnicas de ingeniería social. En definitiva, el objetivo final en todos los casos será la obtención de importantes cuantías dinerarias, producto de la ejecución o inducción de transferencias bancarias *online* de carácter ilícito.

- **Ofertas de trabajo**. Relacionadas con las TEF, son también objeto de investigación las «OFERTAS DE TRABAJO» que tienen como finalidad mover el dinero producto de las transferencias fraudulentas y ponerlo en manos de los autores de la estafa, dentro o fuera de España (para lo que utilizan a los intermediarios conocidos como «mulas de dinero», que se captan mediante estas falsas ofertas de trabajo, publicadas generalmente en portales web de trabajo o anuncios clasificados).

- **Oportunidades de negocio** y timos del tipo «trabaje desde su propia casa». Se ofrece al potencial perjudicado la oportunidad de trabajar desde el hogar y la posibilidad de ser «su

propio jefe» mostrándole unos posibles ingresos muy elevados. Se le requiere a la potencial víctima, para iniciar el proyecto, invertir en la compra de alguna maquinaria o productos que tienen una difícil o nula salida.

- **Estafas en compraventas y subastas fraudulentas o ficticias en Internet**. Se trata del ofrecimiento de un bien o un producto adquirido en la Red que se paga y no se recibe (o que se entrega y el propietario no recibe el dinero), venta de vehículos, alquiler de inmuebles, etc. Estas operaciones se localizan generalmente en plataformas de anuncios, ventas y subastas *online* generalistas.

- ***E-commerce***. Las subastas y ventas ficticias usando páginas de venta donde el cliente realiza el pago por cualquier medio, pero no tiene el producto.

- **Pirámides e inversiones financieras**. Son ofertas realizadas a través del correo electrónico, los foros, las plataformas generalistas de anuncios, etc., que invitan al usuario a realizar pagos económicos, como la inversión en productos bancarios o financieros de diversa naturaleza (auspiciados por entidades del sector simuladas), la inversión en metales y/o piedras preciosas o simplemente por el acceso al carrusel de la pirámide propiamente dicha de socios inversores.

- ***Marketing*** **multinivel o redes piramidales**. Se promete hacer mucho dinero comercializando productos o servicios, ya sea uno mismo o los vendedores que nosotros reclutamos, pero realmente nuestros clientes nunca son los consumidores finales, sino otros distribuidores, con lo que la cadena se rompe y solo ganan los primeros que entraron en ella.

- Estafas relativas a **planes de inversión** que prometen grandes rentabilidades en poco tiempo. Promesas, a los potenciales inversores, de rentabilidades muy altas y predicciones financieras con seguridad absoluta sobre extraños mercados, siendo, realmente, operaciones financieras que suelen encubrir operaciones fraudulentas.

- **Juego y casinos *online***. La conducta generalista más habitual es la utilización de tarjetas de crédito o incluso cuentas bancarias de manera fraudulenta para abonar las jugadas o apuestas, o la no entrega de los premios que los ganadores obtienen.

- **Cartas nigerianas/scam 419**. Básicamente consisten en el envío masivo e indiscriminado de correos electrónicos (*spam*) que ofrecen a sus receptores la obtención de importantes sumas económicas por:

- Participar en supuestas transferencias de fondos gubernamentales, retenidos o excedentes de países en conflicto bélico o político (historia del soldado de Irak).
- Recibir supuestas herencias de familiares inexistentes o desconocidos (coincidiendo con acontecimientos concretos, como la caída de aviones, terremotos, tsunamis, hundimientos de barcos -u otras catástrofes- o atentados terroristas con gran número de víctimas).
- Recibir un supuesto premio de lotería *online*.

En todos los casos, se solicita al receptor interesado/víctima en cuestión el adelanto de diversas sumas de dinero para el pago de gestiones, despachos de abogados, gestorías, sobornos, comisiones o corruptelas. Las sumas de dinero solicitadas por los estafadores son elevadas, aunque proporcionalmente insignificantes y asumibles por la víctima, en

comparación con la fortuna, premio o herencia que se espera recibir.

Otras veces, esta tipología delictiva se ejecuta a través de páginas de contactos y redes sociales en las que el estafador, una vez se gana la confianza de la víctima, le plantea el supuesto negocio dinerario en cuestión o incluso, entablando de manera virtual algún tipo de relación amorosa con ella, le pide dinero para salir del país de residencia, para visados, para el viaje en el que ambos podrían conocerse personalmente, etc.

Solicitud fraudulenta de tarjetas de crédito. Consiste en la apertura *online* de cuentas bancarias utilizando documentación falsificada y domicilios preparados y controlados por los estafadores para la recogida de la documentación bancaria y la recepción de las tarjetas. Una vez preparada la logística anterior, aportando datos laborales y financieros falsos, los autores de la estafa solicitan tarjetas de crédito que permitan un límite elevado, para finalmente dejarlas en descubierto por distintos procedimientos: la ejecución de compras físicas o virtuales de bienes o servicios, la recarga a crédito de otras tarjetas de tipo virtual o cuentas bancarias intermediarias, la remisión de dinero a través de entidades *money-transfer*, etc.

- **Abuso de tarjetas de pago.** Se solicita, al legítimo propietario de la tarjeta de crédito o débito, el número de la tarjeta de crédito, alegándole una razón de seguridad o verificación rutinaria, y posteriormente se le realizan cargos de difícil cancelación.

- **Estafas en campaña.** Se conceptúan como tales aquellas estafas cometidas a través de Internet que se ejecutan en períodos temporales concretos y reiterados anualmente, o bien con motivo de algún acontecimiento público. Se engloban en este apartado las estafas en el alquiler de **apartamentos vacacionales** en época estival o bien aquellos alquileres dirigidos a estudiantes coincidiendo con el inicio del curso universitario. De la misma forma, suelen aparecer estafas en la venta de entradas *online* con motivo de ciertos eventos, como los conciertos musicales, o coincidiendo con la consecución de actividades o gestiones que los usuarios, en mayor o menor grado, tengan que realizar periódicamente, como la campaña anual del impuesto sobre la renta.

- ***Wangiri*.** En este tipo de fraude, la víctima recibe una llamada telefónica que no le da tiempo a contestar (ya que se corta cuando suena el primer tono) desde un número no identificado. Cuando la víctima decide devolver la llamada, al otro lado de la línea hay un contestador automático que le indica que, para poder recibir información de un servicio de su interés, tiene que realizar una llamada a otro número de teléfono, que será de tarificación adicional.

- ***La ballena azul*.** Hay grandes comunidades en Facebook en español que usan nombres como «La ballena azul» o «Ballena Azul». Son grupos cerrados, que requieren autorización de administradores para ingresar. En su descripción muestran una lista de 50 retos en 50 días, el último de los cuales supondría suicidarse.

  Las supuestas 50 pruebas no deberían realizarse de forma individual: hace falta un «guardián» o «curador» que supervise las pruebas.

  Los participantes deben realizar una prueba por día. Estas alternan autolesiones (cortes en brazos y piernas, pinchazos…), privación de sueño (quedarse despierto a las 4:20 o despertarse a esa hora), visionado de vídeos de terror o visitar sitios como azoteas, vías de tren... A los jugadores se les denomina *ballenas azules* y en otras pruebas tienen que

interactuar entre ellos o con su guardián.

En la prueba 26 del listado, el guardián indica al participante la fecha de su muerte. Después, hay una prueba que se repite durante 19 días y es una síntesis de las anteriores: consiste en despertarse a las 4:20, ver los vídeos de terror que el curador indique, hacerse un corte y hablar con otra ballena azul. La prueba 50 es «saltar de un edificio alto, tomar su propia vida».

Ni siquiera está claro el porqué del nombre del reto: la explicación más extendida es que se hace referencia al suicidio de las ballenas que, al igual que otros cetáceos y delfines, acabarían con su vida usando el método de acercarse demasiado a la costa para quedar varados.

- **Criptodivisa o monedas virtuales**. Las criptodivisas son un tipo de divisa virtual descentralizada que utiliza la criptografía y el esquema de red *peer-to-peer* para permitir que no sea necesario que exista una entidad que controle y regule el uso de esta divisa, sino que sea la propia comunidad la que garantice su funcionamiento.

  Actualmente, se usan en Internet como medio de pago en los mercados clandestinos de la *Darknet*, para pagar los «rescates» del *ransomware*, e incluso como forma de pago de extorsiones realizadas por cibercriminales, pero poco a poco se esta generalizando su uso cotidiano para operaciones legales.

  El *bitcoin* es una criptomoneda digital, descentralizada y anónima, creada bajo el pseudónimo Satoshi Nakamoto en 2008. Actualmente, es la criptodivisa más utilizada. La base tecnológica para el funcionamiento del *bitcoin* es la criptografía de clave asimétrica, la red *peer-to-peer* y el registro público *blockchain* o cadena de bloques.
  El *blockchain*, tecnología indispensable para el funcionamiento del *bitcoin*, está formado por bloques, cada uno de los cuales contiene una serie de transacciones realizadas. El *blockchain* es al *bitcoin* lo que Internet es a los *mails*.

  Es una base de datos que contiene todas las transacciones efectuadas desde la creación del *bitcoin*. No está guardada en ningún servidor central, sino en una multitud de servidores, son los *nodos* de la red. El *blockchain* permite intercambiar valores, como los *bitcoins*, sin intermediarios.

  Al ser completamente público, todos los usuarios pueden ver cuánto dinero hay en una determinada dirección, cuánto se ha gastado desde ella, a qué dirección se ha enviado dinero, desde cuál se ha recibido o cuánto dinero se ha movido en total, entre otras operaciones. Sin embargo, dado que las direcciones *bitcoin* no tienen ningún dato identificativo, estas no revelan la identidad de quien realiza las transacciones.

  Para realizar una transacción de *bitcoins*:
  - Es necesario tener una billetera o *wallet*, para gestionar los *bitcoins*.
  - Mandarlos a la dirección electrónica del destinatario.
  - Dicha transacción y otras se agrupan en un bloque.
  - Los nodos de la red validan el bloque de transacciones resolviendo problemas matemáticos.
  - El bloque se añade al *blockchain*.
  - El destinario recibe los *bitcoins*.

- **Fraude en subastas**. Después de enviar la cantidad económica en que se ha adjudicado la subasta (la puja), se recibe un producto cuyas características no se corresponden con las prometidas o incluso un producto que no tiene ningún valor.

- **Timos de ISP** (proveedores de servicios de Internet). Los clientes poco experimentados suscriben contratos *online* sin haberse leído el clausulado por completo, lo que puede originar que se encuentren «atados» a un contrato de una determinada duración, del que no pueden salir si no es abonando una penalización por la rescisión anticipada.

- **Fraudes promocionales**. Cargos inesperados en la factura del teléfono a tenor de servicios que nunca se han solicitado ni contratado por parte del usuario legítimo.

- **Fraudes en viajes** o paquetes vacacionales contratados y/o promocionados a través de Internet. Consiste en vender ofertas y promocionar viajes y alojamientos de una calidad superior al servicio que realmente le prestarán en su destino. También se encuentran casos en los que le pueden cargar, al perjudicado, importes por conceptos sobre los que no se le había informado y/o que el perjudicado no había contratado.