UNIVERSIDAD POLITÉCNICA DE MADRID

ESCUELA UNIVERSITARIA DE

INGENIERÍA TÉCNICA DE

TELECOMUNICACIÓN

Ciberdelincuencia

Desarrollo y persecución tecnológica

Autor

Ivan Mateos Pascual

Tutor

Pedro Costa Morata

Septiembre 2013

PROYECTO

CIBERDELINCUENCIA. DESARROLLO Y PERSECUCIÓN TECNOLÓGICA

Tema y Título: Ciberdelincuencia. Desarrollo y persecución tecnológica.

Autor: Ivan Mateos Pascual
Titulación: Telemática
Tutor: Pedro Costa Morata
Departamento: Diatel

Tribunal

Presidente: Manuel Cesar, Rodríguez Lacruz
Vocal: Pedro Costa Morata
Vocal Secretario: Javier Martín Rueda

Fecha de Lectura: 26 de Septiembre de 2013

"¿Internet? No estamos interesados en eso"

-- Bill Gates, 1993 --

Agradecimientos

A mis padres,

porque sin ellos no habría llegado hasta aquí.

A mi dentista preferida,

porque sin ella no lo habría conseguido

Al señor Luis de Miguel,

porque es el mejor compañero que se puede tener

A mis amigos,

porque son la motivación perfecta

Resumen

La aparición de Internet y los sistemas informáticos supuso un antes y un después en el modo que las personas emplearían para acceder a los sistemas de información. El crecimiento exponencial seguido en los años posteriores ha llevado este hecho hasta la situación actual, donde prácticamente todos los ámbitos del día a día se encuentran reflejados en la Red.

Por otro lado, a la par que la sociedad se desplazaba al ciberespacio, también comenzaban a hacerlo aquellos que buscaban obtener un rendimiento delictivo de los nuevos medios y herramientas que se ponían a su disposición. Avanzando a pasos agigantados en el desarrollo de técnicas y métodos para vulnerar unos sistemas de seguridad, aún muy inmaduros, los llamados ciberdelincuentes tomaban ventaja sobre las autoridades y su escasa preparación para abordar este nuevo problema.

Poco a poco, y con el paso de los años, esta distancia ha ido reduciéndose, y pese a que aún queda mucho trabajo por hacer, y que el crecimiento de los índices de ciberdelincuencia, junto con la evolución y aparición de nuevas técnicas, sigue a un ritmo desenfrenado, los gobiernos y las empresas han tomado consciencia de la gravedad de este problema y han comenzado a poner sobre la mesa grandes esfuerzos e inversiones con el fin de mejorar sus armas de lucha y métodos de prevención para combatirla.

Este Proyecto de Fin de Carrera dedica sus objetivos a la investigación y comprensión de todos estos puntos, desarrollando una visión específica de cada uno de ellos y buscando la intención final de establecer las bases suficientes que permitan abordar con la efectividad requerida el trabajo necesario para la persecución y eliminación del problema.

Abstract

The emergence of Internet and computer systems marked a before and after in the way that people access information systems. The continued exponential growth in the following years has taken this fact to the current situation, where virtually all areas of everyday life are reflected in the Net.

On the other hand, meanwhile society moved into cyberspace, the same began to do those seeking to obtain a criminal performance of new media and tools at their disposal. Making great strides in the development of techniques and methods to undermine security systems, still very immature, so called cybercriminals took advantage over the authorities and their lack of preparation to deal with this new problem.

Gradually, and over the years, this distance has been declining, and although there is still much work to do and the growth rates of cybercrime, along with the evolution and emergence of new techniques, keep increasing at a furious pace, governments and companies have become aware of the seriousness of this problem and have begun to put on the table great efforts and investments in order to upgrade their weapons to fight against this kind of crimes and prevention methods to combat it.

This Thesis End of Grade Project focuses its objectives on the research and understanding of all these points, developing a specific vision of each of them and looking for the ultimate intention of establishing a sufficient basis by which to manage with the required effectiveness the type of work needed for the persecution and elimination of the problem.

Índice de Contenidos

Índice de Figuras

Capítulo 1. **Introducción y objetivos**

1.1 Introducción

El uso de los medios informáticos y de Internet para delinquir, ha dotado a los nuevos delincuentes un poder de difusión tal, que prácticamente cualquier lugar del planeta con conexión a la red, se encuentra vulnerable al alcance de sus métodos.

Teniendo en cuenta, que los efectos causados por un ataque informático podrían llegar a tener consecuencias más devastadoras que las causadas por los más importantes ataques terroristas de la historia, se plantea un problema de considerables dimensiones el cual necesita ser tratado con la mayor dedicación y esfuerzo posibles.

El estudio realizado a lo largo de este PFC se propone como una de las formas de analizar en detalle toda esta problemática, intentando localizar y describir las principales características del mundo de la ciberdelincuencia, tanto en los conceptos relacionados con su desarrollo como en el ámbito relacionado con su persecución tecnológica.

Con este cometido, se realiza una revisión bibliográfica de las publicaciones realizadas hasta el momento, acudiendo tanto a los medios digitales como físicos, que los principales organismos, empresas y autores, dedicados al sector de la seguridad informática, ponen a disposición pública para tal efecto. Buscando además avanzar un paso más en la calidad de este contenido, ha sido empleada también documentación técnica proporcionada por fabricantes y proveedores tanto de software como de hardware de seguridad.

1.2 Objetivos

El objetivo de este PFC es el de dar a conocer los diferentes aspectos de los que se compone un tema de la magnitud y la infinidad de posibilidades de estudio como es el de la ciberdelincuencia. Sin la intención de obtener una compleja guía técnica orientada a personal especializado en el mundo de las telecomunicaciones, se intentará tratar el tema principal de la manera más atractiva posible y desde un enfoque general y objetivo.

Con objeto de intentar abordar el mayor número de puntos de vista posible, en cuanto al propio concepto y desarrollo de la ciberdelincuencia, así como en de los medios empleados para combatirla, el estudio realizado se detendrá únicamente en mayor profundidad en aquellos puntos donde se considere necesario un mayor detalle para la correcta comprensión del contenido.

De este modo, los objetivos que este documento intentará abordar a lo largo de los capítulos en que se ha definido son:

- Introducir el concepto de ciberdelincuencia, así como representar los diferentes tipos y formas en que esta puede ser clasificada y las técnicas empleadas para practicarla.
- Identificar a los diferentes tipos de cibercriminales según su perfil y modus operandi.
- Conocer los aspectos más importantes del nacimiento y desarrollo de la ciberdelincuencia y como esta ha influido a lo largo de nuestra historia.
- Presentar y analizar los diferentes métodos empleados hoy en día, tanto para combatir esta nueva forma de delincuencia como para proteger los sistemas de información a los que afecta.

1.3 Organización de la memoria

Capitulo 1. En este primer capítulo se realiza una pequeña introducción al concepto de ciberdelincuencia. A continuación se presentan los objetivos buscados en la realización del documento.

Capitulo 2. En este capítulo se aborda en detalle el concepto de ciberdelincuencia realizando un análisis completo del propio significado del término. Por otro lado, se realiza una revisión sobre quiénes forman parte de este mundo, analizando tanto el papel de las víctimas como el de los delincuentes.

Capitulo 3. Continuando con el capítulo anterior, en este apartado se profundiza sobre las diferentes formas de ciberdelincuencia, analizando en detalle diferentes ejemplos de

técnicas y métodos empleados en su práctica. Con la intención de mostrar claramente el objetivo de cada uno de estos métodos, se realiza el estudio de cada uno de ellos dentro del marco de la ciberdelincuencia en que han sido encasillados.

Capítulo 4. En este cuarto punto, se realiza un repaso sobre la historia de la ciberdelincuencia, desde su aparición hasta nuestros días. Se hace mención también, a las figuras más representativas del mundo del Cibercrimen y se hace una breve revisión sobre la localización geográfica de las fuentes de los principales tipos de amenazas encontradas en la red.

Capítulo 5. Una vez realizado un análisis completo sobre los diferentes aspectos de la ciberdelincuencia, en este siguiente bloque se realiza una revisión sobre los diferentes medios y técnicas empleadas para combatirla tanto en el ámbito técnico como legislativo. Siguiendo la terminología empleada en el capitulo anterior, se hace mención a los problemas existentes y a las medidas adoptadas para solucionarlos.

Capitulo 6. En este último capítulo se describen las conclusiones alcanzadas tras la realización de este PFC, haciendo una reflexión sobre cada uno de los puntos tratados a lo largo del documento.

Capítulo 2. **El concepto Ciberdelincuencia**

2.1 Qué es la Ciberdelincuencia

Cibercrimen, piratería, delincuencia informática,... son muchos los términos y acepciones utilizados para definir un concepto tan amplio como es el de la Ciberdelincuencia, más aun en este caso, pudiendo enfocar la definición en términos como a quien va dirigida, por quién es originada o cual es la naturaleza del delito.

Con el objetivo de partir de una idea común, podemos definir la Ciberdelincuencia como el conjunto de aquellas acciones cometidas a través de un bien o sistema informático cuya consecuencia final recae en un hecho considerado como ilícito. En otras palabras, se trata de una vertiente del crimen tradicional que utiliza las nuevas tecnologías para extenderse y desarrollarse de manera exponencial.

Profundizando un poco más en este aspecto, se definirá como ciberdelictivos "aquellos actos atentatorios de la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos, así como el uso fraudulento de tales sistemas, redes y datos" (Definición basada en el Convenio sobre cibercriminalidad de Budapest del 23 noviembre 2001)[1].

Pese a que un elevado porcentaje de las formas de ciberdelincuencia se establecen en torno a la obtención de información sensible para usos no autorizados, la ciberdelincuencia también comprende actos criminales tradicionales, como puedan ser robos, suplantación de identidad, fraude, acoso y así un innumerable etcétera de delitos, los cuales, en este caso, sean cometidos a través de la red.

Respecto a la distribución geográfica de la Cibercrimen, la compañía Symantec coincidiendo con varias de sus homólogas del mismo sector, realizó un ranking de los 20 países más afectados por la ciberdelincuencia[2]. Para elaborar esta lista, Symantec tuvo en cuenta de

[1] Convenio sobre cibercriminalidad , Budapest 23/11/2001
http://conventions.coe.int/Treaty/en/Treaties/Html/185-SPA.htm
[2] Cybercrime is a Global Problem; Increasingly Social and Mobile (2012 Norton Cybercrime Report)
http://www.symantec.com/connect/blogs/cybercrime-global-problem-increasingly-social-and-mobile-2012-norton-cybercrime-report

manera cuantitativa el número de intrusiones realizadas en ordenadores personales, infecciones zombi, sitios web afectados por Phishing, número de sistemas afectados por bots o troyanos y otros tipos de malware, países con mayor número de Ciberataques originados y países con mayor tasa de Ciberdelitos denunciados.

Como resultado de estas informaciones, EEUU destaca en la primera posición del ranking como país más afectado por el Cibercrimen siendo a su vez la mayor fuente de ataques perpetrados. Este hecho no resulta sorprendente debido a las avanzadas infraestructuras de comunicaciones desplegadas en el país y la alta penetración de redes de Banda Ancha extendidas por todo su territorio, las cuales sirven como un magnífico canal a disposición de ciberdelincuentes en todas partes del mundo.

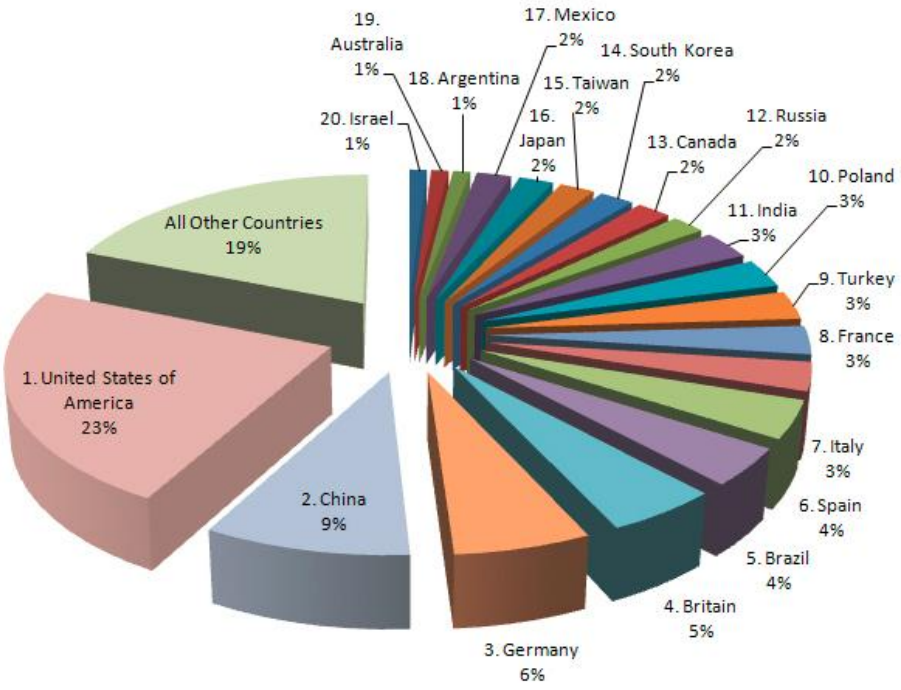

Fig. **1** Top 20 de países afectados por la ciberdelincuencia según la compañía Symantec

Derivados del término Ciberdelincuencia, surgirán numerosos términos que irán directamente relacionados con las particularidades del Ciberdelito en cuestión. De este modo,

nos encontraremos con términos como Ciberacoso, Ciberguerra, Ciberterrorismo, Ciberataques… y un largo etc., que se irán viendo en detalle.

2.2 Quiénes son los ciberdelincuentes

Numerosos estudios, coinciden en que el perfil típico del ciberdelincuente es el de un sujeto varón, de entre 25 y 35 años de edad y con un mínimo de conocimientos informáticos y de la tecnología que le permiten considerar la red como el medio ideal para desarrollar sus actividades.

Retrocediendo unos años hasta situarse en los comienzos de la Informática tal y como se conoce hoy en día, fue sobre el año 1959 cuando apareció el termino Hacker, nombre con el cual la mayoría de la población identifica a los ciberdelincuentes hoy en día, para referirse a un grupo de jóvenes con altos conocimientos de programación que se dedicaban a buscar formas de modificar programas o a encontrar pasadizos dentro de ellos. Este tipo de soluciones conocidas como “Hacks” (del inglés, Hachazos) dieron nombre a estos individuos que poco a poco cambiaron los programas por la búsqueda de vulnerabilidades y agujeros de seguridad en cualquier sistema informático. A pesar de que los Hacker tradicionales siguen la conocida ética Hacker (la cual no busca el mal ajeno, sino la autorrealización y el estudio de los sistemas informáticos, incluyendo la seguridad de los mismos), esta práctica da lugar a situaciones potencialmente peligrosas y cuya legalidad en la mayoría de ocasiones queda en entredicho, incluyendo aquellas ocasiones en las que no conllevan el perjuicio ajeno.

Un hacker, por norma, desconfía de la autoridad opresora, y considera que el acceso a cualquier información que pueda servir para conocer el funcionamiento del mundo debería ser ilimitado y por supuesto gratuito.

Con el fin de comprender mejor los diferentes tipos de Hacker, y no caer en el error de encasillarlos a todos ellos dentro de un mismo rol, a continuación se enumerarán los perfiles más destacados dentro de una clasificación muy común, utilizada incluso dentro del propio colectivo, en base a unos patrones de comportamiento muy definidos.

Black Hat Hacker: (Del inglés, Hacker de sombrero negro) Son aquellos a los que normalmente se les refiere como simples Hacker. Son identificados por no seguir ningún tipo de ética de comunidad, y por buscar a menudo el beneficio personal o económico. El Hacker negro se dedica a buscar la forma de colapsar servidores, entrar en zonas restringidas o tomar el control de sistemas y redes. Se siente orgulloso de demostrar sus habilidades y su grado de autorrealización es mayor cuanto mayor sea el impacto del perjuicio provocado.

White Hat Hacker: Conocidos también como los Hacker éticos o Hacker tradicionales, acerca de los cuales se ha comentado con anterioridad. Su mayor fechoría era la de dejar una tarjeta de visita informando al administrador del sistema las vulnerabilidades o fallos encontrados tras una incursión en su sistema, y/o realizando, en el peor de los casos, como únicas modificaciones, aquellas estrictamente necesarias para mantener su anonimato. En ocasiones los Hacker Blancos, son sujetos que han formado parte de los Hacker Negros, y que han decidido cambiar sus propósitos maliciosos por el apoyo a los administradores de los sistemas de seguridad y a la lucha contra el Cibercrimen, utilizando los mismos conocimientos para luchar contra estos. Los términos Black Hat y White Hat provienen de las antiguas películas del Oeste donde los buenos llevaban sombrero blanco y los malos llevaban siempre el sombrero negro.

Grey Hat Hacker: Conocidos también como Hacker de sombrero Gris. Sujetos cuya ética es ambigua, los cuales poseen conocimientos comparables a los de un Black Hat Hacker pero que sin embargo utilizan para encontrar vulnerabilidades o fallos de seguridad que posteriormente se ofrecen a solventar bajo un acuerdo económico.

Cracker: Podrían incluirse dentro del grupo de los Hacker de sombrero Negro. Son considerados el grupo más agresivo y su único objetivo es, utilizando la expresión comúnmente usada por este colectivo, “reventar sistemas” ya sean informáticos o electrónicos. Los cracker son expertos programadores que utilizan sus conocimientos para modificar el comportamiento de sistemas y redes explotando cualquier vulnerabilidad encontrada, actuando de manera obsesiva e insaciable guiados por su afán destructivo y ególatra.

Phreaker: Colectivo enfocado mayormente al mundo de los sistemas telefónicos, incluyendo también la telefonía móvil y Voz sobre IP (VoIP). Conocen el funcionamiento de

dichas tecnologías así como sus protocolos de comunicación y se dedican a alterar el comportamiento de dichos sistemas por placer y en ocasiones con fines económicos.

Lammer: Repudiados dentro del colectivo Hacker, son aquellos internautas que se dedican a recopilar información y ejecutar códigos maliciosos buscando el reconocimiento social como Hacker sin tener un conocimiento real del impacto de sus acciones, ni del funcionamiento del código ejecutado. En ocasiones son realmente molestos aunque sus acciones no suelen provocar grandes daños.

Scriptkiddie: Son simples usuarios de internet con afición a los temas de Hacking aunque sin demasiados conocimientos al respecto. Suelen utilizar programas o malware que encuentran por la red que ejecutan sin mayor estudio, llegando a infectar sus propios sistemas en multitud de ocasiones.

Newbie: Conocidos como los aprendices de Hacker. Son aquellos novatos que comienzan a leer y experimentar con la información encontrada y que en ocasiones perpetran intrusiones en sistemas débiles aunque sin mayor trascendencia dados sus escasos conocimientos. Su único objetivo es el de aprender.

Wannaber: Son aquellos que "quieren ser". Aspirantes a Hacker con poca perseverancia y capacidad técnica, en su gran mayoría inofensivos, que utilizan sus escasos conocimientos para obtener el reconocimiento social fuera de la red.

Piratas informáticos: Pese a que a menudo se confunde esta denominación con la del término Hacker, los piratas informáticos únicamente se dedican a la copia y distribución de software, música, juegos y un largo etc. de contenidos de manera ilegal, atentando contra la propiedad intelectual y los derechos de sus propietarios.

Bucaneros: Hacen el papel de comerciantes en la red. Se dedican a comprar y vender material ilegal obtenido por medio de otros, tales como identidades, tarjetas de control de acceso, software crackeado, etc.

La siguiente figura muestra un pequeño esquema sintetizando esta información de manera algo más simplificada:

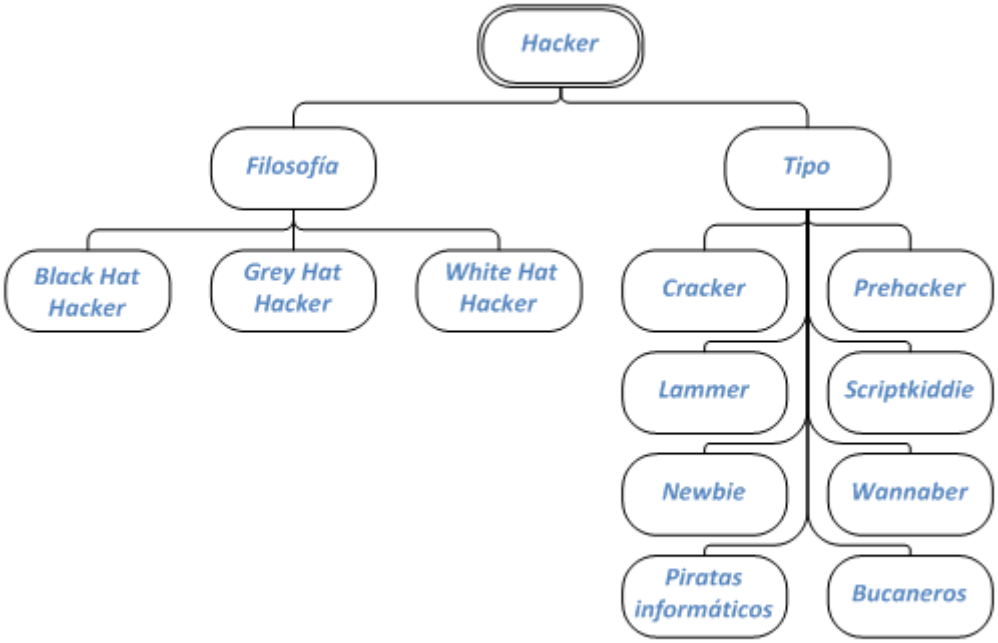

Fig. **2** Tipos de Hacker

Siguiendo con la terminología empleada, parece que queda claro entonces, considerar como ciberdelincuente a todo aquel acusado de ejercer la ciberdelincuencia o el Cibercrimen. Igualmente se consideran ciberdelincuentes aquellos cuya actividad ilícita anteriormente perseguida ha evolucionado con la tecnología y ha ampliado sus horizontes en la red como pueden ser ***Pederastas, Proxenetas, Terroristas***, etc.

Si bien hemos mencionado los diferentes tipos de Hacker, o sujetos dedicados a la Ciberdelincuencia según su forma de actuar, se considera muy interesante añadir algunos perfiles adicionales aparecidos hoy en día basándonos en diferentes artículos tecnológicos encontrados, destacando entre ellos el Informe sobre Criminología Virtual[3] que la compañía de seguridad informática McAfee realiza cada año.

[3] McAfee.Informe sobre Criminología Virtual 2009. http://www.mcafee.com/mx/resources/reports/rp-virtual-criminology-report-2009.pdf

Instaladores de Bots: *Son* aquellos cuya intención es la de conseguir el control de un equipo remoto a través de la instalación de software malicioso. Para conseguir dichos fines se valen de malware pre-programado, el cual es embebido de manera oculta en todo tipo de interacciones que el usuario realiza mientras navega por la web.

Carders: Este tipo de ciberdelincuentes se centran exclusivamente en el robo de identidad y en la consecución de fraudes mediante tarjetas de crédito en la Red. Podemos considerar a los Carders como la evolución natural de los tradicionales carteristas. Una vez conseguida la información necesaria, pueden realizar transacciones y compras online encubriendo su identidad y cargando el coste a su víctima.

Ciberpunks: Sin llegar a tener un objetivo lucrativo en sus actos, los Ciberpunks, termino surgido del movimiento literario con el mismo nombre, pueden llegar a suponer grandes pérdidas a sus víctimas, tanto económicas como de imagen. Considerado como el ciberdelincuente travieso, el ciberpunk se dedica a alterar sistemas públicos, como pueden ser una página Web, con objeto de mofarse y ridiculizar a aquellos que considere sus víctimas.

Insiders: Empleados o ex-empleados que actúan desde dentro de las propias compañías utilizando su experiencia y conocimiento de los sistemas "desde dentro", para acceder, distribuir información confidencial o perjudicar de algún modo a sus empresas. Sus motivaciones suelen ser tanto económicas como personales incluso con fines de venganza.

Phisher, Spammer: Especializados en utilizar el correo electrónico como forma o via de comunicación con sus víctimas. Buscan el beneficio económico a través de engaños y señuelos que llevan a confusión al cibernauta despistado mostrándose como fuentes aparentemente confiables.

¿Cómo trabajan los ciberdelincuentes?

Si hasta este momento han sido analizados los diferentes tipos de ciberdelincuentes según su perfil técnico y su filosofía, se considera igualmente interesante y necesario realizar una última clasificación adicional de los diferentes tipos de individuos dedicados al mundo de la ciberdelincuencia, según el papel que estos desempeñan.

Al igual que ocurre en la delincuencia tradicional, además de trabajar de manera independiente, los delincuentes pueden formar parte también complejos entramados y estructuras jerárquicas, donde cada miembro de dicha estructura juega un papel totalmente diferente al resto. Es en este punto donde aparece concepto del denominado crimen organizado.

Las organizaciones criminales funcionan del mismo modo que podría hacerlo cualquier empresa común, contando con especialistas en cada campo, proveedores y por su puesto individuos encargados de de la dirección y organización de la misma.

En este caso, y empleando una clasificación definida por la compañía de seguridad Panda Security[4], con el objetivo de definir los diferentes tipos de ciberdelincuentes que pueden encontrarse en la estructuración del Cibercrimen organizado, es posible diferenciar entre los siguientes perfiles mostrados en la figura.

[4] Panda Security. Los profesionales del Cibercrimen [en línea]
http://cybercrime.pandasecurity.com/blackmarket/cybercrime_professions.php?lang=es

Fig. **3** Roles del crimen organizado

¿Soy yo un ciberdelincuente?

Esta pregunta, sería a su vez la respuesta ante una posible acusación de ciberdelito por parte de más de la mitad de los usuarios de Internet. Si bien todos tenemos claro cómo identificar cuándo somos víctimas de un fraude, en muchas ocasiones la corriente social puede llegar a hacer perder al usuario la objetividad a la hora de calificar su comportamiento en la red. Muchos delitos contra la propiedad intelectual y contra la ley de protección de datos son

cometidos de manera inconsciente por parte de los usuarios sin ser catalogados ni denunciados como tales.

En una entrevista realizada al reconocido Hacker español Jose María Alonso[5], el cual actualmente trabaja para el departamento de seguridad de la empresa Telefónica Digital, este señalaba textualmente, *"Os sorprenderíais de descubrir que los verdaderos hackers sois vosotros. Yo llevo 14 años dedicándome a la seguridad informática y la gente me pide que le enseñe a hackear directamente. Hay personas que me piden que le cambien las calificaciones de los exámenes, acceder a las pruebas de acceso a la universidad o degradar el servicio de una empresa de la competencia".*

Y es que, según datos obtenidos en diferentes estudios, alrededor del 15% de los individuos que utilizan internet considera que es "legal" la descarga de una canción, un álbum, o una película sin pagar por ello. El hecho de asumir que Internet ofrece un sinfín de recursos gratuitos inagotables, ha convertido en una tarea muy complicada el hecho de hacer pensar a las personas que han de pagar por lo que a menudo obtienen de forma gratuita.

A parte de esto, muchas otras conductas, que originadas en un desconocido no se tendría duda a la hora de catalogar como delitos hacia nuestra persona, son también consideradas como "legales" sin provocar ningún tipo de remordimiento en la mayoría de aquellos que las realizan.

En cifras netas, según una encuesta realizada a más de 7.000 individuos de 14 países por la compañía Norton Security en 2012[6] podemos obtener algunos ejemplos.

- El 30% de los encuestados considera legal compartir o editar fotografías de otras personas.
- Un 24% el hecho de ver correos electrónicos personales y el historial de navegación de otras personas.

[5] Entrevista completa: en http://www.marketingdirecto.com/marketing-directo-tv/ponencias/clubm-by-maxus-con-chema-alonso-hacker-love-your-hackers/
[6] Norton Cybercrime Report 2012.
http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

- Un 17% utilizar un trabajo y/o estudio realizado por otro.
- Un 33% de los adultos encuestados ha utilizado en alguna ocasión una identidad falsa online y un 45% ha mentido sobre sus detalles personales en internet.

Estos e infinidad de ejemplos del mismo tipo, son pequeñas acciones que del mismo modo que no suelen ser perseguidas en su gran mayoría, sirven para realizar una pequeña reflexión ante la ambigüedad de la ética aplicada al mundo de los delitos informáticos.

2.3 Quiénes son las víctimas de la Ciberdelincuencia

Como ocurre con el crimen tradicional, se considera como víctima potencial de un Ciberdelito a cualquiera que pueda encontrarse dentro del campo de acción de un posible delincuente, en este caso, informático. Teniendo en cuenta que dicho campo de acción ocupa la totalidad del Ciberespacio que conforma Internet a nivel mundial, se establece el hecho de que cualquier ciudadano, empresa o gobierno que tenga presencia en dicho entorno, se encuentra expuesto a las miradas de los ciberdelincuentes.

2.3.1. **El ciudadano de a pie**

Según los últimos datos ofrecidos por el informe del ONTSI[7] (Observatorio Nacional de las Telecomunicaciones y de los Sistemas de Información), organización que se encarga de sintetizar y analizar indicadores y datos sobre Sociedad de la Información, el aumento progresivo en los últimos años de la población que utiliza internet en su día a día es más que

[7] Uso de Internet de individuos en http://www.ontsi.red.es/ontsi/es/indicador/individuos-que-usan-frecuentemente-internet

evidente. Si bien nadie duda de las ventajas derivadas de la utilización de la Red para tareas cotidianas, esto se ha traducido en un incremento del uso de Internet que alcanzó en 2012, en el caso de España, el 51% de la población, cifra que supone un crecimiento de un 33% desde 2004. Este mismo dato aplicado sobre la población europea arroja un 58% frente al 23%.

En la siguiente figura, podemos observar dichos valores actuales representados en el marco europeo.

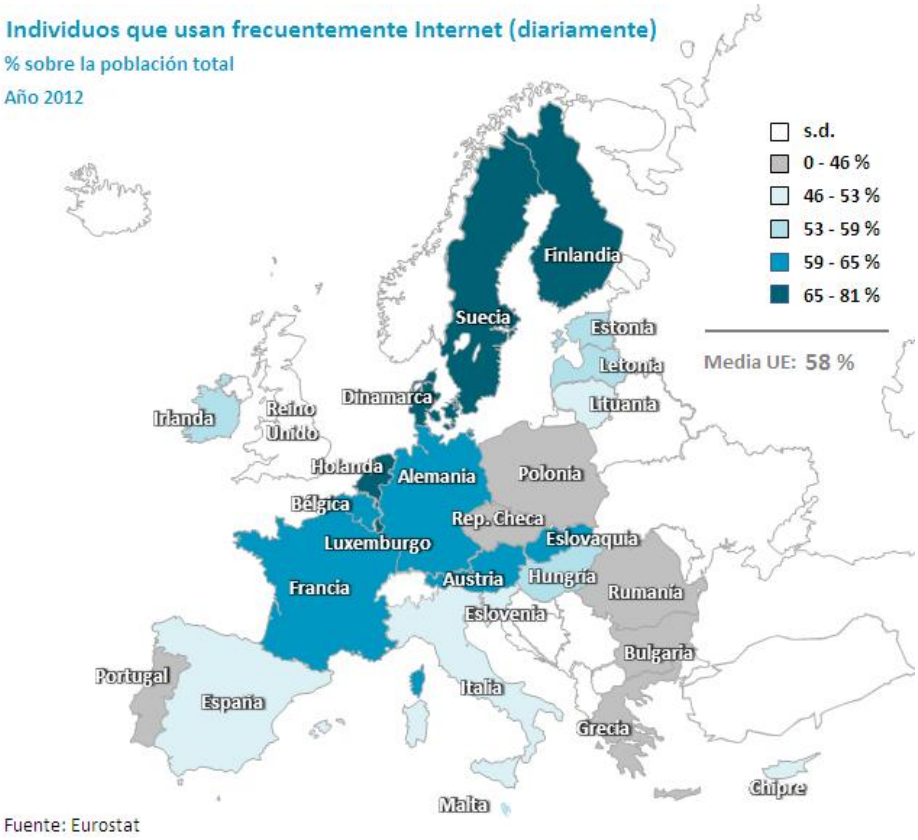

Fig. **4** Uso de Internet en Europa

Centrando este estudio en España y enfocándolo a definir aún más el perfil del tipo de usuario más expuesto a ser víctima de un Ciberdelito, según los datos obtenidos por el INE (Instituto Nacional de Estadística), en el año 2012, el 69,8% de la población de 16 a 74 años afirma haber utilizado Internet en los últimos 3 meses del año (siendo estos un 72,4 % de los varones y un 67,2% de las mujeres). Siendo la población de entre 16 y 24 años de ambos sexos los más asiduos al uso de Internet a través de cualquiera de sus vías de acceso y sufriendo un ligero descenso, aunque manteniendo un porcentaje importante, el grupo de 25 a 34 años.

Estos datos se pueden observar de manera más detallada en el siguiente gráfico:

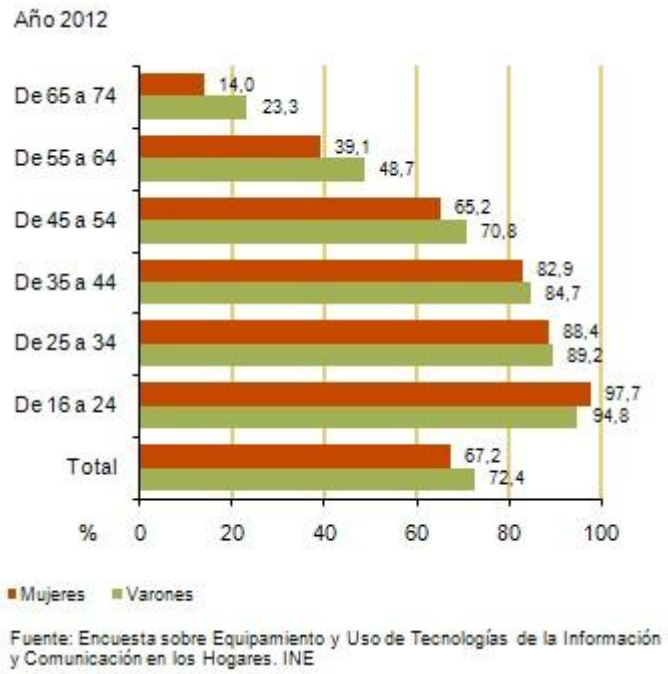

Fig. **5** Estadística de uso de Internet por rangos de edad

Aunque pudiera parecer contradictorio, son precisamente los usuarios más asiduos al uso de internet, es decir, jóvenes de entre 16 y 24 años, y de los que por tanto pudiera deducirse una mayor experiencia en el uso de las nuevas tecnologías, aquellos que en mayor número de ocasiones sufren algún tipo de Ciberdelito. Este hecho podría ser debido a la falta de preparación y educación, en cuanto a las medidas de seguridad necesarias para el uso de la Red, que reciben aquellos, cada vez de menor edad, que de la noche a la mañana sienten una necesidad imperativa de encontrarse online el mayor número posible de horas al día, compartiendo toda su información personal sin ningún tipo de control a través de su conexión ADSL, su teléfono móvil smartphone o su perfil o perfiles en las diferentes redes sociales, a la vez que intentando explotar al máximo todo el contenido disponible en la web.

Según el informe presentado en 2012 por la compañía de seguridad Norton Security, realizado a partir de 13.000 encuestados adultos en 24 países, cada segundo que pasa se suman 18 nuevas víctimas de algún tipo de ciberdelincuencia, lo que supone una cifra de 1,5 millones de afectados cada día. Este mismo informe presenta que cerca de 556 millones de

adultos han sido víctimas del Cibercrimen de alguna manera en los últimos 12 meses, cifra que si bien supera la de la población total de la Unión Europea, además supone un 46% del total de internautas en el mundo.

Por último se indica, que el crecimiento exponencial del uso de las redes sociales y los dispositivos móviles se desmarca como foco principal en los actuales medios de actuación de los delincuentes dejando algunos ejemplos:

- Un 15% de los usuarios de redes sociales afirma que en alguna ocasión ha sido hackeado su perfil y se han hecho por ellos.

- 1 de cada 10 usuarios de redes sociales afirma haber sido víctima de engaños tales como falsos enlaces también denominado “scam”.

- Tan solo el 44% de los usuarios de redes sociales declara utilizar alguna solución de seguridad y menos de la mitad (49%) dice utilizar la configuración de privacidad para controlar el tipo de información compartida.

- Alrededor del 31% de los usuarios de terminales móviles recibió un mensaje de texto con remitente desconocido solicitando el acceso a enlaces, envío de sms o marcación de algún número para escuchar un mensaje de voz.

El objetivo de todos estos datos estadísticos no es otro que el de mostrar una clara presencia constante, por no decir prácticamente permanente, por parte del ciudadano de a pie convertido en internauta, en el ciberespacio, hecho que junto con su condición de miembro más vulnerable de la sociedad, le convierte en la principal víctima de la ciberdelincuencia.

Si analizamos el porqué de esta condición de vulnerabilidad, podemos comprobar cómo, en la mayoría de ocasiones, el internauta medio no es consciente de los riesgos que supone para sí mismo, e incluso para sus empresas en el caso de trabajadores, la falta de celo y de información en cuanto a las medidas de seguridad aplicadas ya sea a su sistema informático o a su información confidencial.

Si bien es cierto que alrededor de un cuarto de los usuarios adopta mecanismos personales para enfrentarse a un Ciberdelito, estos pasos suelen no ser útiles y en muchos casos ni siquiera seguros, entre estas medidas se encuentran limitar el acceso a determinados sitios web considerados inseguros, eliminar correos sospechosos, hacer que un miembro de la familia se encargue de solucionar el problema o incluso intentar identificar al delincuente y buscar justicia por sí mismos.

Como ejemplo de este último punto, podemos continuar extrayendo datos del citado informe de Norton 2012:

- El 40% de los usuarios no utiliza contraseñas seguras, utiliza datos personales para ellas, o no cambia su contraseña con frecuencia.

- Más de un tercio afirma no comprobar si el icono del candado (símbolo indicativo de conexión cifrada mediante certificado digital) está activo cuando introduce información personal como por ejemplo datos bancarios.

- Uno de cada tres usuarios no cierran su sesión al finalizar el acceso a su perfil de red social.

- Un 44% acceden a través de redes Wi-FI gratuitas o inseguras y realizan tareas de intercambio de información confidencial tales como acceso a emails personales (67%), compras online (31%), acceso a cuentas bancarias (24%), acceso a su perfil en alguna red social (63%).

- Dos de cada tres adultos señalan no utilizar ninguna solución de seguridad en sus dispositivos móviles, indicando un 44% el desconocimiento de la existencia de estas medidas, mientras que el 35% de propietarios han extraviado o sufrido el robo de tu terminal en alguna ocasión.

- El 55% de los usuarios no está seguro de si su equipo se encuentra actualmente libre de virus y el 44% desconoce que un programa malicioso pueda actuar de manera discreta en segundo plano.

La siguiente imagen muestra un ejemplo del uso potencialmente inseguro que los internautas hacen del correo electrónico personal:

Fig. **6** Utilización del correo electrónico

2.3.2. **Las empresas**

Sin lugar a dudas, las empresas son el ente cuya información de carácter sensible, es más claramente cuantificable en aspectos económicos por estar directamente relacionada con el volumen de negocio de las mismas. Sin apenas esfuerzo, un ciberdelincuente puede evaluar el daño que ha ocasionado u ocasionará a una compañía, según sea su posición en el mercado y el sector donde esta desempeña su actividad.

El crecimiento de las redes sociales y de las transacciones electrónicas comerciales por parte del sector servicios, ha provocado que los delincuentes centren uno de sus principales objetivos en el robo de información confidencial ya sea interna o financiera de la propia compañía, comprometiendo su posición competitiva o, en la mayoría de los casos, extraída de las bases de datos de clientes, lo que conlleva nuevamente a poner en peligro la seguridad de los usuarios finales.

Para conocer el impacto que la ciberdelincuencia ocasiona al mundo empresarial, es necesario detenerse, en primer lugar, en un pequeño análisis de lo que el crecimiento del uso de Internet supone hoy en día en este ámbito.

Del mismo modo que cada día la población pasa más tiempo conectada a Internet, y por esta misma razón, las empresas necesitan de su presencia en la Web para obtener una serie de beneficios que les otorguen la competitividad necesaria para mantenerse a flote.

Algunos de esos beneficios serían los siguientes:

- Expansión de mercado
- Difusión de nuevos productos y campañas de marketing
- Captación de clientes
- Mejorar la calidad de sus servicios
- Acelerar el proceso de negocio
- Mantener el nivel de sus competidores
- Reducción de costes
- Mejorar la imagen de la compañía

…

El informe Global Security Report 2013[8] publicado por la compañía Trustwave , coloca al sector servicios en la cabeza de la lista de afectados en el mundo, siendo este el objeto del 45% de los ataques, dato un 15% por encima del registrado en el mismo periodo del año pasado destacando los primeros casos a servicios basados en la nube. Este aumento se debe tal y como se ha mencionado anteriormente al aumento de transacciones a través de tarjetas de crédito y débito que se realizan en esta industria. Tal es dicho crecimiento, que el 96% de los Ciberataques se han producido por esta vía a través de las cuales los ciberdelincuentes obtienen completas fichas de datos a las que no sólo estafar sino con las que poder realizar compras y delitos de manera totalmente anónima.

[8] Trustwave Global Security Report 2013
http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf

Si se analiza este hecho localmente, según los datos obtenidos por el INE (Instituto Nacional de Estadística), con fecha Enero de 2013[9], ya el 98% de las empresas españolas disponen de algún tipo de conexión a Internet y el 68% disponen de página Web donde publicitan sus servicios.

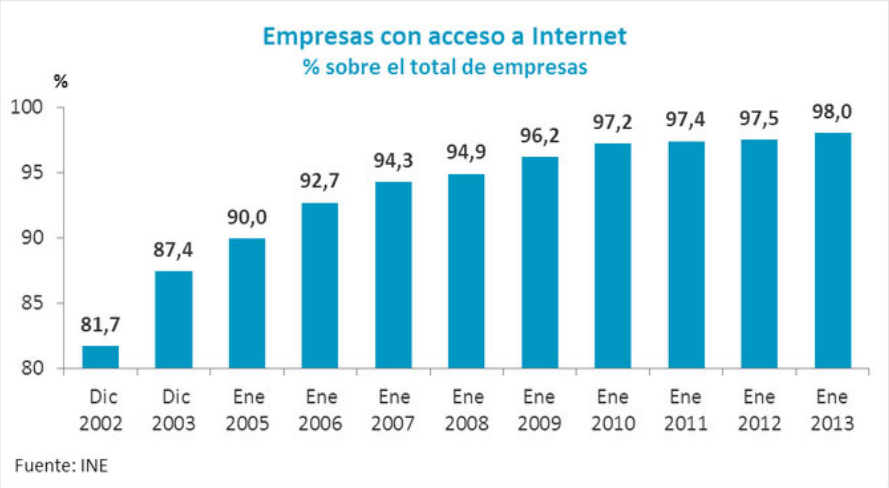

Fig. **7** Empresas con acceso a Internet en España

Partiendo del estudio realizado por la OBS (Online Business School), en 2012, del total de ventas realizadas en España, el 14% se realizó por Internet y un 31% de las personas que compraron lo hizo por este medio. Suponiendo este porcentaje un total de 12,324 millones de personas las que realizaron una compra por internet (un 26% del total de la población española).

En referencia al número de empresas que realizaron alguna operación de venta mediante comercio electrónico fueron en 2012 un 14,4% del total de empresas en España.

[9] Encuesta sobre el uso de Tecnologías de la Información y las Comunicaciones (TIC) y del Comercio Electrónico en las empresas 2011/12 http://www.ine.es/prensa/np718.pdf

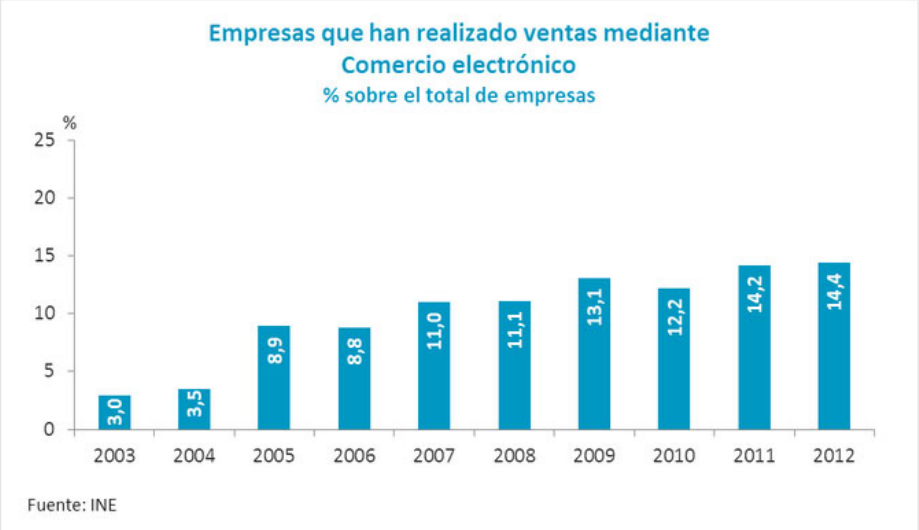

Fig. 8 Empresas que han realizado ventas mediante comercio electrónico en España

Como se observa en las figuras anteriores, todos los indicadores señalan la creciente presencia de las empresas en internet de cara a ofrecer sus servicios a los clientes. Este hecho las coloca como fuentes, en continuo crecimiento, de información valiosísima para los ciberdelincuentes.

Pese a todos estos datos, y si bien las empresas no tienen miedo de reconocer ser víctimas de todo tipo de ataques, un muy reducido porcentaje de las empresas reconoce públicamente perdidas de información de sus clientes y en la mayoría de los casos achacan las noticias publicadas a campañas de marketing viral por parte de la competencia para dañar su imagen.

Algunos de los casos que pueden servir como ejemplo de los ataques más significativos registrados en el último año son los siguientes:

Twitter: La conocida red social, fue víctima el pasado 1 de Febrero de un ataque el cual supuso el acceso ilícito a la información de cerca de 250.00 usuarios. Dos de los casos más comentados fueron el acceso a las cuentas de Burger King y Jeep, cuyas imágenes de fondo fueron modificadas por los logotipos de sus competidores directos (McDonalds y Cadillac respectivamente) indicando que habían sido adquiridos por estos. Pocas semanas después, **Facebook**, **Apple** y **Microsoft** indicaron haber sido víctimas del mismo ataque.

Dropbox: La empresa de servicios en la nube sufrió el robo de datos de sus clientes, supuestamente a través del acceso a una de las cuentas corporativas de la compañía, los cuales a los pocos días comenzaron a ser víctimas de SPAM indiscriminado. Pese a que la compañía nunca confirmó el número de cuentas vulneradas, afirmó haber contactado con todos los afectados para brindarles ayuda.

Reuters: La agencia sufrió dos hackeos en su plataforma de blogging, donde se publicaron informaciones falsas sobre noticias de actualidad.

Adobe: Sufrió el ataque contra sus servidores internos del que se obtuvo un certificado digital de la empresa, que fue utilizado para firmar dos ejemplares de malware.

KT Corp: La multinacional telefónica sufrió el robo de datos de 8.7 millones de usuarios.

Fig. **9** Imagen de la cuenta de Twitter de Burguer King tras ser hackeada

El peligro del fenómeno BYOD

Bring your own device, (BYOD) es el nuevo fenómeno en auge en las empresas. Este fenómeno reside en la permisividad que conceden las compañías hoy en día para que sus empleados puedan conectarse desde sus propios dispositivos, tales como terminales móviles, PCs portátiles, tablet, IPad, o cualquier otro gadget que disponga de conectividad WiFi, a Internet. Esta permisividad no va únicamente encaminada a que sus trabajadores puedan conectarse a sus redes sociales en sus momentos de ocio, sino que también tiene como objetivo que aquellos que así lo requieran puedan trabajar y conectarse a los recursos internos de su empresa (correo electrónico, servidores de ficheros, bases de datos, etc.) de manera cómoda y sencilla.

Según el estudio presentado por la prestigiosa compañía de software antimalware Trend Micro, cerca del 78% de las empresas permiten que sus empleados puedan utilizar sus propios dispositivos para realizar labores corporativas. Del mismo modo, el 50% de un total de 850 empresas de EEUU, UK y Alemania encuestadas, admitió en algún momento haber sufrido brechas de seguridad y problemas de datos, originados en su totalidad a través de un dispositivo personal de alguno de sus empleados. Curiosamente según dicho estudio el 75% de los CEO de las compañías utilizaban de manera habitual smartphone y otros dispositivos para conectarse a su red corporativa.

Si bien está política tiene unas indudables ventajas, de cara a una estrategia de empresa moderna y cercana al empleado, las consecuencias de una falta de previsión a la hora de administrar la conectividad de los dispositivos, en cuanto a segmentación de la red, sistemas de autenticación implementados, así como una correcta formación e información sobre el correcto uso de sus dispositivos, puede ocasionar y ocasiona en numerosas circunstancias la entrada de malware, virus y accesos no controlados a los sistemas de información de la compañía, cuyas consecuencias pueden ser desastrosas.

Fig. **10** Cartel promocional de la estrategia empresarial BYOD.

2.3.3. **Los gobiernos**

Si entre 1945 y 1991 la llamada Guerra Fría marcó un antes y un después en la forma en que los gobiernos resolvían sus diferencias, la evolución natural hoy en día de este método sería la guerra en el ciberespacio.

Los casos de Ciberespionaje entre países son noticia cada poco tiempo y las amenazas de terrorismo físico ahora comparten su lugar con casos de Ciberterrorismo ya sea proveniente de otros países o de bandas organizadas. Este nuevo uso de internet por parte de los terroristas, no sólo para perpetrar ataques, sino para captar adeptos y propagar sus ideales supone una grave amenaza para la seguridad tanto nacional como internacional.

Centrales energéticas, redes de suministro eléctrico y cualquier otra infraestructura gubernamental relacionada con las tecnologías de la información, suponen puntos vulnerables para los gobiernos y sus ciudadanos.

Al igual que en una guerra es difícil definir quiénes son las víctimas y quiénes están del lado transgresor, en este punto los gobiernos ocupan también las dos caras de la moneda.

Como mención especial, es interesante destacar los casos de Ciberespionaje atribuidos al gobierno chino, el cual es sospechoso de gran parte de los ataques que han tenido lugar en los últimos tiempos a grandes empresas así como en instituciones públicas de todo el mundo.

En Febrero de este año, la compañía americana Mandiant publicó un informe titulado "*China's Cyber Espionage Units*" [10] en el cual se detallaban diferentes informaciones utilizando más de 3.000 evidencias con el objetivo de demostrar que el ejército chino llevaba realizando estas acciones desde el año 2006 y robando información al menos a 141 compañías en todo el planeta, en su mayor parte a empresas estadounidenses. Esta ha sido la primera vez, en la historia de la investigación contra la Ciberdelincuencia, en la que se han presentado pruebas suficientes para acusar directamente a un gobierno de infiltrarse y robar información a empresas de todos los sectores a nivel mundial.

Poco después de la publicación de dicho informe se atribuyeron casos de Ciberespionaje, también con origen en el país oriental, contra la EADS (European Aeronautic Defence and Space Company), empresa fabricante del avión Eurofighter y dueña de Airbus y también contra la compañía alemana ThyssenKrupp.

Fig. **11** Portada del periódico estadounidense New York Times, anunciando el ataque recibido desde China el pasado 30 de Enero de 2013

[10] Inform "China's Cyber Espionage Units" http://intelreport.mandiant.com

Por otro lado, tal y como ocurre en el ámbito empresarial y en el de los internautas, en el mundo de la ciberdelincuencia prácticamente nadie puede asumir únicamente el papel de víctima. Si en el párrafo anterior señalábamos a EEUU como una de las principales víctimas del espionaje chino, el pasado mes de Julio de este año las grandes compañías de Internet, entre ellas Apple, Google, Facebook, Microsoft y Twitter emitieron un escrito dirigido al gobierno estadounidense para solicitar de manera formal autorización para informar a la ciudadanía sobre los datos que suministran a la Agencia Nacional de Seguridad americana NSA estas empresas.

En esta carta, 63 empresas entre las que se encontraban compañías de Internet, Inversionistas y ONG solicitaban permiso para hacer públicas las peticiones recibidas sobre la información de sus usuarios tales como cantidad de individuos, cuentas o dispositivos desde los cuales provienen dichos datos además de otros datos personales.

La petición fue firmada también por compañías como AOL, Dropbox, Yahoo, Mozilla, LinkedIn, Meetup, Reddit, Tumblr y varias organizaciones de derechos civiles, como la fundación The Electronic Frontier

Ya sean empresas o gobiernos, ambos tienen mucho que perder ante los posibles ataques y desastres ocasionados por los ciberdelincuentes, y es por este motivo que son quienes mayores desembolsos económicos realizan a la hora de invertir en la seguridad de sus infraestructuras.

Sin embargo, y por contradictorio que parezca, según apunta el informe realizado por McAfee, al contrario que en el caso de las empresas privadas donde la inversión realizada en seguridad va limitada por la capacidad económica de la compañía, los gobiernos siguen relegando la seguridad a un segundo plano, por detrás de la crisis económica mundial y de las amenazas de terrorismo tradicional. A pesar de un aumento evidente del riesgo para la seguridad nacional, la ignorancia técnica por parte de las últimas cabezas decisorias y la falta de previsión de riesgos generalizados y a largo plazo, provocan que no se dedique a este campo ni el tiempo ni los recursos tanto económicos como legislativos que serían necesarios.

Capítulo 3. **Formas y métodos de Ciberdelincuencia**

3.1 Técnicas comunes

A pesar del incontable número de técnicas empleadas por los ciberdelincuentes, y la constante aparición de nuevas formas de comprometer y eludir las medidas de seguridad de los sistemas, cuyo estudio en profundidad daría lugar a un documento de magnitudes muy superiores a este mismo, a continuación se puede encontrar una pequeña revisión de las técnicas más comunes hoy en día.

3.1.1. **Botnets**

Las llamadas Botnets o redes de Bots, diminutivo de la palabra robot, son redes o grupos de ordenadores infectados, que pueden ser controladas de manera remota por el propietario del malware de control o bot, instalado en los equipos. El fin de estas redes es el de contar con todo un ejército de equipos anónimos, los cuales pueden recibir órdenes como la distribución del malware, el envío de Spam o la ejecución de ataques de denegación de servicio (**DDoS**).

Algunas de estas redes pueden llegar a estar formadas por decenas de miles de equipos repartidos por todo el planeta, conocidos también como equipos **zombis**, multiplicando el potencial y el poder de intimidación de los posibles actos ciberdelictivos y por consiguiente las ganancias de estos.

La siguiente imagen muestra un ejemplo del funcionamiento de una botnet en la que se puede observar como los llamados Spammer aprovechan el anonimato y la potencia de la red para obtener sus ganancias, mientras que esta a su vez va trabajando de manera autónoma en la captación de nuevos equipos zombis.

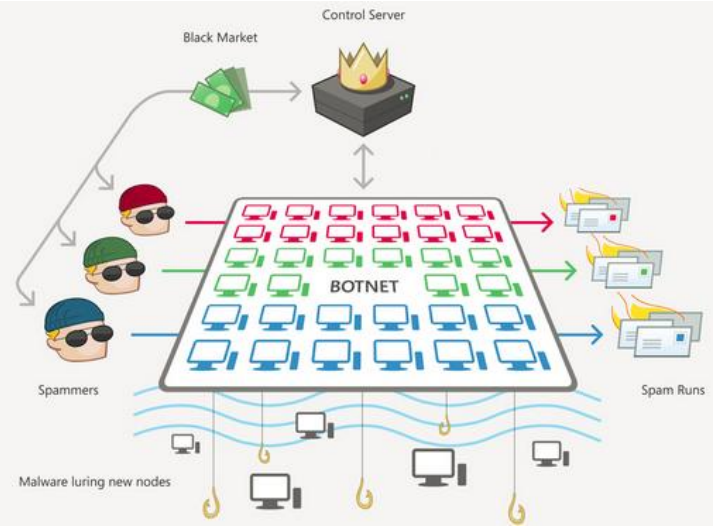

Fig. **12** Ejemplo de Botnet.

3.1.2. **Spoofing**

El término Spoofing se refiere al uso de técnicas de suplantación de identidad con objeto de interceptar, alterar o conseguir establecer una comunicación. Sin llegar a entrar a un elevado nivel de detalle, podemos diferenciar los siguientes tipos de Spoofing:

IP Spoofing: Como su nombre indica, la identidad a suplantar en este caso sería la dirección IP de una tercera entidad, la cual sería realmente el origen o destino de un paquete. Esta técnica puede ser utilizada para conseguir el acceso no autorizado a recursos de red o a la administración de equipos.

ARP Spoofing: En este caso, el objetivo es el de falsear la tabla ARP, relación construida entre direcciones de red (IP) y direcciones físicas (MAC) de los equipos de routing de una red, de modo que sea posible interceptar los paquetes destinados a un host víctima y analizarlos para otros fines.

DNS Spoofing: Se trata de la alteración o falsificación de una o varias entradas de las tablas de resolución, Nombre de Dominio – IP, de un servidor de resolución de nombres (DNS). Esta técnica se realiza en ocasiones combinada con la de IP Spoofing, tomando la identidad de un Servidor DNS de segundo nivel, de modo que los servidores DNS primarios acepten la

información propagada por este. Técnicas como el **Pharming** se sirven de este tipo de herramientas.

Web Spoofing: Consiste en la falsificación de parte o la totalidad de un sitio Web, con objeto de interceptar y recoger información proporcionada por un usuario durante la navegación. A diferencia del **Phishing**, esta técnica permite la comunicación entre la víctima y el sitio real, es decir, se ejecuta de manera transparente al usuario, el cual realiza el acceso a sus perfiles y cuentas sin notar ningún tipo de variación mientras que el falso sitio web recoge y almacena la información introducida a la vez que la reenvía al sitio real.

Mail Spoofing: Principalmente utilizada en casos de **Hoax** y como medida para eludir los equipos de seguridad en el envío de Spam, esta técnica consiste en la suplantación de manera parcial (únicamente el dominio) o completa de direcciones email con el fin de simular la confiabilidad necesaria tanto para los equipos de seguridad como para los destinatarios del correo, respectivamente.

GPS Spoofing :De reciente aparición, esta técnica, consiste en emitir una señal hacia un receptor GPS, fingiendo ser un Satélite autorizado, de modo que este considere que tal información proviene de uno de los satélites del sistema GPS real, consiguiendo de esta manera que el equipo tome como verdadera una ubicación errónea. El modo de operación común de esta técnica consiste en ir alterando poco a poco la información real sobre la ubicación de un sistema, consiguiendo dirigirle finalmente a la localización deseada.

Su principal aplicación, reside en la manipulación de vehículos con sistema de tripulación automática.

Las diferentes técnicas de Spoofing son utilizadas, entre otros, por los ataques conocidos como **Man in the Middle** (MiTM).

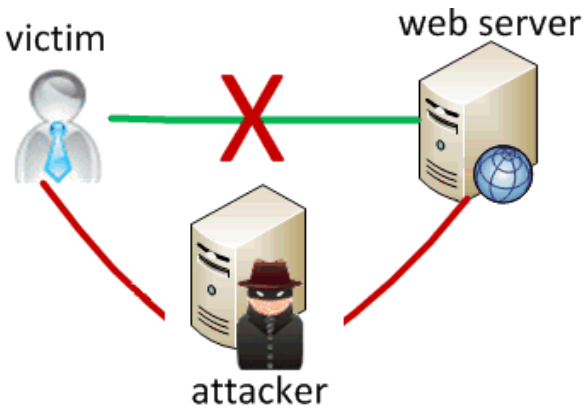

Fig. **13** Esquema de ataque Man in the Middle utilizando la técnica de Web Spoofing.

3.1.3. **Ataques Brute Force**

Los ataques Brute Forte, del inglés, ataques por Fuerza Bruta, suelen estar destinados a la superación de sistemas criptográficos o protegidos por contraseñas.

Se denominan ataques de fuerza bruta, a aquellos cuyo método empleado, para conseguir el acceso a un sistema restringido, consiste en recorrer todas y cada una de las posibilidades existentes dentro de un algoritmo de posibilidades de composición (como son el número de caracteres mínimo y máximo u otros requerimientos de complejidad) de credenciales de acceso, hasta conseguir obtener el resultado correcto, que permita la intrusión no autorizada.

Para este cometido, existen numerosas herramientas, como pueden ser sencillos script donde únicamente es necesario indicar las variables necesarias, a partir de las cuales generan un listado completo de posibilidades que van recorriendo de principio a fin, hasta complejos programas que realizan los diferentes intentos de validación de manera distribuida, consiguiendo de este modo eludir los sistemas de bloqueo por intentos fallidos presentes en gran parte de los casos.

3.1.4. **Ataques JavaScript**

Con la popularidad del desarrollo de las web 2.0 (término empleado para aludir a la nueva modalidad de sitios web, diseñados para facilitar la interoperabilidad y la participación de los usuarios), JavaScript se ha convertido en uno de los lenguajes de programación web más populares de Internet. Al contrario que el tradicional código HTML, orientado principalmente a la lectura de contenidos, este lenguaje es empleado principalmente para la creación de pequeñas aplicaciones que se ejecutan en el lado cliente, a través principalmente del navegador web, y que permiten al usuario actuar directamente sobre la interfaz, el formato y contenido del sitio.

Esta funcionalidad es utilizada por los ciberdelincuentes para introducir código adicional en sitios web con gran volumen de visitas, buscando entre sus principales objetivos redirigir a los usuarios hacia web maliciosas.

Otro método de actuación común, en un ataque JavaScript a un sitio web, consiste en la introducción de un reducido número de líneas de código o secuencias de comandos a una determinada página web considerada como legítima. Una vez el usuario visita dicha web, la modificación añadida lleva al navegador de la víctima a descargar una serie de contenido malicioso de manera transparente para esta. Este contenido suele estar formado por un paquete de componentes, diseñados con el fin de aprovechar determinadas vulnerabilidades del lado cliente, ya sea en el propio navegador o en su sistema operativo, conocidos con el nombre de **exploits**, los cuales han podido ser diseñados por el propio atacante o adquiridos a través de terceros.

La peligrosidad de este tipo de ataques reside, por un lado en el hecho de que un usuario simplemente necesita visitar un sitio web habitualmente legítimo, pero en ese momento comprometido para poder ser infectado, y por otro la facilidad de uso y el enorme dinamismo de los paquetes de exploits, en continua evolución debido a la constante persecución por parte de los proveedores de seguridad, y siempre a la vanguardia en el aprovechamiento de vulnerabilidades zero-day.

Por este motivo, a pesar de que los fabricantes suelen mitigar este tipo de amenazas sin excesiva dificultad, el daño que pueden llegar a ocasionar desde sencillas aplicaciones hasta

ataques de elevada complejidad, la convierten en una de las técnicas más a tener en cuenta hoy en día.

3.1.5. **SQL Injection**

Otra de las técnicas más comunes para explotar vulnerabilidades, en este caso relacionada uno con los sistemas de consultas de bases de datos más empleados en los últimos años, son los ataques por inyección de código SQL.

Pese a tratarse de un tipo de vulnerabilidades bastante estudiado, y resuelto en la mayoría de sitios web de cierta envergadura, aún a día de hoy existen un sorprendentemente elevado número de entornos donde este tipo de ataques resultan efectivos.

El funcionamiento de los ataques mediante SQL Injection se basa en la introducción de código SQL adicional a un aplicativo, generalmente a través de un formulario de login (donde es requerido un usuario y una contraseña de acceso) con el cual se pretende alterar el funcionamiento del entorno programado para realizar las consultas a la base de datos, de modo que sea posible conseguir, modificar o acceder a la información restringida contenida en esta.

El hecho de que el lenguaje SQL sea muy común en el diseño de bases de datos y que en la gran mayoría de programas se empleen sentencias muy similares, convierte a estos entornos en el objetivo de un gran número de ataques, donde los ciberdelincuentes simplemente van empleando y probando determinadas secuencias de código, con el objetivo de encontrar posibles fallos o descuidos en la programación, que el creador del aplicativo pueda haber cometido.

Una de técnicas más famosas, por su simplicidad y efectividad en este tipo de ataques, es el uso de la sencilla secuencia **'or '1'='1** (y sus derivaciones), la cual, por increíble que parezca y pese a ser sobradamente conocida tanto por delincuentes como por programadores y desarrolladores de software, aún a día de hoy resulta exitosa en numerosos casos, consiguiendo gracias a ella acceder a listados completos de usuarios existentes en la base de datos.

Este tipo de técnica, no sólo permite el acceso a la información de las bases de datos sino que, una vez identificadas las vulnerabilidades de un sistema, es posible añadir, modificar o eliminar registros y datos así como ejecutar otro tipo de código malicioso, que permita alterar el funcionamiento del programa según las intenciones del atacante.

3.1.6. **Rootkits**

Se denominan de este modo al conjunto de herramientas que permiten, a una determinada aplicación diseñada por un tercero (con fines habitualmente dañinos) la ejecución de procesos y modificación de archivos del sistema, cuyo acceso se encuentra restringido a exclusivamente a usuarios con privilegios de administrador o superusuario, también conocido como usuario “root”.

Este tipo de herramientas permiten a todo tipo de aplicaciones maliciosas permanecer ocultas y con elevados privilegios sobre el sistema de manera continuada.

3.2 Tipificación del delito Informático

Si bien es cierto que la ciberdelincuencia es tratada comúnmente como un único concepto, es decir, la delincuencia en internet, es necesario tener en cuenta que, a pesar de que estas converjan en alguno u otro punto de su uso y presencia en nuestra sociedad, existen diferentes formas, métodos y situaciones en las que este concepto es utilizado.

Por dicho motivo, en este apartado comentaremos las formas más comunes de Ciberdelincuencia, así como los métodos más utilizados por los ciberdelincuentes para el desarrollo de sus actividades.

En primer lugar, y con objeto de tener una visión completa, necesitaremos conocer los diferentes tipos de delitos informáticos, para lo que utilizaremos dos clasificaciones consideradas marco común en el ámbito legal de la ciberdelincuencia.

La **primera** de ellas, sin duda la más importante por su alcance internacional, sería la basada en el ya mencionado "Convenio sobre cibercriminalidad", firmado en Budapest en Noviembre de 2001, en la que podemos diferenciar cuatro grupos de delitos telemáticos, añadiendo una pequeña descripción a cada uno de ellos.

Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

- Acceso ilícito a sistemas informáticos.
- Interceptación ilícita de datos informáticos.
- Interferencia en el funcionamiento de un sistema informático.
- Abuso de dispositivos que faciliten la comisión de delitos.

Delitos informáticos:

- Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.
- Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.

Delitos relacionados con el contenido:

- Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.

Delitos relacionados con infracciones de la propiedad intelectual y derechos afines:

- Como pudieran ser la copia y distribución de programas informáticos, o piratería informática.

Adicionalmente, y con el fin de criminalizar los actos de racismo y xenofobia cometidos mediante sistemas informáticos, cabe añadir, que en Enero de 2008 se promulgó el "*Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa*[11]" el cual incluye como delitos las siguientes acciones:

- **Difusión de material xenófobo o racista**.
- **Insultos o amenazas con motivación racista o xenófoba.**
- **Negociación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad.**

La **segunda** de ellas, la cual a pesar de tener un carácter menos global también hemos de tener en cuenta, sería la utilizada, y publicada en su sitio web, por La Brigada de Investigación Tecnológica de la Policía Nacional Española[12]. Según esta clasificación podríamos categorizar los delitos telemáticos de la siguiente manera:

Ataques contra el derecho a la intimidad:

- Delito de descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos. (Artículos del 197 al 201 del Código Penal)

Infracciones a la Propiedad Intelectual a través de la protección de los derechos de autor:

- Especialmente la copia y distribución no autorizada de programas de ordenador y tenencia de medios para suprimir los dispositivos utilizados para proteger dichos programas. (Artículos 270 y otros del Código Penal)

[11] Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa
https://www.gdt.guardiacivil.es/webgdt/media/Legislacion/Protocolo_adicional_convencion_cibercrimen.pdf
[12] www.policia.es/bit/index.htm

Falsedades:

- Considerando como documento todo soporte material que exprese o incorpore datos. Extensión de la falsificación de moneda a las tarjetas de débito y crédito. Fabricación o tenencia de programas de ordenador para la comisión de delitos de falsedad. (Artículos 386 y ss. del Código Penal)

Sabotajes informáticos:

- Delito de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos. (Artículo 263 y otros del Código Penal)

Fraudes informáticos:

- Delitos de estafa a través de la manipulación de datos o programas para la obtención de un lucro ilícito. (Artículos 248 y ss. del Código Penal)

Amenazas:

- Realizadas por cualquier medio de comunicación. (Artículos 169 y ss. del Código Penal)

Calumnias e injurias:

- Cuando se propaguen por cualquier medio de eficacia semejante a la imprenta o la radiodifusión. (Artículos 205 y ss. del Código Penal)

Pornografía infantil:

- Entre los delitos relativos a la prostitución al utilizar a menores o incapaces con fines exhibicionistas o pornográficos.
- La inducción, promoción, favorecimiento o facilitamiento de la prostitución de una persona menor de edad o incapaz. (art 187)
- La producción, venta, distribución, exhibición, por cualquier medio, de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o

incapaces, aunque el material tuviere su origen en el extranjero o fuere desconocido. (art 189)

- El facilitamiento de las conductas anteriores (El que facilitare la producción, venta, distribución, exhibición...). (art 189)
- La posesión de dicho material para la realización de dichas conductas. (art 189)

Una vez identificados los diferentes tipos de delitos informáticos, en base a los cuales los ciberdelincuentes son juzgados, el siguiente paso necesario para ampliar nuestro conocimiento sobre las formas de ciberdelincuencia, sería conocer los métodos más comúnmente utilizados en la práctica de esta.

Dichos métodos han ido evolucionando con el tiempo como consecuencia de los fines con que eran empleados, y es según estos fines a partir de los cuales podemos clasificar las diferentes formas de ciberdelincuencia.

3.3 Ciberdelincuencia económica

En ocasiones conocida simplemente como **Cibercrimen**, dadas sus connotaciones similares a las del crimen tradicional, si hay una clara tendencia que el mundo de la ciberdelincuencia ha seguido desde su aparición, donde los principales motivos eran la repercusión social y el idealismo, hasta nuestros días, ese ha sido el fin económico. Desde hace ya varios años, los ciberdelincuentes han cambiado su forma de actuar y han pasado a buscar constantemente la manera de obtener rentabilidad a sus acciones.

Para ello, utilizando la Ingeniería social como base principal de sus desarrollos, los delincuentes han aprendido a estafar, chantajear a empresas y/o usuarios utilizando la extorsión y el miedo de estos, e incluso son contratados por grandes y medianas empresas para la prestación de sus servicios como hacker, difusores de contenido y captadores de clientes, entre otros.

Los métodos descritos a continuación, son precisamente aquellos cuyo objetivo final es claramente económico y que por tanto definen este tipo de Ciberdelincuencia.

3.3.1. **Malware**

El termino Malware proviene de la combinación de términos en inglés, “malicious” y “software”, dicho de otro modo, Software malicioso. La distribución de este tipo de software, programado para ejecutar acciones concretas dentro de los sistemas remotos, es sin duda la principal herramienta utilizada por los ciberdelincuentes para propagar sus amenazas por la red.

Dentro del propio malware, existen diferentes tipos de técnicas, cada una de las cuales tiene características muy particulares, y que forman amenazas tanto de manera independiente como fruto de la combinación de varias de ellas. En general, se puede dividir el malware en las siguientes clases:

Virus: El principal objetivo de los virus es el de servir como método de propagación a otro malware o modificar archivos del sistema para alterar su estabilidad. Para su funcionamiento, los virus se alojan en archivos infectados, los cuales contienen el código malicioso y que, una vez ejecutado por el usuario habitualmente de manera involuntaria, les permitirá modificar el comportamiento del sistema y propagarse dentro del mismo y otros sistemas de la red.

Ransomware: Esta nueva modalidad, a su vez situada entre las más lucrativas para sus autores, se trata del tipo de malware más cercano a un delito convencional: el secuestro.

Ubicado en ocasiones dentro de la categoría de los virus, debido a su comportamiento alterador del sistema. Este tipo de amenaza cifra la información almacenada en el equipo e impide al usuario el acceso a sus recursos mostrando un mensaje imperativo que obliga a pagar una cantidad de dinero o rescate a cambio de recuperar sus datos. El pago de dicho rescate, en la mayoría de ocasiones no supone la liberación del sistema, y los usuarios poco experimentados se ven en la obligación de recurrir a personal cualificado para resolver el problema ocasionándoles importantes perjuicios.

Merece la pena destacar en este caso como ejemplo, el famoso "***virus de la policía***", el cual se propagó recientemente en sus diferentes versiones y por numerosos países del mundo, acusando a los usuarios de acceder a contenidos ilegales desde su ordenador, en nombre de las autoridades nacionales, y solicitando el pago inmediato de una multa administrativa, en este caso de 100 euros. Tal ha sido el impacto de esta amenaza, que ha provocado la necesidad de un gran despliegue de medios policiales y de la cooperación internacional de las fuerzas de seguridad para la detención de sus autores.

En la imagen se muestra una captura de la pantalla mostrada a los usuarios en nuestro país, la cual en su última versión incluía hasta una ventana con imágenes capturadas por la Webcam del PC con objeto de fingir el grabado de estas imágenes.

Fig. **14** Imagen mostrada por "el virus de la policía" en España.

Gusanos: También llamados "*Worm"*, por su traducción en inglés, son un tipo de malware capaz de duplicarse por sí mismo. A diferencia de los Virus, no necesitan de la ejecución por parte del usuario sino que utilizan los propios procesos de ejecución de los

sistemas. Este tipo de malware usa los recursos del equipo infectado para distribuirse y lo hace ejecutando de manera transparente servicios de correo electrónico y sistemas de mensajes instantáneos con libretas de contactos, utilizando redes de archivos compartidos (p2p), redes locales, redes globales y todo tipo de recursos y protocolos de comunicación de los que disponga el sistema. Debido a este comportamiento autónomo, su velocidad de propagación es muy alta y suelen ocasionar graves consecuencias.

Troyanos: Basados en conocida la historia del caballo de Troya, esta clase de programas, sin duda el tipo de malware más abundante en la red, se presentan generalmente en forma de algún tipo de software confiable que el usuario instala de manera consciente. El objetivo de los troyanos es el de instalarse y recolectar todo tipo de información, ya sea del usuario (bancaria, personal, etc.) o de los sistemas, que posteriormente envían a sus creadores. Otra de las funcionalidades de los troyanos es la de habilitar una "puerta trasera" o "*backdoor"* en el equipo remoto, a través del cual los ciberdelincuentes pueden tomar el control del equipo infectado. A diferencia de los virus y gusanos, el objetivo de los Troyanos no suele ser la modificación ni alteración del sistema sino que buscan permanecer de manera inadvertida el mayor tiempo posible.

Spyware: O como su nombre indica, *software espía*. Al igual que los troyanos, su comportamiento se basa en la recopilación de información del usuario de manera no permitida. En este caso, la información recogida suele tener fines comerciales y busca registrar los gustos y formas de uso que el internauta refleja en su comportamiento en la Web. A diferencia de los Troyanos, este tipo de malware puede realizar modificaciones en el sistema, siendo habituales las modificaciones en la configuración del navegador tales como página de inicio y motores de búsqueda.

Adware: Generalmente embebido en la descarga e instalación de software gratuito, este tipo de malware se instala in autorización por parte del usuario en su sistema y su función principal es la de mostrar y/o descargar anuncios publicitarios en la pantalla de la víctima. Normalmente funciona de manera combinada con spyware o Troyanos y utiliza la información recopilada para seleccionar los anuncios mostrados al usuario. En ocasiones, los propios programas que contienen el adware incluyen la opción de eliminar esta molestia a cambio de cantidades económicas o incluso son los propios usuarios los que aceptan la visualización de contenido publicitario a cambio de poder utilizar determinado software de manera gratuita.

Fig. **15** Ejemplo de Adware en el navegador.

Scareware/Rogue: En ocasiones conocidos simplemente como falso software, se trata de un modo de malware que simula ser una aplicación anti-malware o de seguridad, la cual es justamente lo contrario. Su comportamiento habitual en los sistemas simula una infección real, notificando al usuario de la necesidad de descargar un software adicional como solución, en unas ocasiones de pago, recogiendo además los datos bancarios de este y posibilitando nuevas estafas, y en otras, otro tipo de malware con diferentes intenciones.

Según el informe publicado por los laboratorios PandaLabs, a lo largo de 2012[13] aparecieron 27 millones de nuevas muestras de malware, es decir, 74.000 nuevas muestras diarias. Siendo 3 de cada 4 muestras creadas del tipo troyanos. De manera adicional, dicho informe muestra el porcentaje de infecciones detectadas según el tipo de malware durante todo el año.

[13] Panda Labs. Infore Trimestral Q1 2013
http://prensa.pandasecurity.com/wp-content/uploads/2010/03/Informe-Trimestral-Q1-2013-ES.pdf

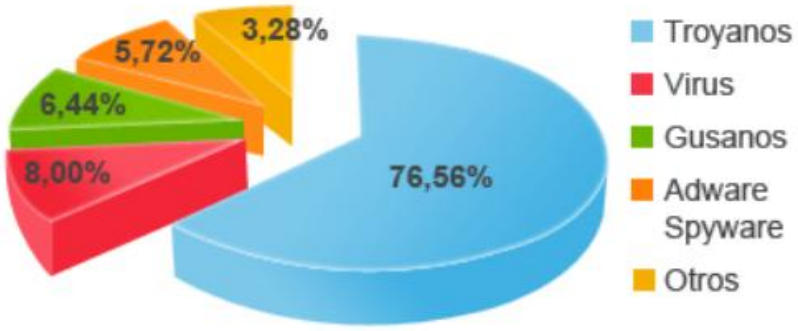

Fig. **16** Infecciones por tipo de malware en 2012 según el equipo de desarrollo de Panda Labs.

Los métodos de distribución de malware que llegan a utilizar los ciberdelincuentes, van desde el ya mencionado software falso o webs ficticias con enlaces de descarga, hasta casos tan ingeniosos como puedan ser olvidar intencionadamente una llave de almacenamiento usb en la cafetería de una empresa con el virus listo para autoejecutarse. Otros métodos comúnmente utilizados son la utilización de los protocolos de comunicación en la red del propio equipo y en la gran mayoría de los casos, el correo electrónico.

3.3.2. **Spam**

Según los datos publicados por organizaciones dedicadas a la seguridad como la Organización sin ánimo de lucro Spamhaus, o las compañías Cisco Systems, Sophos y Kaspersky, las cuales mantienen una lucha constante contra el Spam, en sus informes de amenazas anuales, este tipo de amenaza es, sin duda alguna, el mayor medio de difusión de malware en el mundo.

El Spam, conocido también como correo electrónico no deseado o correo basura, consiste en el envío de manera masiva de emails, ya sea por parte de fuentes desconocidas o haciendo uso de técnicas que permitan enmascarar el remitente dotándolo de mayor confiabilidad, con el fin de difundir contenidos publicitarios, servir como herramienta de difusión a otros delitos como el "**phishing**" (el cual será comentado en el siguiente punto), o

como medio de distribución de amenazas de malware, a través de las cuales es posible infectar a millones de equipos con troyanos y virus que permiten tomar el control de estos de manera transparente para el usuario**.**

Como ejemplo explicativo de este último caso, la siguiente figura muestra el proceso hipotético que se desarrollaría ante una infección de malware espía, donde el objetivo final del delincuente sería obtener acceso a los datos bancarios de la víctima.

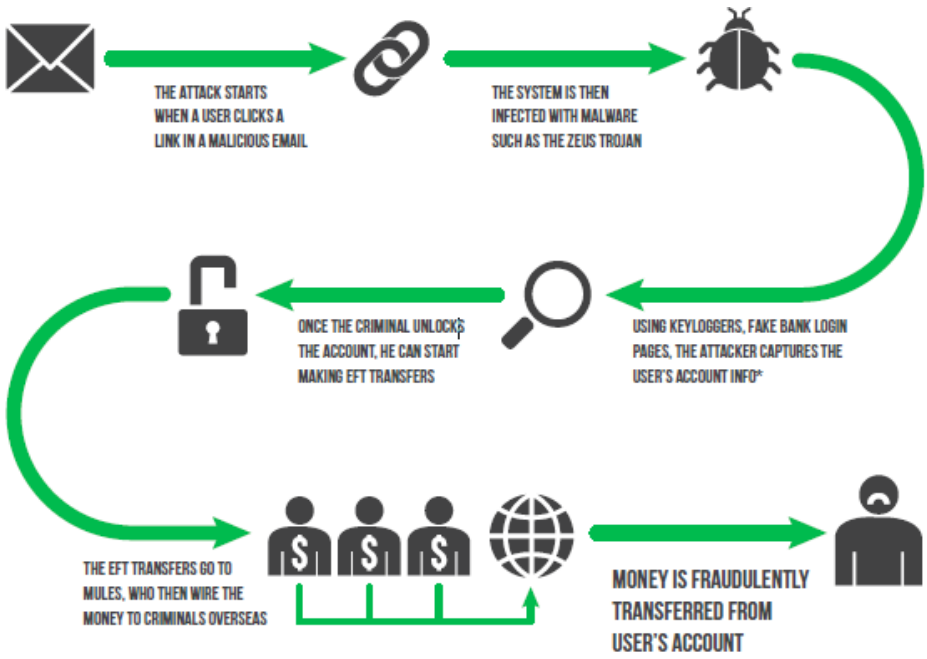

Fig. **17** Ejemplo del proceso seguido en una estafa bancaria, obtenida a través de una infección difundida por Spam

La agencia de estadísticas "*Internet World Stats*[14]" publicaba en su informe de 2012 que de los 144.000 millones de correos electrónicos que fueron enviados diariamente de media por más de 2.200 millones de usuarios en el mundo, más del 68.8% de este tráfico resultó ser correo electrónico no deseado. Otras fuentes consideran que este volumen es notablemente superior, situándolo entre un 80-85% llegando en los casos más extremos a 95% del total de mails enviados.

[14] Web de Internet World Stats http://www.internetworldstats.com/

La siguiente figura muestra el porcentaje de países con mayor volumen de Spam enviado en el mundo según los datos publicados por la compañía antimalware Kaspersky en su reporte anual de 2012[15]. En ella se puede observar como China y Estados Unidos, encabezan la lista junto con la India, ocupando entre estos tres países más de la mitad del Spam enviado en el mundo durante ese periodo.

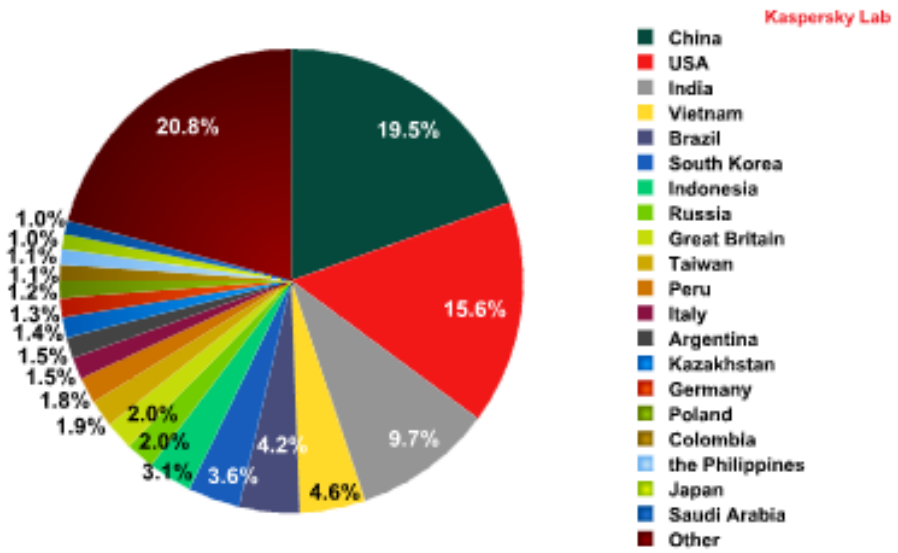

Fig. **18** Top 20 de países emisores de Spam en 2012 según Kaspersky Labs.

Analizando un nuevo informe, publicado por la misma compañía, esta vez basado únicamente en el segundo tercio de este año[16] (2Q 20013), puede observarse como, pese a variar las posiciones inferiores, incluyendo la aparición de España en la lista, los dos principales emisores de Spam mantienen su posición.

[15] Kaspersky Security Bulletin: Spam Evolution 2012 http://www.securelist.com/en/analysis/204792276
[16] Kaspersky spam in Q3 2012 http://www.securelist.com/en/analysis/204792251/Spam_in_Q3_2012

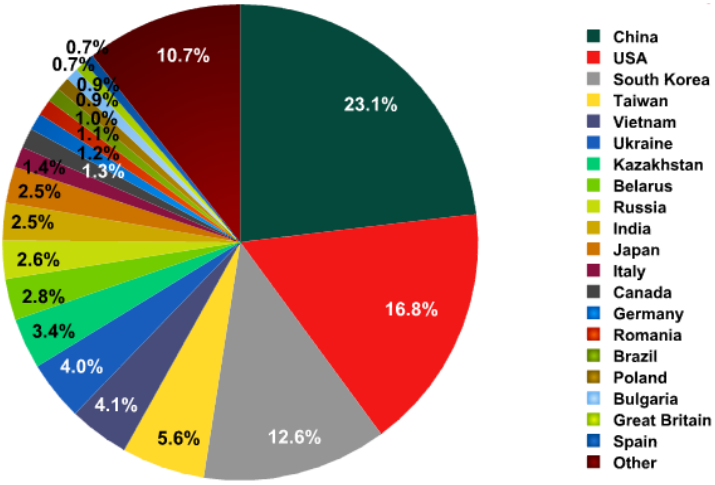

Fig. **19** Top 20 de países emisores de Spam 2Q 2013 según Kaspersky Labs.

Además de los beneficios obtenidos por las infecciones, el Spam proporciona grandes beneficios económicos a través de la difusión de campañas publicitarias, las cuales en ocasiones son generadas por las propias empresas y en otras por la subcontratación de estas a especialistas en el envío de Spam. Este beneficio no termina aquí, sino que esta amenaza también reporta sustanciales ganancias a través de la comercialización de enormes listas de direcciones de correo electrónico conseguidas a partir de infecciones malware o de los llamados "**Hoax" o bulos.**

Estos bulos, se envían en forma de mensajes con contenido llamativo para los usuarios, tales como ganchos publicitarios, injusticias sociales o historias inverosímiles, a los cuales se les solicita reenviar dicho email al mayor número de contactos formando las llamadas "cadenas" de emails. Si bien este método no constituye ningún delito como tal, proporciona a los ciberdelincuentes grandes cantidades de direcciones de usuarios las cuales almacenan y disponen para usos futuros.

3.3.3. **Phising**

Orientado directamente al robo de información personal y, en la mayoría de los casos, financiera al usuario, consiste en la falsificación y suplantación de la interfaz usuario de una entidad de confianza, la cual solicita a su víctima aquella información sensible que el ciberdelincuente necesite para perpetrar su estafa.

Habitualmente se presenta a los usuarios a través de un email cuyo origen es una dirección aparentemente fiable, el cual aludiendo un problema de seguridad urgente, redirige al usuario a un sitio web, el cual cumple toda la iconografía y apariencia de la entidad real, donde se le solicitarán y a su vez capturarán sus datos.

En las siguientes capturas se muestra un ejemplo de correo recibido aparentemente de la Entidad Bancaria online del Banco Santander (Openbank), y la web mostrada a continuación comparada con la original. Pequeñas diferencias como el indicador de conexión segura, o el acceso cifrado https en vez de http convencional nos hacen diferenciarlas.

Fig. **20** Ejemplo de correo recibido en una estafa de phishing.

Fig. **21** Comparación entre las web falsa y verdadera de Openbank.

Sin embargo, en los últimos años, tanto los casos del ya mencionado Spam como los de Phishing, han disminuido su presencia de manera notable en el envío de correos electrónicos y han traslado su presencia a las redes sociales con un incremento de casos en estas que comienza a preocupar en gran medida a las autoridades y a los propietarios de dichas redes. Atraídos por el crecimiento de tráfico de Facebook, Twitter y, aunque en menor medida, de Instagram y Pinterest.

Según el Informe sobre las amenazas para la seguridad de los sitios web, publicado por Symantec para el segundo trimestre de 2013[17]: "[…] *allí tientan a los usuarios con vales-regalo falsos o encuestas tras las que se oculta una estafa. Las ofertas falsas son el método elegido para más de la mitad (el 56 %) de los ataques realizados en las redes sociales. Por ejemplo, la víctima de una estafa de este tipo podría ver en un muro de Facebook o en Pinterest (donde los usuarios ven los «pines» de las personas a las que siguen o navegan por categorías) un mensaje que diga: «Haz clic aquí para conseguir un vale de 100 dólares». Al hacer clic en el enlace, se abriría un sitio web donde tendría que facilitar sus datos personales para poder*

[17] Informe sobre las amenazas para la seguridad de los sitios web 2013
https://www.symantec-wss.com/campaigns/14385/es2/int/assets/symantec-WSTR2-ES.pdf

beneficiarse de distintas ofertas. Los vales, por supuesto, son falsos, pero los emisores de Spam ganan dinero cada vez que alguien se inscribe en una oferta.

A veces, se utilizan sitios web falsos para obtener los datos personales o contraseñas de las víctimas (p. ej., los datos de su cuenta de Facebook o Twitter). Muchos de estos casos de Phishing aprovechan la fascinación que sienten muchas personas por los deportistas, actores o cantantes famosos. "

Por otro lado, algunos ejemplos de técnicas cuyo modus operandi es muy similar al empleado en el Phishing, y que igualmente tienen como objetivo la estafa al usuario son las siguientes:

Smishing: La variación respecto al Phishing es que el contacto con el usuario se realiza vía sms. El usuario recibe un mensaje de texto donde se le insta a verificar sus datos o acceder a su cuenta a través de un enlace que le redirige al sitio web falsificado.

Fig. **22** Ejemplo de Smishing

Pharming: Al igual que el Phishing, esta técnica redirige al usuario hacia uno o varios sitios web falsos, los cuales simulan ser los auténticos. Sin embargo, la diferencia reside en que en este caso el ataque no se realiza directamente contra el usuario sino contra los propios servidores DNS (Domain Name System) de un sitio, de modo que cuando el usuario intente acceder al sitio original a través de la URL correcta, será redirigido a una web falsa. Si bien esta técnica requiere de un nivel alto de conocimientos para su realización, consigue afectar a un número de víctimas mucho mayor en un solo ataque.

Pharming local: al igual que en el caso anterior, esta técnica se basa en modificar el sistema de resolución de nombres (DNS) del usuario. La diferencia en este caso es que esta modificación se realiza únicamente de manera local en el PC de la víctima, a través de la alteración del archivo "host". A diferencia del Pharming, esta técnica requiere un nivel de conocimientos técnicos mucho menor, por el simple hecho de únicamente tener que enfrentarse a los sistemas de protección de un usuario y no de un sitio web.

Vishing: Aunque podríamos considerar está técnica dentro del Phreaking, por el hecho de que el medio de contacto con el usuario sea a través del teléfono, dado que la línea de comunicación sigue siendo la red de datos se ha decidido incluirla en este punto. En este caso, el usuario recibe un correo o una llamada telefónica donde se le indica que ha de contactar con un número gratuito el cual, a través de una locución, solicita los datos personales o bancarios de la víctima.

3.3.4. **Scam**

Si hubiera que utilizar una palabra para referirse a las estafas o timos más tradicionales en internet este sería el término Scam. Dicho de otro modo, es el nombre utilizado para las estafas y engaños a través de medios tecnológicos.

Este tipo de estafas, no requieren de una técnica especial ni conocimientos avanzados de informática, sino que su principal arma es la ingeniería social. En ellas los delincuentes llegan a sus víctimas a través del correo ofreciendo grandes ganancias o pidiendo ayuda desde algún país de reconocida pobreza. Este tipo de estafas aparecen también en anuncios de compra/venta o webs de contactos donde los ciberdelincuentes establecen una relación con la víctima hasta conseguir engañarle y pedirle una suma de dinero para poder continuar su idilio. Algunos ejemplos de este tipo de estafas son los siguientes:

Citas online fraudulentas

Las citas online fraudulentas tocan la fibra sensible de las víctimas para acometer su propósito. La típica estafa online de citas comienza cuando el estafador publica una foto atractiva en un sitio de citas en Internet. A continuación, el estafador envía mensajes a otros

miembros del sitio web expresando su interés. El siguiente paso es iniciar una conversación personal con las víctimas, normalmente a través del correo electrónico o mensajes instantáneos, en los que los ciberdelincuentes cuentan una triste historia, creando una relación personal para pedir dinero, bienes u otros favores.

Fraude nigeriano

Este timo, también conocido como el "fraude de pago por adelantado", por lo general consiste en un mensaje de correo electrónico no deseado de un extranjero que necesita ayuda para grandes sumas de dinero de su país y ofrece al destinatario un porcentaje de su fortuna por ayudarle en la transferencia. Por desgracia, a pesar de que este timo es demasiado bueno para ser verdad, muchos de los destinatarios han picado y han perdido miles de euros en el proceso, ya que los ciberdelincuentes solicitan varios pagos por adelantado para facilitar el trato.

A precio de chollo por motivos personales

Al igual que en el caso anterior, en este timo también se requiere el pago por adelantado de una cantidad para efectuar una transacción claramente ventajosa para la víctima. En el mercado de compra/venta, aparecen anuncios que destacan por sus excelentes condiciones en los que al contactar con el vendedor para realizar la operación, este señala que por motivos personales o laborales no se encuentra en disposición de hacer el trato en persona pero sí muy interesado en finalizar el negocio. El estafador suele hacer pensar a su víctima que es ella quien estará en condiciones de realizar una operación increíblemente rentable y se ofrece a dar una serie de facilidades con el único requisito de enviar una pequeña cantidad de dinero. Una vez hecho el pago, el vendedor desaparece sin dejar rastro alguno.

3.3.5. Ataques DoS y DDoS

El objetivo de los ataques de Denegación de Servicio (en inglés Denial of Service) y de su versión extendida, los ataques DDoS (Distribute Denial of Service), consiste en, tal y como su nombre indica, conseguir provocar la indisponibilidad total o parcial de un sistema o red a través de la saturación o el agotamiento de sus recursos. La facilidad de ejecución de este tipo

de ataques y la dificultad encontrada en multitud de ocasiones para su mitigación, sitúan este tipo de ataques entre los más populares en la red.

La diferencia entre los ataques DoS y los ataques DDoS, reside en el número de máquinas origen de la amenaza, y por lo tanto en las dimensiones de esta. De este modo, mientras que el ataque original se realiza comúnmente desde un único equipo, los ataques de Denegación de Servicio Distribuidos, utilizan numerosos equipos como fuente para efectuar su ataque.

La utilización de una o varias **Botnets,** de manera coordinada, es la principal herramienta utilizada por los Ciberdelincuentes tanto para multiplicar el impacto de un ataque de Denegación de Servicio ejecutado desde un único equipo zombi, como para mantener su anonimato.

En otras ocasiones, la captación de equipos fuente se consigue a través de convocatorias sociales con motivos ideológicos. Este es el caso de la herramienta **LOIC** (siglás en inglés de Low Orbit Ion Cannon), la cual ha sido publicada a través de diferentes sitios web, en varias ocasiones, por parte de grupos de Ciberdelincuentes Organizados, con objeto de realizar ataques contra entidades enfrentadas ideológicamente a estas bandas.

A continuación se realiza una pequeña descripción de los tres tipos de ataques de Denegación de Servicio más comunes:

Ataques por Volumen: El objetivo de este método consiste en saturar el Ancho de Banda a través del cual un servidor determinado pone a disposición sus servicios a la red. La magnitud de estos ataques se mide a partir del tamaño del volumen de datos enviado, es decir, en Megabits o Gigabits por segundo.

Ataques por protocolo: Orientados a la capacidad de recursos hardware de un sistema, ya sean servidores o equipos de seguridad perimetral de una red, el objetivo de este tipo de ataque consiste en agotar dichos recursos hasta llegar al punto en que los sistemas dejan de responder y por tanto de ofrecer servicio. Podemos encontrar numerosas técnicas utilizadas para este tipo de ataques tales como los diferentes métodos de Spoofing, ataques de fragmentación de paquetes y sin duda la más popular, la generación de **SYN floods,** cuya técnica es utilizada por el famoso script *Slowloris***,** y que consiste en el intento de apertura de un gran número de conexiones simultáneas contra un servidor, sin llegar a realizar la

finalización de estas. El objetivo de esta consiste en alcanzar el límite de sesiones concurrentes que el sistema puede gestionar. La medición de este tipo de ataques se realiza en paquetes por segundo.

Ataques de capa de aplicación: Basados en la utilización de herramientas que atacan directamente a vulnerabilidades de los sistemas, bases de datos o aplicaciones, este tipo de ataques resultan por su dinamismo lo más difíciles de controlar. Su objetivo es, al igual que en el caso anterior provocar la saturación o caída de un servicio de modo que este quede totalmente indisponible. Los ataques **JavaScript** o el uso de **Xploits** de vulnerabilidades no resueltas y **Zero Day,** también conocidas como vulnerabilidades de día cero con objeto de hacer referencia a aquellas vulnerabilidades de reciente aparición aun no detectadas por las compañías responsables, son las principales herramientas para ejecutar esta técnica.

Si hasta este momento, los métodos descritos servían a los ciberdelincuentes en su gran mayoría para conseguir rentabilidad económica a través de la estafa y el engaño, los ataques de Denegación de Servicio utilizan como recurso la extorsión y el chantaje contra empresas y gobiernos, a los cuales instan a abonar cantidades de dinero a cambio de respetar o, en el segundo de los casos, restablecer sus servicios informáticos si las primeras amenazas no fueron atendidas.

Las consecuencias económicas que sufren las víctimas de dichos ataques, surgen a partir de la indisponibilidad de sus servicios, o lo que es lo mismo, de las ganancias no generadas durante el tiempo en que la plataforma permanece inaccesible, o de la pérdida de imagen o posición competitiva debido a dicha indisponibilidad.

Fig. **23** Esquema de un ataque DDoS.

El peligro de los ataques DoS y DDoS, reside además en la facilidad con que este tipo de amenazas están comenzando a ser ejecutadas por individuos inexpertos, gracias a los Kit de Herramientas disponibles en la web. Tutoriales de uso y explicitas instrucciones, consiguen que hasta un recién iniciado con los conocimientos justos del uso de internet pueda intentar este tipo de ataques.

3.3.6. **Defacement**

Del término inglés desfiguración, este método consiste en la alteración visual de un sitio web, generalmente modificado el directorio índice de la estructura de la página web utilizando, entre otras, técnicas de elevación de permisos como por ejemplo la de SQL Injection. El Defacement, es en algunas ocasiones la tarjeta de visita empleada por los Ciberdelincuentes, con objeto de mostrar, al administrador de la web o a los usuarios, su paso por allí y los fallos de seguridad encontrados en la misma. En otras, sin embargo, es simplemente el método empleado para deteriorar la imagen pública de la víctima o una forma de diversión para los delincuentes.

Al igual que los ataques Dos y DDoS, el beneficio económico obtenido a través de estas técnicas de sabotaje informático, reside en los delitos de extorsión y el chantaje a empresas o altos cargos, cuya imagen pública supone gran parte de la rentabilidad de su negocio.

En algunas ocasiones, también se han registrado casos de este tipo de vandalismo contra webs de partidos políticos, los propios miembros de dichos partidos o incluso contra organizaciones religiosas, todas ellas con motivo de protestas ideológicas (este tipo de sabotajes son conocidos como Ciberdelincuencia Ideológica).

3.3.7. **Ciberespionaje y ciberguerra**

Dentro del concepto de Ciberdelincuencia Económica, el Ciberespionaje o robo de información a través de la red, supone un enorme problema cuya trascendencia va más allá del simple robo de información personal o bancaria a un usuario común.

Utilizando, como ya se ha comentado anteriormente, la distribución de diferentes tipos de malware, principalmente del tipo troyano, capaz de sustraer datos confidenciales, además de otros métodos que conllevan la intrusión en sistemas remotos a través de diferentes técnicas de Hacking como el uso de Rootkits, ataques por fuerza bruta o SQL Injection, entre muchos otros en constante evolución, el problema del Ciberespionaje cobra una dimensión superior cuanto mayor es el valor de la información sustraída.

De este modo, cuando las víctimas pasan de ser simples usuarios, cuyas cuentas bancarias se han visto comprometidas, a diplomáticos, directivos de empresas, militares, trabajadores del sector industrial o de infraestructuras, o los propios sistemas y repositorios de datos tanto públicos como privados de los que cada uno de ellos hacen uso respectivamente, el Ciberespionaje se convierte en una herramienta capaz de obtener una información donde su valor no es sencillo cuantificar de manera trivial y la economía en juego es la propia viabilidad de una empresa o el desarrollo económico de un país.

Sin embargo, tanto empresas como gobiernos, conscientes de este tipo de herramientas, una vez más no juegan únicamente el papel de víctimas sino que, en ocasiones, son ellos mismos quienes, ya sea utilizando sus propios recursos internos o acudiendo al

mercado clandestino con el objetivo de contratar los servicios de profesionales del Ciberdelito con la capacidad técnica necesaria, utilizan el Ciberespionaje como herramienta habitual, para perpetrar el robo o filtración de datos confidenciales a través de los cuales es posible conseguir una ventaja competitiva sobre sus rivales más directos.

Analizando en primer lugar el caso de las empresas, el hecho de que a día de hoy, gracias al uso de las TIC (Tecnologías de la Información y la Comunicación), prácticamente toda la información tanto corporativa como de procesos económicos e industriales se encuentre informatizada y almacenada en red, , ha provocado que los tradicionales métodos de competencia desleal que pudieran utilizarse en el pasado hayan quedado obsoletos, para dejar su lugar a ataques de Denegación de Servicio, que interrumpan los procesos de negocio de sus competidores, y al **Ciberespionaje Industrial**, a través de diferentes métodos de intrusión y evasión de los sistemas de seguridad corporativos.

De igual manera, este hecho se sucede en el entorno del los desarrollos industriales y militares de muchos países, llegando incluso a afectar a las relaciones diplomáticas entre sus gobiernos, donde políticas de carácter tradicionalmente bélico, como son los Estados Unidos y países de asiáticos como China, Rusia, Irán o Irak, destacan en este sentido.

El hecho de que estos países se defiendan de dichas acusaciones alegando emplear el Ciberespionaje como una forma de defensa más que como una intrusión, con la consecuente controversia y reacciones adversas de los afectados, conlleva a una batalla de magnitudes iguales o superiores a los tradicionales conflictos bélicos, que se desarrolla de manera constante y en la mayoría de los casos silenciosa, conocida con el término **Ciberguerra**, en la que los gobiernos invierten gran parte de sus esfuerzos y recursos por mantener su estatus mundial y superar a sus enemigos.

Como no podía ser de otra forma, y haciendo honor a su denominación como “guerra de la información”, el papel que juegan los medios de comunicación en esta batalla es primordial, siendo estos quienes llevan el papel de mensajero y quienes en ocasiones hacen saltar la chispa de los conflictos.

Un claro ejemplo de ello, es la organización dedicada a la filtración de noticias **WikiLeaks**[18], fundada en 2007 por el hacker, programador y periodista australiano Julian Paul Assange[19] y aun activa a día de hoy con una importante repercusión mediática.

Saltando a la fama en el años 2010, en el que la organización publicara un video grabado 3 años antes en Afganistán, donde aparecían varios soldados estadounidenses disparando de manera indiscriminada y quitando la vida a un grupo de personas entre las que se encontraba el periodista de la agencia de prensa Reuters, Namir Noor-Eldeend, y dedicada a difundir todo tipo de información clasificada principalmente por parte del gobierno de los Estados Unidos, y a ofrecerse como organismo abierto a la recepción de todo tipo de informaciones verídicas que demuestren de algún u otro modo abusos o prácticas fraudulentas por parte de gobiernos o instituciones públicas o privadas, siempre asegurando mantener el anonimato de la fuente, la organización ha supuesto un verdadero problema institucional, y legal en algunos casos, a aquellos cuyo nombre ha aparecido en alguna ocasión en los supuestos escándalos filtrados a numerosas agencias de prensa.

Atacada y perseguida por gobiernos, con la intención de censurar sus acciones, y defendida públicamente por numerosos grupos Hacktivistas, entre los que destaca el grupo Anonymous, quien desde su aparición ha realizado numerosos ataques contra aquellos que no han decidido apoyar a la organización, aludiendo a la necesidad defender a aquellos que se exponen a los gobiernos opresores con el fin de mostrar a la opinión pública sus prácticas ocultas. La organización ha llegado a publicar numerosos casos de Ciberespionaje por parte del gobierno estadounidense a través de su Agencia de Nacional de Seguridad (NSA) a varias potencias mundiales como por ejemplo, contra el ejército chino[20], lo que le ha llevado a vivir verdaderos momentos de tensión entre ambos países en los últimos meses.

Sin embargo, Estados Unidos también ha sido víctima en numerosas ocasiones de casos de Ciberespionaje. Uno de los casos con mayor trascendencia en los últimos años, en

[18] Web de Wikileaks wikileaks.org
[19] Julian Assange biography. http://www.biography.com/people/julian-assange-20688499
[20] NSA fears Snowden saw details of China spying.
http://www.usatoday.com/story/news/nation/2013/07/11/nsa-snowden-espionage-china-microsoft/2510623/

este caso de **Ciberespionaje Industrial Militar**, fue el publicado en diciembre de 2011[21], en el que un avión de reconocimiento no tripulado estadounidense modelo Lockheed Martin RQ-170 Sentinel, fue capturado por el ejército iraní al intervenir en su sistema de navegación, mediante técnicas de GPS Spoofing, y hacerle aterrizar en suelo Iraní cuando el sistema consideraba estarlo haciendo en su base en Afganistán.

Además de este, el sistema fue atacado en diferentes vulnerabilidades de su sistema, que permitieron a los encargados de perpetrar el secuestro, anular el sistema de autodestrucción del aparato del que iba dotado el aparato como método de seguridad.

Fig. **24** Imagen del avión Lockheed Martin RQ-170 Sentinel capturado por el ejército iraní.

Un último ejemplo de casos de Ciberespionaje interesante de comentar, pese a no tratarse específicamente de un delito con aspiraciones económicas, sino como un mecanismo de investigación. Sería el publicado recientemente como una de las mayores redes de espionaje electrónico del mundo, cuya legalidad se encuentra actualmente en entredicho, y que sin embargo si muestra la increíble vulnerabilidad de los usuarios en Internet. Se trata del llamado caso PRISM.

[21] Iran 'building copy of captured US drone' RQ-170 Sentinel http://www.bbc.co.uk/news/world-middle-east-17805201

Una vez más con el gobierno de Estados Unidos como protagonista, las controvertidas publicaciones sobre el sistema informático utilizado por su Agencia Nacional de Seguridad NSA (National Security Agency) y sus servicios de inteligencia, con el fin de obtener todo tipo de información personal de los usuarios de las mayores empresas de Internet, tales como fotos, videos o mensajes, provocado toda una revolución en los medios de comunicación internacionales.

En palabras del director de inteligencia Nacional, James Clapper[22]: "*PRISM es un sistema informático interno del gobierno usado para facilitar la recolección autorizada por el gobierno de información de inteligencia extranjera desde proveedores de servicios de comunicación electrónica bajo supervisión de un tribunal [...] Esta autoridad fue creada por el Congreso y ha sido ampliamente conocida y discutida en público desde su creación en 2008*. *Estados Unidos ha desclasificado la existencia del programa para aclarar "impresiones indebidas" e "imprecisiones*". Según Clapper, PRISM no es un "*programa de recolección o minería de datos no divulgado", sino una herramienta para monitorizar las comunicaciones de ciudadanos no estadounidenses a través de sus metadatos*" (es decir, la información sobre quién envía una comunicación, a quién va destinada y cuándo se produce, sin llegar a acceder al contenido).

Sea cual fuere el cometido real y los medios empleados, esto ha provocado que empresas como Google, Apple, Microsoft, AOL, Facebook y Yahoo entre otras, estén viendo como cada vez más usuarios, mostrando su indignación ante este hecho, han comenzado a registrarse en servicios de mensajería que se publicitan como seguros y ajenos al programa, incrementando los ingresos de aquellos que rápidamente han visto un lecho de mercado emergente. Por otro lado empresas de mensajería como Lavabit, Silent Circle o Groklaw, han anunciado el cese de sus actividades en este sector por no encontrarse dispuestos a dar servicio bajo tales condiciones de espionaje.

[22] EEUU desclasifica PRISM al tiempo que se filtra su herramienta de catalogación de datos
http://es.engadget.com/2013/06/09/eeuu-desclasifica-prism-catalogador-boundless-informant-filtrado/

Las reacciones por parte de los gigantes de Internet afectados no se han hecho esperar y rápidamente han solicitado públicamente al gobierno de los estados unidos, una mayor transparencia y detalle sobre el alcance y uso de los datos recogidos, de cara a recuperar la confianza perdida por sus usuarios.

De igual modo, el parlamento europeo ha mostrado su malestar al gobierno americano y ha declarado investigar las actividades de vigilancia de los Estados Unidos sobre los ciudadanos europeos[23].

3.4 Ciberdelincuencia Social

Pese a que hasta este momento, se ha hablado de la Ciberdelincuencia como la ejecución de delitos de carácter lucrativo para los delincuentes, existen algunas acepciones más que pueden ser consideradas de igual modo dentro de ese concepto, como es el ejemplo de la Ciberdelincuencia Social.

Si bien es cierto, que su presencia en las Redes Sociales se sitúa como su mayor foco, y el crecimiento de estas ha marcado claramente su desarrollo, es necesario excluir de este estudio a las ya mencionadas estafas de Spam, Phishing o Scam ejecutadas en dichas redes, y cuyo objetivo no pertenece a este ámbito.

Al contrario que la Ciberdelincuencia Económica, la aplicación al delito Social que se busca en este término no tiene como finalidad la búsqueda de ningún tipo de rentabilidad monetaria.

Se considerará por tanto como Ciberdelincuencia Social, a aquellos delitos informáticos cometidos contra los derechos o la integridad propia de una persona, individuo o sociedad tanto en su carácter público como privado y cuyo único objetivo es el de obtener un

[23] El Parlamento Europeo investigará el espionaje electrónico de PRISM en los países de la Unión http://es.engadget.com/2013/07/04/parlamento-europeo-investigara-espionaje-eeuu-prism/

beneficio ,o satisfacer una motivación, personal por parte de los ciberdelincuentes a costa de sus víctimas.

Pese a que en algunas legislaciones, como es el caso de la española, aún no se tipifica acusaciones específicas para las diferentes formas de Ciberdelincuencia social, aunque sí estas si son penadas catalogándolas en sus versiones como delitos tradicionales, el Artículo 5 de la Declaración [24] Universal de los Derechos Humanos, deja muy clara a través de la afirmación citada textualmente: "*Nadie será sometido a torturas ni a penas o tratos crueles, inhumanos o degradantes",* la necesidad de tener muy en consideración y perseguir este tipo de amenazas.

A continuación se describen algunas de las formas más comunes de este tipo de Ciberdelincuencia.

3.4.1. **Ciberacoso**

Debido a la gravedad de sus consecuencias, por la dimensión del medio en que se desarrollan, y las dificultades que presenta para su prevención y lucha, el Ciberacoso o Acoso Cibernético, supone una amenaza a tener muy en cuenta en nuestra sociedad. La telefonía móvil junto con las redes sociales y los diferentes servicios de publicación de contenido audiovisual de la red, se presentan como el principal medio de acción de este tipo de delincuencia.

Se puede considerar como Ciberacoso, el intento o pretensión, de manera repetida, de causar: amenazas, daño psicológico, humillación, angustia, deterioro de la imagen, etc. a través del uso de los diferentes medios telemáticos.

Siguiendo el concepto principal, el Ciberacoso presenta dos ligeras variaciones que sin embargo son diferenciadas en el mundo de la Ciberdelincuencia.

[24] Declaración Universal de los Derechos Humanos http://www.un.org/es/documents/udhr/

***Ciberbullying*:** Término utilizado para aludir a los casos de Ciberacoso en los que, sirviéndose de los mismos medios que el anterior, tanto víctima como agresor son menores de edad.

En otras palabras, se trata de los tradicionales casos de acoso entre menores, los cuales se han trasladado, en general desde las aulas de colegios e institutos, a Internet aprovechando la sensación de impunidad y anonimato que ofrece la red.

La carencia de conocimientos y educación acerca del uso de la red como medio de difusión, por parte de muchos menores a la hora de publicar contenido personal, además de la falta de consciencia en cuanto a la gravedad de las acciones realizadas por parte de los agresores, son también en este caso factores agravante a la hora de ver como la integridad de las víctimas se ve vulnerada.

Insultos, amenazas y coacciones junto con vejaciones, humillaciones y escarnios públicos, ya sea en redes sociales, foros, blogs, fotologs o paginas de videos online, suponen la mayoría de los casos reportados en este ámbito, los cuales ocasionan graves consecuencias sociales y psicológicas para las víctimas, agravadas por su temprana edad y percepción particular de la realidad.

Tal es el impacto que puede llegar a ocasionar la presión sufrida por algunos jóvenes en este tipo de delitos, que ya son varios los casos de suicidio publicados en los últimos años. Como ejemplo reciente, podemos encontrarnos con noticias como la publicada por el diario el mundo, el pasado 19 de Agosto de este 2013[25], en la que se señala que representantes de la red social Ask.fm, donde jóvenes de todo el mundo se relacionan de forma digital, se han comprometido a reforzar su política de seguridad de cara a combatir los casos de Ciberacoso detectados en su página, entre los que se encuentra el caso de la menor de 14 años, Hannah Smith, la cual se quitó la vida tras sufrir un caso de Ciberbullying a través de su perfil.

La peculiaridad de esta web reside en la posibilidad de realizar preguntas a otros usuarios de forma anónima, lo cual que ha dado lugar a casos de acoso entre menores. Las

[25] Noticia de El Mundo.esLa red social Ask.fm toma medidas contra el ciberacoso tras el suicidio de una joven http://www.elmundo.es/elmundo/2013/08/19/navegante/1376937003.html

medidas anunciadas serán entre otras la de facilitar el acceso a la opción "denunciar usuario" y añadir requisitos adicionales, tales como una cuenta de correo electrónico, al formulario de registro que permitan poder localizar físicamente, mediante su dirección IP, a un posible acosador.

Otro caso de gran repercusión mediática fue el de la joven canadiense Amanda Todd, la cual fue hallada muerta en su casa en Octubre de 2012, tan solo un mes después de haber publicado un video en la web de videos online Youtube, en el que denunciaba estar sufriendo un agotador caso de Ciberbullying a raíz de un caso de **sexcasting** (término utilizado para aludir al intercambio de imágenes de contenido sexual por internet), en el que se mostraba parcialmente desnuda con 12 años.[26]

Fig. **25** Captura del video publicado por Amanda Todd denunciando su caso de Ciberbullying en Octubre de 2012

Cyberstalking: Con origen en el término en inglés, stalking, en español acecho, se basa en las acciones desempeñadas por algunos individuos, generalmente con algún tipo de trastorno o motivación obsesiva, mediante el uso de las tecnologías de comunicación, para acechar o acosar a una persona, grupo de personas u organización.

[26] Video de Amanda Tood http://www.ciberbullying.com/cyberbullying/2012/10/17/el-video-con-el-que-amanda-todd-luchaba-contra-el-ciberbullying-subtitulado-al-espanol-por-pantallasamigas/

Esta obsesión les lleva a espiar y perseguir la actividad en Internet de su víctima, enviar sms o publicar declaraciones en medios públicos así como a realizar falsas acusaciones o amenazas (además de otras acciones similares) contra sus objetivos, los cuales en multitud de ocasiones permanecen ajenos a este seguimiento durante mucho tiempo.

Cybergrooming: Conocido también simplemente como **Grooming**, o **Child Grooming,** la utilización de este término se emplea para referirse al tipo de técnicas empleadas en los casos de acoso sexual hacia un menor a través de Internet. El principal comportamiento de los individuos que lo practican se basa en el establecimiento de una relación y control emocional sobre un menor para, posteriormente, mantener una relación sexual de manera virtual.

En los casos de Gybergrooming, los delincuentes suelen presentarse ante sus víctimas a través de servicios de chat, redes sociales o incluso sitios web de juegos online para niños, donde estos dejan sus datos de contacto para compartir experiencias con sus iguales, presentando falsas identidades que les permitan establecer un primer contacto y una relación de amistad.

Posteriormente, los acosadores comienzan conducir las conversaciones con su víctima de modo que estas le permitan obtener determinada información sensible de carácter personal, como datos de sus contactos y familiares, y en algunas ocasiones también de una índole más íntima, la cual llegado el momento les permita chantajear y coaccionar al menor forzándoles a continuar con la relación en contra de su voluntad.

Una vez llegados a este punto, es cuando se desvelan los verdaderos deseos delictivos y el acosador comienza a requerir del menor el intercambio de imágenes vía, webcam, fotos de contenido sexual, incluso en ocasiones citas presenciales con intención de llevar a la realidad las relaciones establecidas por la red.

3.5 Ciberdelincuencia Ideológica

También conocida como **Ciberguerra Ideológica** o **Ciberdelincuencia Política,** está última denominación debido al hecho de ser el terreno político una de sus motivaciones principales, este tipo de Ciberdelincuencia, basada en expresar y difundir las diferencias de ideales, utiliza en su versión más nociva, el robo de información, el sabotaje, y la extorsión como sus principales armas.

Con el objetivo central de reivindicar y mostrar al mundo una forma de pensar opuesta a la de sus víctimas, a pesar de que ello conlleve la vulneración de derechos como los de la propiedad y privacidad, la Ciberdelincuencia Ideológica podría considerarse como la forma más antigua de este tipo de delincuencia, situando sus orígenes junto con la aparición de aquellos primeros hacker revolucionarios, cuyas motivaciones eran la de promover el libre acceso y difusión de la información y del conocimiento.

Un ejemplo de aquella forma de pensar, puede observarse en el siguiente fragmento, extraído y traducido al español del texto original en inglés, *"The Conscience of a Hacker"*[27] también conocido como "*El Manifiesto Hacker*", escrito el 8 de Enero de 1986 por el conocido pirata informático americano **Loyd Blankenship**, más conocido como "*The Mentor*", y que es considerado como una de las piedras angulares de la cultura Hacker:

"[…] Hacemos uso de un servicio que ya existe sin pagar, porque podría ser ridículamente barato, si no estuviera en manos de glotones hambrientos de ganancias, y ustedes nos llaman criminales.

Nosotros exploramos. . . y ustedes nos llaman criminales.

Nosotros buscamos detrás del conocimiento. . . y ustedes nos llaman criminales.

Nosotros existimos sin color, sin nacionalidad, sin prejuicios religiosos. . . y ustedes nos llaman criminales.

[27] Original article, "The Conscience of a Hacker". http://www.phrack.org/issues.html?issue=7&id=3&mode=txt

Ustedes construyen bombas atómicas, ustedes hacen la guerra, asesinan, engañan y nos mienten y tratan de hacernos creer que es por nuestro bien, pero nosotros somos los criminales."

Sin embargo, no se debe confundir esta declaración de aparentemente nobles intenciones con una única y común forma de pensar, sino que, tal y como ya se ha tenido ocasión de mencionar anteriormente en este documento, dentro de esta misma filosofía existen también muchas otras no tan nobles y mucho más perjudiciales motivaciones.

Tanto el perfil del ciberdelincuente como el de nuestra sociedad, han cambiado mucho desde aquellos años hasta ahora, y los primeros casos de divulgación de información sobre códigos fuente de programas informáticos, se han convertido a día de hoy en luchas anti sistema contra los gobiernos y leyes así como contra las empresas, cuyas prácticas contra el mundo y la sociedad, son entendidas por aquellos considerados por sus seguidores como héroes y defensores del pueblo, como el verdadero delito, provocando a estos grandes quebraderos de cabeza y llevándoles a inversiones millonarias en reforzar sus sistemas e infraestructuras de seguridad de la información.

3.5.1. **Ciberterrorismo y Hacktivismo**

Tal es daño, que los ciberdelincuentes pueden llegar a ocasionar a los gobiernos y a sus infraestructuras, que estos no han dudado en asignarles la denominación de ***Ciberterroristas,*** englobando en este término a todos aquellos que, ya sea por unas u otras motivaciones, atenten contra la integridad, la imagen o el bienestar de un estado o de sus habitantes, es decir, desde el terrorista y organizaciones terroristas tradicionales cuyo principal argumento es la religión y que han pasado utilizar la red como una de sus armas, hasta los nuevos grupos o bandas organizadas de Ciberdelincuentes cuyo fin es la protesta política o ideológica, donde sus miembros son conocidos como ***Hacktivistas***.

El Hacktivismo (término formado a partir de la unión de las palabras Hacker y activismo), consiste precisamente, en la gran mayoría de los casos, en la defensa de una serie

de ideologías políticas, comúnmente a favor de la libertad de expresión, de información y de una interpretación particular de los derechos sociales, cuyas protestas por parte de sus miembros se realizan a través del amplio abanico de posibilidades que ofrece internet, empleando comúnmente métodos no aprobados por el colectivo Hacker purista, por su carácter destructivo, como son los ataques de Denegación de Servicio o el Defacement de sitios web.

A diferencia del Hacktivismo, los actos de Ciberterrorismo no suelen contar con miembros cuya participación activa se realiza de manera consciente, sino que, en este caso los "soldados" que se sitúan en el frente del ataque son usuarios infectados, y adheridos como miembros de grandes botnets, que permanecen totalmente ajenos a su participación mientras sus equipos son controlados de manera remota por los verdaderos ejecutores.

Algunas de las primeras apariciones del Hacktivismo se publicaron a principios de los años 1990, con casos como el ataque, por medio de la propagación del gusano WANK[28] (siglas en inglés de War Against Nuclear Killers, en español, guerra contra asesinos nucleares), contra las redes de del Departamento de Energía Norteamericano (DOE), la Red Física de Alta Energia (HEPNET) y el programa de la NASA, SPAN, en motivo de protesta contra su programa nuclear y el uso de plutonio como combustible para el envío de vehículos espaciales y que infectó todos sus sistemas informáticos publicando en ellos una pancarta que indicaba el mensaje "*Sus sistemas han sido oficialmente WANKeados. Habláis de tiempos de paz para todos, y mientras os preparáis para la guerra*".

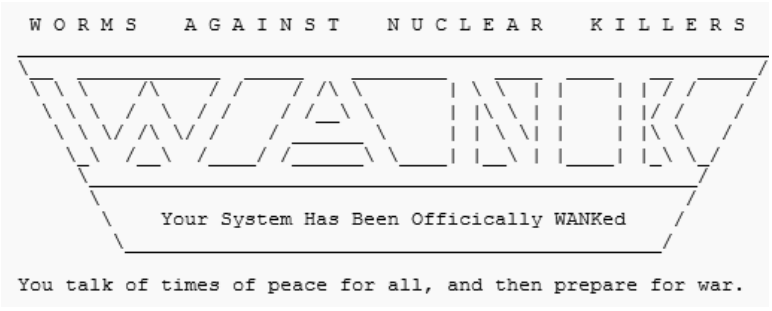

Fig. **26** Mensaje mostrado por el gusano WANK

[28] Advisory CA-1989-04 WANK Worm on SPAN Network. http://www.cert.org/advisories/CA-1989-04.html

A pesar de ello, estos grupos no cobraron la fama e importancia de la que gozan actualmente hasta finales de 2010, cuando se produjeron sabotajes como los perpetrados por defensores de la organización de filtraciones WikiLeaks lanzando ataques de Denegación de Servicio contra instituciones de pago como Paypal o MasterCard, que supuestamente boicoteaban a la organización. Este ataque, ejecutado con motivo de protesta por las persecuciones que estaban sufriendo los miembros de dicha organización, demostró el potencial de este tipo de bandas organizadas, las cuales aseguraron actuar en defensa de la libertad de expresión y la transparencia.

Ya sea de una u otra forma, tanto el Hacktivismo como el Ciberterrorismo han ido ligados a lo largo de los años, y tanto se han publicado casos de Ciberterrorismo ejecutados por grupos Hacktivistas, como se ha acusado y condenado a miembros de a estos grupos por la asociación ilícita para la práctica de acciones consideradas como terroristas.

A continuación, se describen dos de los grupos Hacktivistas más activos de los últimos años.

Anonymous

Sin ningún tipo de organización jerárquica conocida, y funcionando más bien como una red de activistas, agrupados en colectivos temporales, donde cualquiera puede formar parte del conjunto, con un mayor o menor compromiso, el movimiento Anonymous supone sin lugar a dudas el grupo más importante y numeroso del panorama del Hacktivismo actual.

El término “Anonymous” (anónimos en español), tiene su origen en el modo de identificación utilizado por algunas páginas web, donde era posible publicar comentarios sin identificarse. Estos comentarios de usuarios no registrados, se etiquetaban como “Anónimo”, y fue de esta calificación de donde empezó a surgir la idea de un colectivo de al cual se tachaba de no identificarse en sus publicaciones.

Surgido como un movimiento por diversión en el año 2003, el grupo comienza a manifestarse en acciones y protestas a favor de la libertad de expresión, la independencia en Internet y en contra de diferentes organizaciones, organismos públicos y sociedades de derechos de autor. Sin embargo es a partir del año 2008 cuando su fama comienza a crecer y en 2010, con su apoyo a la organización WikiLeaks cuando, la imagen del grupo salta a todos

los medios internaciones tras diversos ataques de Denegación de Servicio (DoS) realizados contra los sistemas de la CIA y otras compañías que se mostraron en contra de la organización.

Considerados por algunos como Ciberterroristas, y por otros como una organización revolucionaria compleja, cuyo centro de operaciones se plantea difícil de identificar, la filosofía del grupo dicta que básicamente se trata de gente disconforme con diferentes situaciones de la sociedad actual, la cual esconde su identidad tras la máscara del anonimato para sumarse a causas de reivindicación comunes, convocadas a través de la red.

Utilizando una simbología cuyos iconos han ganado una gran popularidad en nuestros días debido a su gran poder de difusión, el grupo no sólo muestra su presencia en internet si no que ya desde el 2011 se muestra en convocatorias y manifestaciones donde sus participantes adoptan la imagen del grupo en la red, correctamente vestidos con traje y corbata, y ocultos tras una máscara, que oculta su identidad real pero que sin embargo les identifica como miembros del movimiento, cuya figura representa al personaje Guy Fawkes[29], la cual ya fue utilizada por el protagonista en la versión cinematográfica de la novela V de Vendetta[30].

Fig. **27** Miembros del grupo Anonymous enmascarados públicamente con la imagen del personaje de Guy Fawkes.

[29] History of Guy Fawkes http://www.bbc.co.uk/history/people/guy_fawkes
[30] Película V de Vendetta http://wwws.warnerbros.es/vforvendetta/

El grupo colecciona una larga lista de víctimas de sus ataques por todo el mundo, entre las que se encuentran diferentes sitios web de gobiernos latinoamericanos (países con una gran actividad revolucionaria en la red), el sitio web de la CIA, las compañías Sony y Amazon, los sitios web de asociaciones de derechos de autor como la española SGAE (Sociedad General de Autores y Editores), o las páginas web del Ministerio de Cultura Español y de diferentes organismos públicos de países árabes como Túnez y Egipto.

Utilizando, como forma común de actuación, ataques Distribuidos de Denegación de Servicio (DDoS), a través de, entre otros métodos, el reclutamiento de internautas voluntarios, a disposición de los cuales se publican sencillas y diferentes aplicaciones web, previamente programadas con todas las herramientas necesarias, para unirse a las ofensivas.

Pese a que algunas fuentes han publicado su desarticulación por parte de operaciones de las fuerzas de seguridad de diferentes países, en varias ocasiones, la popularidad y propagación del grupo ha llegado a tales límites que a cada noticia publicada señalando un golpe contra la banda, individuos que se autoproclaman como parte del movimiento Anonymous responden de inmediato, haciendo notar su presencia latente e incontrolable en internet.

Ejemplo de esto fue el ataque de Denegación de Servicio recibido en la web de la Policía[31] Nacional Española el 11 de Junio de 2011, promovida a través de Twitter con el "hashtag" [32] #OpPolicia, y que se produjo tan solo un día después de la detención de tres personas acusadas de formar parte de la cúpula de la banda, como si de una organización jerárquica se tratara.

Sin lugar a dudas su actividad permanecerá latente al menos aún durante bastante tiempo debido a la constante aparición de nuevas divisiones y pequeños grupos organizados que se adhieren a la ideología y emplean las técnicas y la imagen del grupo.

[31] Anonymous ataca la web de la Policía Nacional http://www.cadenaser.com/espana/articulo/anonymous-ataca-web-policia-nacional/csrcsrpor/20110612csrcsrnac_2/Tes
[32] Using hastags on Twitter https://support.twitter.com/articles/49309#

LulzSec

El nombre de LulzSec, tiene su origen en la combinación de los términos, "lulz" y "security", siendo la primera de ellas una variación de la popular abreviación como símbolo de risa "lol" [33] (del inglés lots of laughts). Se trata de una simplificación del que es uno de los principales lemas del grupo "Riéndonos de su seguridad desde 2011".

Fue fundado a mediados de 2011, y a diferencia de la numerosa participación del grupo Anonymous, esta nueva asociación sólo se encontraba formado en sus inicios por 6 miembros, caracterizados por poseer altos conocimientos de seguridad informática, y cuyo número no ha llegado a ser mucho mayor.

También presenta diferencias en sus motivaciones, entre las que la defensa de ideales únicamente representa una minoría de estas siendo, en la mayor parte de los casos, búsqueda de vulnerabilidades y la diversión el único objetivo de sus actos..

Este grupo, cuya mayor actividad duró únicamente 50 días, los llamados "50 days of Lulz" (50 días de risa), fue el autor de los ataques en 2011 a la compañía Sony, en la que fueron sustraídas mas de 1.00.000 de cuentas de usuarios, del hackeo del sitio web Public Broadcastin Service, como protesta sobre un documental acerca de WikiLeaks, y de los ataques contra la página web de la CIA y la del Senado estadounidense. También en 2012, a través de la red Twitter, cuando ya se presuponía su difusión, publicaron un listado de datos personales de trabajadores de la NASA.

En su última etapa, se unieron al grupo de acción de Anonymous, siendo considerados en la actualidad como una división de estos. Colaboraron además en varias operaciones de manera conjunta contra diferentes sitios web de gobiernos, bancos y compañías, siendo la más famosa de estas la denominada "*Operación AntiSec",* la cual buscaba "*luchar contra los gobiernos corruptos*", a través de la sustracción y publicación de informaciones confidenciales con el objetivo de desacreditar y deteriorar la imagen de sus objetivos.

[33] Explicación de la abreviatura LOL http://www.frikipedia.es/friki/LOL

Fig. **28** Logotipos del grupo LulzSec (izquierda) y Anonymous (derecha) en colaboración en la Operación AntiSec.

Finalmente, según algunas fuentes de noticias[34], tras la detención por parte del FBI de varios de sus miembros, con la supuesta colaboración de uno de sus líderes, el grupo ha quedado desarticulado y sus actividades han cesado, siendo sus miembros acusados de delitos de conspiración entre otros.

[34] Associate of Hacking Group LulzSec Indicted for Conspiracy to Conduct Cyber Attacks http://www.fbi.gov/losangeles/press-releases/2012/associate-of-hacking-group-lulzsec-indicted-for-conspiracy-to-conduct-cyber-attacks

Capítulo 4. **Evolución y desarrollo**

4.1 La Ciberdelincuencia en la historia

A pesar de su corta vida, la ciberdelincuencia ha dejado una huella significativa a lo largo del tiempo. Tanto medios de comunicación audiovisuales como la propia red y sus usuarios se han hecho eco de todo tipo de hazañas y hecho famosas a las figuras más relevantes del mundo del Cibercrimen, las cuales han marcado en muchas ocasiones, un antes y un después en el camino seguido por los avances tecnológicos. En este punto se pretende dejar una pequeña aunque significativa muestra de dichos casos y de los sucesos y personajes más destacados de la historia de la ciberdelincuencia.

4.1.1. Un silbato que cambió el mundo

Sobre principio de los años 70, una conocida marca de cereales de la empresa Quaker Oaks, la cual aún hoy se encuentra en funcionamiento, comenzó a realizar una práctica para incrementar sus ventas que consistía en incluir un pequeño juguete en el interior de la caja. Estos cereales comercializados en EEUU se conocían con el nombre de "Cap'n Crunch", y el juguete que incluían era un pequeño e inofensivo silbato azul.

Hasta aquí esta historia no tendría nada de especial, si no fuera porque un día un joven ingeniero llamado **John Draper** recibió la llamada de un amigo ciego el cual le hizo darse cuenta de que, taponando uno de los agujeros del silbato, se obtenía un tono puro de 2600Hz, frecuencia que casualmente coincidía con el tono emitido por el sistema telefónico para indicar, según algunas fuentes el final de una llamada y por tanto de su tarificación, y según otras una redirección de marcado hacia otra numeración, la cual se observó que permitía realizar llamadas de larga distancia a través de la llamada a un número gratuito. Este hecho se debía a que por aquel entonces las líneas de voz y datos de larga distancia utilizadas por la compañía AT&T (American Telephone and Telegraph Corporation) compartían canal debido a diferentes reducciones de costes.

John Draper, utilizando está idea, construyó un dispositivo capaz de reproducir diferentes tonos reconocidos por la centralita los cuales le permitían modificar y controlar el comportamiento de esta para su propio beneficio.

La creación este invento, conocido como "**Blue Box**"[35] o caja azul, se convirtió en el **primer gran caso de lo que hoy conocemos como phreaking** o hacking telefónico de la historia y las noticias de su existencia dieron la vuelta al mundo, permitiendo a miles de usuarios realizar llamadas telefónicas de manera gratuita, ocasionando grandes pérdidas a las compañías de Teléfono, y contribuyendo de manera significativa al crecimiento del movimiento Hacker.

Fig. **29** Silbato regalado en las cajas de cereales Cap'n Crunch.

Esta noticia causó furor entre las Universidades de Ingeniería Electrónica y llegó a oídos de otro joven talento de la electrónica llamado **Steve Woznkiak,** el cual comenzó a fabricar las ya famosas cajas y a venderlas para ganarse un dinero a través del que fue su gran amigo y socio cofundador de su empresa, cuyo logotipo es hoy en día una manzana mordida, **Apple**. El nombre de su amigo no era otro que **Steve Jobs**. Con los pocos ahorros conseguidos de dichas ventas, ambos amigos consiguieron la financiación necesaria para lo que posteriormente daría un vuelco a su pequeña empresa y sacar a la luz otro de sus grandes proyectos, la creación de su proprio ordenador. Este prototipo, de lo que hoy en día

[35] Historia de la Blue Box. http://www.ionlitio.com/hackers-capitulo-i/

conocemos como ordenadores personales, dio lugar al primer ordenador de Apple: el Apple I y posteriormente al Apple II, ordenador más vendido durante los años 1970 y principios de los 1980.

Si bien, nadie duda de la parte negativa de cualquier tipo de acto delictivo, esta historia es sólo un ejemplo de cómo la ciberdelincuencia, desde sus orígenes hasta el día de hoy, ha ido condicionando y participando de manera constante la evolución de las tecnologías de la información. Es inevitable pensar, que quizá si aquellos jóvenes entusiastas y llenos de curiosidad no se hubieran saltado las leyes de la época, con el fin de satisfacer sus ansias de conocimiento y su curiosidad, muchos de los elementos de la sociedad de la información en la que vivimos serían diferentes.

4.1.2. **Figuras más representativas del cibercrimen**

John Draper: Conocido también con el sobrenombre de "Captain Crunch", debido a la marca de Cereales que le llevó a la fama, es considerado una leyenda en el mundo hacker. La magnitud de su descubrimiento comentado anteriormente dio nombre a una de las revistas del sector de la piratería informática más famosas de la historia, "The 2600 Magazine". Fue detenido en 1972 y posteriormente en 1977 por delitos de fraude contra las compañías telefónicas y trabajó durante un tiempo para la compañía Apple. Programó durante su estancia en prisión el editor de Textos EasyWriter, utilizado por dicha compañía, y actualmente trabaja como programador de software de seguridad informática.

Stephen Wozniak: Mencionado anteriormente como cofundador de Apple, y creador de los ordenadores Apple I y II. Genio de la electrónica que construyó su primera estación de radio a los 11 años y comenzó a diseñar sus propios ordenadores a los 13, comenzó su carrera como hacker de sistemas telefónicos para realizar llamadas de manera gratuita, llegando a llamar, según algunas fuentes, al mismísimo Papa en los años 70. El poseedor de la placa que le acredita como empleado nº1 de Apple, abandonó la compañía en 1985 y hoy en día se dedica a la enseñanza de manera altruista.

Kevin Mitnick: Denominado por el FBI y el Departamento de Justicia de los Estados unidos como "el criminal informático más buscado de la historia". También conocido como "El

Cóndor", es uno de los cracker y phreaker más famosos de la historia. Su habilidad para conectarse a servidores, robar información, interceptar teléfonos o desarrollar virus sorprende aún a día de hoy a los mejores en su campo. Considerado como un auténtico experto en el uso de la ingeniería social, fue procesado judicialmente en 1981, 1983, 1987 y por último en 1995, gozando esta última ocasión de una gran popularidad entre los medios debido al prolongado tiempo que llevó el proceso (más de dos años hasta que se celebró el juicio) y las excepcionales condiciones de aislamiento aplicadas a su reclusión, en las que se le prohibía estar en contacto con cualquier aparato informático y telefónico.

Ha sido acusado, en los diferentes procesos judiciales, de acceder y robar información a algunos de los sistemas informáticos más seguros del mundo, tales como la red del Pentágono, o los de las compañías Nokia, Motorola y Sun Microsystems. Tras su puesta en libertad en 2002 se dedica a la consultoría de seguridad en su compañía Mitnick Security.

Fig. **30** Cartel de busca y captura de Kevin Mitnick.

La vida de Kevin Mitnick sirvió como inspiración a varios autores para sus obras entre la que se encuentra el título "Takedown", el cual fue incluso llevada al cine.

Para su detención, fue crucial la ayuda del famoso Hacker Blanco ***Tsutomu Shimomura,*** el cual se tomó como un reto personal encontrar y desenmascarar a Mitnick cuando descubrió haber sufrido la intrusión y el robo de numerosos ficheros de su propio ordenador por parte del delincuente.

Kevin Poulsen: Ganó sus minutos de fama en 1990 tras hackear las líneas telefónicas de un programa de radio y asegurarse el premio consistente en un Porsche 944 S2. También conocido como "Dark Dante" se ganó la distinción de ser el primer pirata informático acusado de espionaje por el supuesto robo a través de escuchas telefónicas de información clasificada a las Fuerzas Aéreas estadounidenses. Tal era la actividad criminal que desarrollaba, que era conocido en los medios como el "Hannibal Lecter de los delitos informáticos". Al igual que Kevin Mitnick fue perseguido por el FBI y condenado, en este caso a 51 meses de prisión y una multa de 56.000 dólares. Su vida fue el tema del libro "The Watchman" y hoy en día es periodista y editor de la revista Wired. Al igual que muchos de los ciberdelincuentes en la historia, cambió de bando y en 2006 ayudó a la policía a identificar a 744 individuos por delitos sexuales en MySpace.

Adrian Lamo: Conocido como ***"***El hacker Vagabundo" por realizar todos sus ataques desde cibercafés, bibliotecas y edificios abandonados. Lamo consiguió vulnerar las defensas de grandes compañías como Yahoo, Google y Microsoft aunque en algunos de los casos informó a estas de los agujeros de seguridad encontrados, incluso ayudándoles de manera desinteresada a solucionarlos. En 2003 accedió a los servidores del New York Times de donde extrajo información de miles de personas que en alguna ocasión habían escrito para el periódico, incluyendo celebridades y ex presidentes.

En los últimos años, Lamo ha colaborado con la justicia en la investigación sobre Bradley Manning, soldado del ejército estadounidense acusado de filtrar documentos clasificados a la organización WikiLeaks.

En abril de 2010, se le diagnosticó el síndrome de Asperger, trastorno del espectro autista comúnmente asociado a individuos de gran inteligencia con dificultades para socializarse.

Gary McKinnon: Considerado por muchos como el mayor hacker militar de todos los tiempos y acusado de acceder en hasta 97 ordenadores militares abarcando desde bases del ejército estadounidense hasta las redes de la NASA o El Pentágono. Eliminó 1.300 cuentas de usuarios y dejó sin servicio durante casi una semana la red informática del Departamento de Defensa de EEUU. Los ataques perpetrados por "Solo" (como era conocido en la red) tenían un objetivo cuanto menos peculiar, según sus propias declaraciones *"buscar evidencias de la*

existencia de OVNIs y probar que el gobierno estadounidense posee tecnología antigravitatoria".

Utilizando técnicas de sorprendente sencillez, las cuales básicamente buscaban sistemas cuyas credenciales de acceso por defecto no habían sido modificadas, el gobierno de Estados Unidos estimó los daños causados por las intromisiones de "solo" en más de 1.220.000 dólares, siendo, según declaraciones del fiscal, "el mayor caso de hackeo militar de la historia". Se enfrenta a un proceso judicial aún en curso que le puede suponer hasta 5 años de prisión y una multa de unos 228.000 euros.

Robert Tappan Morris: Hoy en día profesor en el Instituto Tecnológico de Massachusetts, es considerado como el creador del que pudo ser el primer "gusano" informático. En 1988, aún siendo estudiante, liberó un virus que llegó a infectar 6.000 equipos basados en Unix causando graves daños y pérdidas millonarias. Aunque Morris declaró estar midiendo el tamaño del entonces recién nacido internet, se convirtió en la primera persona condenada por la ley de Fraude computacional de Estados Unidos. Siendo condenado a tres años de libertad condicional y 400 horas de servicios comunitarios. Actualmente se exhibe en el museo de la Ciencia de Boston un disco duro que según dicen contiene el código de su virus.

Albert González: Considerado por la prensa en 2009 como "*el autor del robo del siglo*", fue acusado ese mismo año de ser el presunto cerebro del robo y venta ilegal de 130 millones de números de tarjetas de crédito y débito, batiendo todos los record registrados. Las empresas T.J. Maxx y Marshalls, fueron las más afectadas en su último golpe, sufriendo el robo de más de 45.6 millones de números almacenadas en sus bases de datos.

Curiosamente fue detenido previamente en 2003 por un caso de robos de números de tarjetas donde las autoridades le ofrecieron trabajar en el servicio secreto del gobierno, cargo que aceptó y cuyas investigaciones utilizó para afianzar aún más sus contactos y conocimientos. González, que lideraba un grupo formado por varios Hacker de diferentes partes del mundo, conocido como "ShadowCrew" fue condenado a 20 años de prisión a su vez que también sus cómplices recibieron diferentes condenas según la legislación de su país, destacando entre estas la condena aplicada a ***Maksym "Maksik" Yastremskiy*** de 30 años, por parte de las autoridades Turcas.

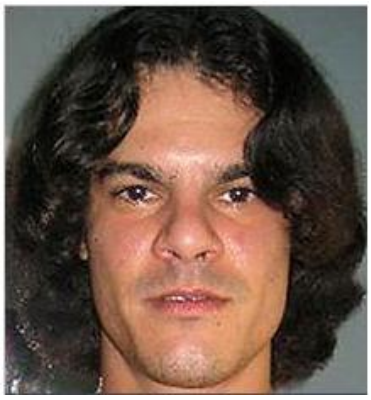

Fig. **31** Albert Gonzalez

Jonathan James: conocido por ser el primer menor de edad enviado a prisión por hacking. En el año 2000, con tan solo 16 años de edad fue condenado a 6 meses de cárcel por acceder a los sistemas del Departamento de Defensa y de la NASA y copiar software e información sensible por valor de 1.7 millones de dólares. James, también conocido como "c0mrade" (camarada), declaraba no provocar ningún daño con sus acciones pese a las acusaciones y pérdidas económicas reclamadas.

En el año 2008, pese a encontrarse en libertad y haber creado una empresa de seguridad informática, agentes del FBI entraron en su casa como parte de una investigación de robo de datos de tarjetas de crédito de gigantescas dimensiones (por la que posteriormente fue juzgado Albert Gonzalez). Dos semanas después apareció muerto en su casa junto a una nota de suicidio declarando su inocencia y sintiéndose perseguido.

Michael Calce: Popularmente conocido como "MafiaBoy", en febrero del año 2000 y con tan sólo 15 años, lanzó un ataque de Denegación de Servicio (DDoS), contra las web de gigantes de Internet tales como la cadena CNN, Amazon, Ebay, Yahoo, Dell y E*TRADE. Tal fue el impacto de los daños provocados a estas empresas, que el mismo Presidente de los Estados Unidos en ese momento, Bill Clinton, convocó la primera cumbre de ciberseguridad de la Casa Blanca con objeto de su detención inmediata.

Finalmente fue detenido y acusado de 56 cargos de hacking contra sitios web y sentenciado a ocho meses de internamiento en un centro de recuperación juvenil y un año de libertad condicional.

Su vida se narra en el relato "*Mafiaboy: A Portrait of the hacker as a young man*" y hoy en día se dedica a participar como columnista en diferentes revistas escribiendo sobre temas de seguridad informática y compartiendo sus conocimientos en diferentes foros.

Otras figuras, no tan conocidas pero que igualmente causaron graves daños y pérdidas económicas son ***David L. Smith***, creador del virus Melissa propagado en 1999 y que causó daños estimados en más de 80 millones de dólares y ***Sven Jaschan***, creador del virus Sasser con tan solo 17 años ,el cual afectaba varios de los sistemas operativos de Microsoft (Windows 2000, 2003 Server y XP), y que fue detenido en 2004 tras la denuncia por parte de sus vecinos motivados por la recompensa ofrecida por parte de la compañía.

4.1.3. **Casos de mayor trascendencia desde el año 2000**

Continuando con el repaso sobre la historia de la ciberdelincuencia, desde el año 2000, hasta nuestros días, el Cibercrimen ha ido dejando muestra de su crecimiento. La compañía McAfee publicó en 2011 un informe titulado "Una gran década para el Cibercrimen[36]", el cual hacía un análisis muy interesante de los acontecimientos más significativos publicados desde el año 2000 al 2010. Este informe recalca que parte del crecimiento del Cibercrimen se debe al arrollador crecimiento del uso de Internet, partiendo de los 361 millones de usuarios que se contabilizaban en internet en el año 2000, hasta los casi 2.000 millones en 2010. De igual manera se destaca el crecimiento de los sitios web de comercio electrónico, e-commerce, y los servicios de pago y banca online, finalizando con el boom de las redes sociales.

A continuación se comentarán los casos más trascendentales, que fueron noticia a lo largo de los años, siguiendo y basándonos en las cuatro etapas marcadas por McAfee en su informe.

[36] McAfee. Una gran década para el Cibercrimen. 2011 http://www.mcafee.com/es/resources/reports/rp-good-decade-for-cybercrime.pdf

2000–2003

El llamado "Efecto 2000" había pasado, y el mundo continuaba. El ya comentado ataque de DDoS contra CNN, Yahoo y EBay, perpetrado por Michael Calce, sólo tardó dos meses en ser noticia en todo el mundo. Poco tiempo después, comenzó a ponerse de moda entre los ciberdelincuentes el envío de mensajes de correo electrónico con enlaces o archivos adjuntos que provocaban la instalación de software malicioso. Justamente de este modo funcionaba el conocido gusano "**I love you"**.

Creado por el joven filipino ***Onel de Guzmán,*** el cual provocó **la primera infección masiva a nivel mundial**. El virus, llegaba en forma de correo electrónico con un documento adjunto titulado "*Love-Letter-For-You*", se auto ejecutaba y auto enviaba a todas las direcciones de correo de la víctima cuya curiosidad llevaba a abrir el archivo.

Se extendió por un Internet donde todavía prácticamente nadie sentía la necesidad de disponer de ningún software de seguridad, afectando a cerca de 50 millones de ordenadores de todo el planeta en tan sólo una semana desde su aparición, es decir, el 10% de los ordenadores conectados a Internet en aquel momento. Sus daños se estimaron en al menos 5.500 millones de dólares y afectó a sitios como el Pentágono, los parlamentos británico y danés y compañías como Ford, Vodafone, y las españolas Iberia, Prisa, Endesa y Telecinco.

Este virus marcó un antes y un después en las infecciones por correo electrónico y el crecimiento del Spam, y mostró el camino para combinar la ingeniería social con nuevas técnicas de malware.

Mientras tanto el crecimiento de los accesos via Wi-Fi era notable, con una seguridad más que deficiente, y servicios como Napster y la aparición del Ipod comenzaron a poner de moda el uso de la música digital y los archivos .mp3, dibujando un nuevo marco social donde más tarde los temas de mayor éxito serían el medio perfecto donde incluir archivos infectados.

2004–2005

Internet comenzaba a despuntar como medio de comunicación y como tal, la publicidad empezaba a estar presente en todos los rincones. El informe califica de ingeniosa la **aparición del *adware*** o software compatible con la publicidad, la cual aparecía en forma de ventanas emergentes con anuncios basados en las búsquedas del usuario. Las empresas de

publicidad vieron como su negocio aumentaba junto con la proporción de equipos infectados y los ciberdelincuentes comenzaron a hacer negocio de esto y a ganar importantes sumas de dinero, que crecían más cuanto mayor era el número de equipos que infectaban.

También comienza a aparecer el software espía o "Sniffer" que capturaba y reenviaba los sitios web visitados por el usuario e incluso las teclas pulsadas, entre las que se encontraban password de acceso a servicios web.

Pero el avance más importante de esta época fue la aparición del concepto de los equipos zombi o bots y los ejércitos formados por estos, las **botnets**. Los ciberdelincuentes se centraban cada vez más en el beneficio económico de sus actos y llegaban a infectar miles de máquinas al mismo tiempo, las cuales podían controlar de manera remota para lanzar ataques o enviar emails de forma distribuida y a la vez simultánea. Los beneficios obtenidos por chantajes a empresas y por las ventas generadas por el spam de convertían en, cada vez más, una forma de vida.

En 2010 la policía española, cerraría la que hasta el momento se consideraba la mayor botnet del mundo, la **botnet "Mariposa**", la cual llego a contar con cerca de 13 millones de equipos zombis.

Antes de esto, en 2004, aparece el gusano **"Mydoom",** el cual tiene el honor de ser el gusano cuya propagación por la red fue la más rápida hasta la fecha. Generó tal volumen de Spam, que ralentizó el acceso global de internet en un 10% y ocasionó unas pérdidas estimadas en 38.000 millones de dólares según el informe de McAfee.

2006–2008

En esta época, la figura del ciberdelincuente solitario comienza a perder peso, dando lugar a nuevas estructuras organizadas, que comienzan a funcionar como mafias y comunidades, y a actuar de manera más discreta, orientándose más hacia el negocio y menos hacia el reconocimiento social. El famoso problema del Autorun, función de Windows que iniciaba programas de manera automática desde dispositivos externos, es descubierto y empleado en multitud de distribuciones de software malicioso.

En Julio de 2007 se detecta por primera vez el **Troyano Zeus o Zbot**, un virus destinado a la recolección de todo tipo de datos, incluso de banca online, y cuyo código se comercializa

en internet para su libre modificación, lo que convierte su detección en una tarea realmente difícil, llegando hasta las 700 variantes hoy en día. El impacto de este temido virus es tal, que a día de hoy sigue siendo una de las más importantes amenazas de la red y formando una serie **Botnets** cuya estimación de equipos infectados llega a los 3,6 millones de equipos según algunas fuentes. Nuevas oleadas de difusión y versiones del virus han ido surgiendo de manera periódica. En 2009 con el crecimiento de las redes sociales, se estimó el envío de más de 1,5 millones de mensajes de phishing a través de Facebook con el objeto de difundir el Troyano. Recientemente, varios medios han publicado de nuevo una fuerte presencia de otra nueva versión, a través de falsos enlaces en Facebook.

En Octubre de 2008 sale a la luz el virus "**Conficker**", o Downup, el cual infectó a millones de ordenadores con sistemas operativos Windows, pasando a ingresar a las primeras posiciones de la lista del malware más dañino de la historia. Marcando una nueva tendencia de sofisticación en el desarrollo del malware, se basaba una vulnerabilidad de los sistemas operativos de Microsoft que le permitía ejecutar su código malicioso, el cual entre otras funcionalidades incluía un sistema de registro de pulsaciones o Keylogger, que permitía capturar y enviar la información tecleada por el usuario.

Tal fue el impacto causado por esta infección que la compañía de Bill Gates ofreció en enero de 2009 una recompensa de 250.000 dólares por cualquier información que llevara a la detención de su creador. Cinco años después, el creador aún sigue siendo desconocido y el malware ha vivido nuevos brotes en diferentes variantes.

2009–2010

El crecimiento exponencial de las redes sociales, aparecidas tan solo 4 o 5 años antes, no deja indiferente a nadie, y la red de Facebook con más de 500 millones de usuarios, junto con la de Twitter con más de 200 millones, se convierten en el nuevo objetivo.

La **ingeniería social** se convierte en la principal arma utilizada por los ciberdelincuentes para llegar a sus víctimas de aquí en adelante. La vida en internet cobra tal paralelismo con la vida cotidiana de los usuarios que estos vierten de manera indiscriminada todo tipo de información personal en sus perfiles, permitiendo a los criminales conocer hasta el más mínimo detalle de la vida de sus víctimas, temas hasta ahora sin importancia como gustos personales, información de familiares y amigos e incluso dónde pasaron las últimas vacaciones

o el nombre de su pareja, suponen una cantidad suficiente de datos como para diseñar cebos y engaños “hechos a medida”.

Este nuevo método de distribución de malware a través de las redes sociales, utiliza como remitentes a los propios contactos de la red de la víctima, y se disfraza en útiles aplicaciones como por ejemplo conocer quien ha visitado tu perfil, consiguiendo elevados porcentajes de éxito y distribuciones increíblemente ágiles.

Por otro lado, las bandas organizadas cada vez cobran más fuerza. Aparecen ejemplos como los ataques distribuidos de denegación de servicio (DDoS) contra sitios web como los de MasterCard y Visa por parte de los “**Hacktivistas**”, término acuñado como resultado de la combinación de Hacker y activistas, con el que se hacía alusión a los individuos con motivaciones políticas, del sitio de filtraciones de noticias internacionales, WikiLeaks.

La figura de la banda organizada “**Anonymous”,** cuyos primeros ataques se registraron en 2008, comienza a tomar grandes dimensiones en la red, el número de seguidores de la banda crece vertiginosamente a la vez que sus actos de protesta sociales y políticos se irán sucediendo de manera cada vez más frecuente y con mayores consecuencias.

En 2009, el portal de empleo **Monster** recibió un ataque, según varias fuentes con origen en Ucrania, del que fueron sustraídos perfiles, correos electrónicos y números telefónicos a más de 75 millones de usuarios.

2010–2012

Si bien el informe de McAfee no contempla esta última etapa debido a su fecha de publicación, la información bibliográfica disponible es más que suficiente para analizar este último periodo.

Tanto el malware como las estafas por internet continúan su creciente evolución y a los usuarios cada vez le resulta más complicado permanecer seguros en la red por sus propios medios, en una sociedad donde “estar online” la mayor parte posible del día ya es toda una preocupación.

El crecimiento del uso de los teléfonos móviles llevado de la mano del boom de los Smartphones les hace saltar a la palestra como nuevo objetivo del malware, ocupando el sistema operativo de Google “Android”, la gran mayoría de las miradas.

Los **acortadores de URL** devuelven el anonimato a los enlaces a sitios maliciosos y sistemas de autodescarga de adware y malware. Los usuarios acceden a enlaces cuyo destino no pueden verificar fácilmente y esto es empleado por los ciberdelincuentes para propagar sus amenazas. La red Twitter, cuya característica principal es la de publicar contenido en menos de 140 caracteres, se ve inundada por este tipo de enlaces maliciosos.

Además, se recupera un antiguo sistema de escritura de códigos para la difusión de enlaces hacia los dispositivos móviles, los **códigos QR** (Quick Response). Este sistema de códigos, similar a los tradicionales códigos de barras, y que permite codificar caracteres en forma de imagen bidimensional, el cual ya era utilizado en la industria de la automoción desde mediados de los 90s, comienza a ser utilizado por las compañías para distribuir sus campañas de marketing a través de los ya omnipresente Smartphone. Estos, con una pequeña aplicación embebida pueden interpretar dichos códigos y acceder a las URLs promocionales de manera automática.

Como era de esperar, los cibercriminales adoptan rápidamente esta nueva técnica y lo emplean para distribuir, de manera similar a los acortadores de url, malware y spam sirviéndose de la tan valiosa curiosidad de los usuarios.

Fig. **32** Ejemplo de código QR (Quick Response)

Por otro lado aparecen los nuevos servicios “en la nube”, llenos de ventajas de movilidad y rendimiento para el usuario y a su vez abriendo un nuevo campo donde los ciberdelincuentes pueden fijarse nuevos retos accediendo a enormes fuentes de recursos centralizadas.

En septiembre de 2010 el mundo del malware presenta a su nueva creación, el gusano **Stuxnet**[37], considerada por muchos la pieza de malware más sofisticada hasta la fecha. Atacando, la planta nuclear de Bushnehr, en Irán, con el objetivo de sabotear las centrifugadoras de enriquecimiento de uranio, esta nueva forma de malware capaz de interceptar los comandos de los sistemas Siemens SimaticWinCC SCADA, supone el primer caso de **malware industrial**, capaz de interactuar con sistemas electrónicos, hasta el momento ajenos al mundo de la propagación de códigos maliciosos, y capaz de provocar daño físico real a una infraestructura.

Bautizado como el primer arma de de ciberguerra de la historia, Eugene Kaspersky, experto en seguridad informática y cofundador de KasperskyLabs, indicó que Stuxnet sólo pudo ser creado con el apoyo y soporte de una nación. "*Me temo que es el momento del* ***ciberterrorismo, las ciberarmas y la ciberguerra***", señaló el analista, basándose en informaciones que atribuyen la creación del virus al gobierno Israelí, con el apoyo de Estados Unidos, para sabotear el programa nuclear Iraní.

En cuanto a Ciberdelitos, el robo de información confidencial a grandes compañías, fue noticia una vez más. En Mayo de 2011, la compañía Sony sufrió hasta 10 ataques contra diferentes sectores de su estructura empresarial, siendo el más sonado el ataque contra la división **PlayStation Network**[38]**,** que supuso la sustracción de más de 77 millones de cuentas de usuarios y una caída del servicio de 25 días. La compañía sufrió además duras críticas tras no desvelar, hasta pasados siete días, que los datos bancarios de los usuarios también habían sido comprometidos. Las acciones de la compañía cayeron a valores de hacía 32 años y posteriormente, según citan diversas fuentes, ha sido sancionada con 250.000 libras de multa, motivo de las escasas medidas de seguridad aplicadas a la protección de la información confidencial de sus clientes.

[37] Stuxnet y el nacimiento de la ciberguerra
http://www.theqore.com/articulos/6560/Stuxnet-y-el-nacimiento-de-la-ciberguerra

[38] Securitybydefault. Recopilación de los ataques a Sony.2011
http://www.securitybydefault.com/2011/05/recopilacion-de-los-ataques-sony.html

En Julio de 2011, Microsoft ofrecería una recompensa de hasta 250.000 dólares por información sobre los creadores de **"Rustock",** una botnet mundial con capacidad para enviar más de 30.000 millones de correos electrónicos no deseados al día (Spam). Según una nota de prensa publicada por la compañía Symantec, tras el cierre de la red en Marzo de ese año, la cual llevaba operando desde 2006, el Spam mundial cayó en un 33,6%.

En junio de 2012, la red social **LinkedIn**, también fue atacada en sus bases de datos, sufriendo el robo de más de 6 millones de contraseñas, que posteriormente fueron publicadas, aunque con un sistema de encriptación débil, en un foro ruso. La compañía de seguridad Rapid7, publicó una curiosa infografía que trataba de hacer ver la falta de seguridad que los usuarios habían empleado a la hora de establecer sus contraseñas, siendo las más usadas '1234', 'work' y 'link'. La siguiente imagen muestra una captura de dicha infografía.

Fig. **33** Contraseñas más populares robadas de LinkedIn

4.1.4. Últimos casos de Ciberdelincuencia publicados

La línea ascendente del cibercrimen en la última década no ha cambiado su tendencia en 2013 y, en lo que llevamos de año, numerosos casos han ocupado las páginas de la prensa internacional.

La compañía Panda Security publicaba algunos de los casos de más importantes en su primer informe trimestral de este año. Aunque algunos ya se han citado en este documento, a continuación se muestran con más detalle.

Twitter, Facebook, Apple y Microsoft, víctimas del mismo ataque

El pasado 1 de febrero, Twitter publicaba un artículo en su blog, "Keeping our users secure", explicando cómo la propia red social había sido víctima de un ataque que ha acarreado el acceso ilícito a información de hasta 250.000 de sus usuarios. Un par de semanas más tarde, Facebook publicaba también un artículo en su blog, "Protecting People On Facebook", comentando las características de una agresión donde, aparentemente y según fuentes de la red social, no fueron comprometidos datos de clientes. Tan sólo unos pocos días después del anuncio de Facebook, representantes de Apple informaron a Reuters de que habían sido objetivo de este mismo ataque. Finalmente, Microsoft se sumó también al listado de los atacados. Como denominador común, todas estas agresiones utilizaron un agujero de seguridad en Java desconocido hasta el momento y para el que no existía parche, lo que se conoce como una vulnerabilidad zero day ó 0-day.

[…] La cuenta de Twitter del fabricante automovilístico Jeep sufrió una agresión muy similar. En este caso se anunció que la firma había sido adquirida por Cadillac. Otro tipo de hackeos en cuentas de Twitter que hemos observado a lo largo de este trimestre tienen un tinte más político. Un grupo de ciberdelincuentes autodenominado "Syrian Electronic Army" consiguió hackear diferentes cuentas pertenecientes a diferentes organizaciones. Al parecer, primero lanzaron ataques de phishing para poder obtener las credenciales de acceso a Twitter y posteriormente secuestrar las cuentas. Entre sus víctimas figuran Human Rights Watch, el servicio de noticias francés France 24 o el servicio meteorológico de la BBC

Fuente: Panda Security 05/2013

http://prensa.pandasecurity.com/2013/05/la-lucha-contra-la-ciberdelincuencia-a-nivel-global-discurre-por-buen-camino-durante-los-tres-primeros-meses-del-ano/

Más de 20 países afectados por un ciberrobo bancario de 45 millones de dólares

Una red global de ciberdelincuentes hurtó 45 millones de dólares (unos 34 millones de euros) de dos bancos de Oriente Próximo tras vulnerar la seguridad de unas empresas de procesamiento de tarjetas de crédito y retirar dinero de cajeros automáticos en 27 países.

Fuente: A3 Noticias 11/05/2013.

http://www.antena3.com/noticias/mundo/mas-paises-afectados-ciberrobo-bancario-millones-dolares_2013051000063.html

Los conflictos en Siria y Egipto provocan un aumento de los ciberataques

La guerra civil en Siria y las pugnas políticas en Egipto han abierto nuevos campos de batalla en Internet y han provocado un alza de los ciberataques en Oriente Medio, según informó McAfee.

Fuente: Europapress 04/09/2013

http://www.europapress.es/portaltic/software/seguridad-00646/noticia-conflictos-siria-egipto-provocan-aumento-ciberataques-20130904155433.html

4.2 El Futuro de la Ciberdelincuencia

Tal y como se puede ver en las noticias publicadas a lo largo del año, y revisando distintos informes publicados junto con todo tipo de informaciones publicadas en la web, puede intuirse el camino que seguirán los cibercriminales este y los próximos años.[39]

- Las nuevas tendencias del Cibercrimen centrarán su atención, entre otros aspectos, en avanzar sus técnicas de desarrollo de malware para móviles y redes sociales. Tanto el sistema operativo Android como Facebook y Twitter deberán progresar mucho en sus sistemas de seguridad para no perder la confianza de sus usuarios.

- Los Smartphone y tablets se colocarán al mismo nivel que los ordenadores personales, en su papel de víctimas de robo de información.

- Se prevé también, un claro apunte hacia los servicios en la nube (Cloud) y sus infraestructuras, como importantes víctimas en potencia debido a la cantidad de información confidencial almacenada en sus sistemas.

- Apple y sus sistemas operativos móvil (IOS) y Mac OS X, abandonarán su cómoda posición y sufrirán una importante aparición de ataques y malware específico para sus plataformas.

- La privacidad digital y las autoridades digitales deberán continuar mejorando sus métodos de encriptación o caerán en la más absoluta obsolescencia.

[39] Tendencias de ciberdelincuencia para 2013 [Infografía] abril 17, 2013 by CristinaSanz

http://itercriminisblog.com/index.php/tendencias-ciberdelincuencia-2013/

- El hacktivismo junto con el poder de las bandas organizadas como Anonymous, continuarán su imparable avance y el campo político de la sociedad mundial podría verse seriamente afectado.

- Las vulnerabilidades y los exploits seguirán siendo los métodos más utilizados por los ciberdelincuentes.

Dando un enfoque más técnico a la visión de estas nuevas tendencias, el informe del primer trimestre de 2013 de la compañía de firmas antivirus Sophos, dejaba también los siguientes puntos a tener en cuenta sobre los siguientes pasos del Cibercrimen junto con una serie de recomendaciones:

• **Problemas básicos de servidores web**: Basándose en un aumento de los ataques por SQL Injection, los administradores deberán estar al día en cuanto a la revisión de vulnerabilidades y el estado de seguridad de sus sistemas para afrontar una tendencia creciente de ataques destinados al robo de credenciales para la extracción de información sensible.

• **Aumento del malware 'irreversible':** La aplicación de procedimientos de encriptado y mecanismos de control, ha aumentado considerablemente la capacidad de destrucción del malware. Serán imprescindibles sistemas de protección robustos así como herramientas de Backup disponibles ante desastres.

• **Nuevos Kits de herramientas** de desarrollo de ataques, con scripts y APIs de características mejoradas serán publicados y distribuidos haciendo que ser un ciberdelincuente sea cada día más sencillo.

• **Evolución de la Ingeniería social** y aplicación a nuevas plataformas: Pese a haberse conseguido grandes avances en la mitigación de exploits, esto no significará el final de los mismos. Sin embargo si se verá un decrecimiento en este método de explotar vulnerabilidades compensado por un agudo incremento en ataques de ingeniería social a lo largo de un amplio abanico de plataformas tales como móviles y aplicaciones en las redes sociales.

• Momento crítico en la **integración de nuevas tecnologías y la privacidad**. El hecho de la presencia de tecnología GPS y los nuevos avances de la conectividad de corto alcance NFC (Near Field Communication) cada vez mas integrados en las plataformas móviles, estrechará aún más la línea entre nuestra vida digital y física. Los ataques, empleando este tipo de información, pueden dar un giro muy peligroso al mundo de la ciberdelincuencia.

4.3 Principales fuentes del cibercrimen

Tal y como se ha podido comprobar en el capítulo anterior, son muchas las formas y métodos empleados por el Cibercrimen. A continuación, se muestran algunos datos obtenidos a partir de los diferentes informes publicados por algunas de las principales organizaciones dedicadas a la seguridad informática en el mundo.

En el informe "2013 Global Security Report", publicado por la empresa de seguridad Trustwave[40], la compañía hace una revisión sobre las vulnerabilidades, amenazas y ataques acontecidos en el año 2012, analizando, entre otros factores, la distribución geográfica de diferentes tipos de amenazas en su origen como en sus objetivos.

A lo largo de 2012, la división *Trustwave SpiderLabs*, revisó más de 450 casos de **violación da datos y robo de información** confidencial, localizando hasta 29 países como origen de estos delitos.

[40]Trustwave global security report 2013 https://www2.trustwave.com/2013GSR.html

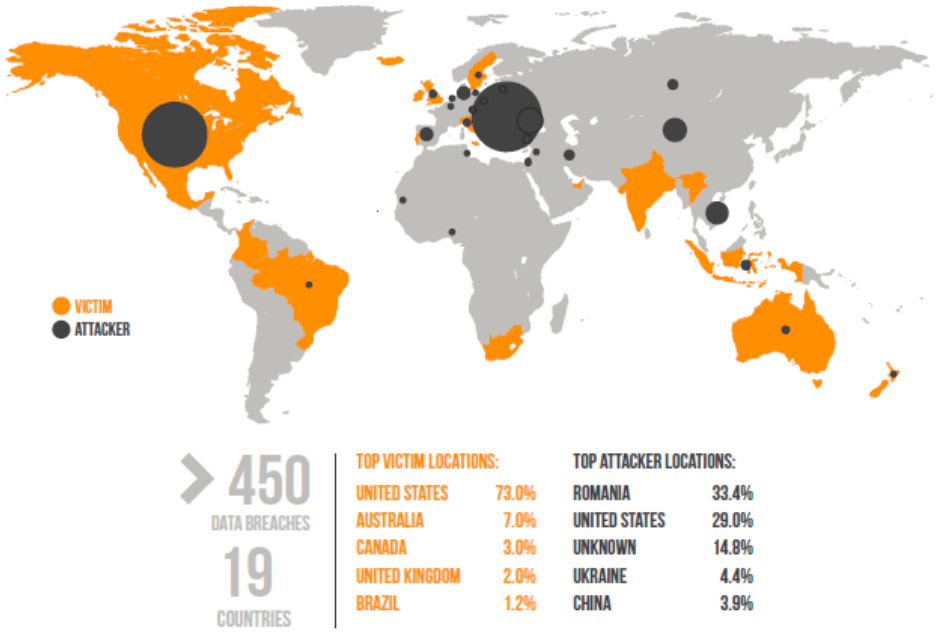

Fig. **34** Distribución mundial de delitos de robo de información en 2012.

Como se puede observar en la figura, Rumanía destacó por encima incluso de países como Estados Unidos, territorio que, sin embargo, fue con gran diferencia el mayor perjudicado en este tipo de delitos.

El país rumano, es considerado desde hace ya varios años como fuente de una gran actividad criminal, sobre todo en cuanto al Cibercrimen organizado, cuya actividad principal recae en el robo de información sobre tarjetas de crédito.

Pese a que resulta realmente complicado ubicar el origen real de un ataque informático, debido a las numerosas técnicas de enmascaramiento empleadas por los ciberdelincuentes, los cuales tienden a utilizar los recursos de naciones con gran representación de redes de banda ancha, el hecho de que este país se desmarque por encima de territorios con una extensión varias veces superior como son Estados Unidos o China, hace ver una realidad que puede llegar a ser bastante superior.

Un claro y curioso ejemplo de cómo la cultura del cibercrimen supone una forma de vida en los países del Este, es el caso de la ciudad conocida mundialmente como "**Hackerville**". Esta remota ciudad, perteneciente a Rumanía y cuyo nombre real es *Râmnicu Vâlcea*, donde

jóvenes de 20 y 30 años conducen todo tipo de vehículos de alta gama, es considerada por muchos como la capital mundial del Cibercrimen, más concretamente de las estafas por internet.

La revista "Wired", describía en uno de sus artículos publicados en 2011[41], como una ciudad donde apenas llegaba algún tipo de información y la población sobrevivía a duras penas, el boom de Internet y las estafas en la red habían convertido el lugar en una concentración de concesionarios de de las más prestigiosas marcas y establecimientos de artículos de lujo, donde al preguntar a uno de los lugareños el motivo de tanta riqueza este afirmó con total naturalidad: "roban dinero en Internet". De hecho, a pesar del empleo del término Hackerville, según describía el artículo, la mayoría de los ciberdelincuentes existentes en la zona no siguen en su metodología la descripción del término Hacker, sino que se dedican principalmente a perpetrar todo tipo de estafas, en su mayoría mediante anuncios de compraventa, a través de Internet. La rentabilidad de este y otros negocios ilegales en la red se había difundido de tal manera entre una población joven, con difíciles expectativas de futuro locales, que rápidamente se convirtió en una rápida y cada vez más habitual salida para obtener importantes ingresos sin necesidad de abandonar su ciudad.

Superando este inciso meramente anecdótico, y continuando con el informe de la compañía *Trustwave,* también fueron analizadas las principales fuentes de ataques de Red durante los 12 meses de 2012. Con más de 100 millones de registros de este tipo de ataques, considerando dentro de este concepto ataques del tipo SQL Injection, uso de Exploits, ataques por Fuerza Bruta y otros intentos de explotar servicios basados en protocolos de Red (FTP,RDP,etc), y teniendo en cuenta que, a pesar de que nuevamente resulta complicado localizar la ubicación exacta de las fuentes, aunque sí sea posible determinar con una certeza aceptable su ubicación general localizando el origen de los archivos maliciosos, podemos ver donde han sido originados este tipo de ataques e infecciones.

[41] How a remote town in Romania has become cybercrime central
http://www.wired.com/magazine/2011/01/ff_hackerville_romania/all/1

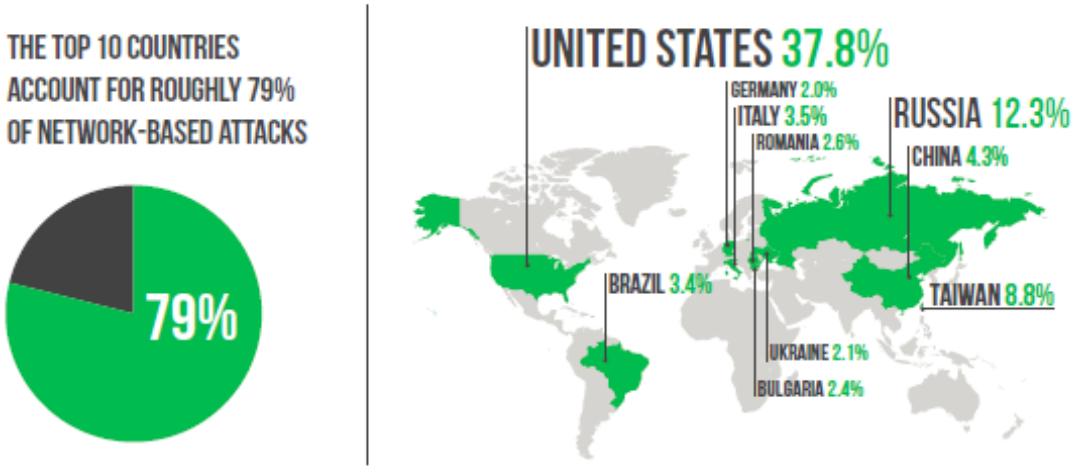

Fig. **35** Distribución mundial del origen de ataques basados en protocolos de red en 2012

Según el informe, siguiendo con la dinámica de años anteriores, y tal y como se puede observar en la figura, Estados Unidos y Rusia se sitúan notablemente por encima del resto de países, participando con un 37,8% y un 12,3% respectivamente como origen de estos ataques. Añadiendo además que ambos países suponen igualmente los mayores contribuyentes a la creación de software malicioso participando con un 39,4% de las creaciones de malware por parte de Estados Unidos y un 19,7% por parte de Rusia.

Cabe destacar, que mientras que los 10 países situados a la cabeza de la lista de ataques de Red suman un 79% del total, esta cifra pasa a elevarse a más del 90% si el dato observado es el origen de las infecciones malware.

Por otro lado, y dejando aparte dicho informe, en cuanto al origen del **Spam** en el mundo y pese a que ya se ha comentado en el correspondiente capítulo dedicado a este punto, se ha contrastado la información en este sentido con otro de los mayores proveedores de seguridad del mundo. La compañía Sophos, en su informe de 2013[42] publicado sobre el estado de las amenazas durante todo el año anterior, mostraba el siguiente gráfico, dividiendo en continentes la distribución del origen del Spam.

[42] Sophos Security Trheat Report 2013
http://www.sophos.com/en-us/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf

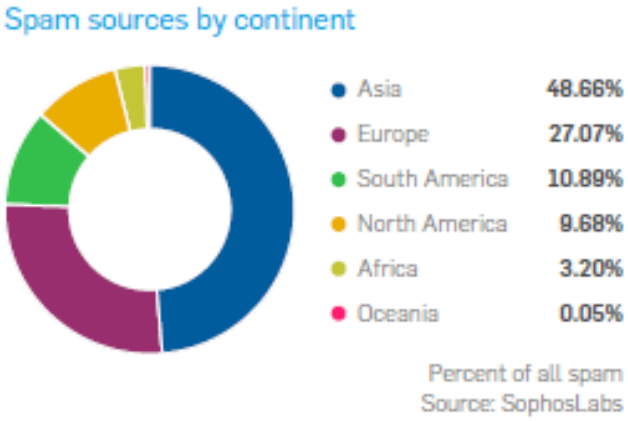

Fig. 36 Distribución de Spam originado por continente según SophosLabs.

Este dato, mantiene numerosas similitudes con el ofrecido también en este mismo año por la compañía Kaspersky, por lo que da la sensación de acercarse en gran medida a la realidad.

Los motivos por los que un atacante puede elegir una u otra ubicación geográfica para emprender un ataque de red, o utilizarlo como fuente de una infección de malware o envío de Spam, dependen de varios factores:

Disponibilidad: El número de equipos comprometidos así como la posibilidad de encontrar servicios de hosting y housing (alojamiento de servidores) de bajo precio, son casualmente más sencillos de encontrar en los países con mayor índice de infecciones malware.

Controles de Acceso: Los sistemas de seguridad son cada vez mayores y los administradores implementan bloqueos contra rangos de IPs geográficamente situadas en países considerados peligrosos. Para superar estas barreras, los ciberdelincuentes están variando sus localizaciones origen.

El cercanía al objetivo: La mayoría de los servicios web, son proporcionados desde un número relativamente reducido de países. Con motivo de eludir las sospechas por la localización de la fuente, los atacantes suelen emplear como origen los propios países a los que pertenece el servicio.

Legislación: Inevitablemente, la legislación de un país, como pueden ser sus normas de extradición (o la ausencia de esta) y el modo de aplicación de las leyes, participa directamente en la elección por parte de los ciberdelincuentes del origen de sus ataques.

Capítulo 5. **Persecución tecnológica**

Una vez realizado un repaso por diferentes aspectos del Cibercrimen y la Ciberdelincuencia, el objetivo de este capítulo se centrará en analizar algunos de los diferentes medios y métodos de lucha, así como también se realizará una revisión de los múltiples sistemas de mitigación y prevención aplicables de cara a implementar soluciones de seguridad tanto en el ámbito teórico como práctico.

5.1 Sistemas de seguridad perimetral

A pesar de las políticas de prevención y concienciación sobre el uso seguro de las TIC, la gran mayoría de usuarios normalmente pasa por alto estas recomendaciones, de hecho según la compañía Cisco, este porcentaje asciende al 70% de los usuarios de una red[43]. Esta falta de celo, sumada a la evolución constante de las amenazas, conlleva a que tanto las organizaciones como los usuarios necesiten de una serie de herramientas que les ayuden a proteger sus sistemas y a solventar sus problemas de seguridad.

De cara a la protección de los sistemas de red y las infraestructuras de comunicaciones e información, el mercado ofrece una serie de soluciones específicas con el fin de luchar contra la Ciberdelincuencia en todas sus variantes, pasando desde soluciones domésticas que cumplen las necesidades del usuario común, a soluciones de mayor complejidad y dedicación, orientadas a los problemas localizados más comúnmente en redes de mayor tamaño pertenecientes a empresas o instituciones tanto públicas como privadas.

El objetivo de los sistemas de seguridad perimetral reside en establecer los medios de protección necesarios para asegurar la disponibilidad, la integridad y la confidencialidad de los sistemas de información y las infraestructuras lógicas de una red.

[43] Cisco Security Applied Intelligence for a Risky World

http://www.cisco.com/en/US/solutions/collateral/ns1015/ns1238/info_graphics_c82-727889.pdf

Pese a que prácticamente la totalidad de ellas se encuentran disponibles en forma de Software distribuible, la mejor solución suele pasar por la implantación en la red de equipos o servidores dedicados, comúnmente denominados con el término inglés *Appliance*, los cuales necesitarán de la pertinente gestión y configuración específica y periódica por parte del administrador/es de Red o Seguridad.

A continuación se detallaran algunas de las principales soluciones de Seguridad Perimetral existentes hoy en día en la industria de la seguridad en las telecomunicaciones.

5.1.1. **Sistemas Antimalware**

Conocidos comúnmente como "Antivirus", utilizando de manera imprecisa la definición del término virus para referirse a cualquier tipo de malware existente, el funcionamiento de un sistema antimalware se basa en analizar la confiabilidad de los diferentes ficheros, procesos e instrucciones presentes en el sistema en el que se encuentra instalado, utilizando para ello un motor de análisis que realiza su inspección comparándolos con una o varias bases de datos de reputación volcadas en el sistema, conocidas con el nombre de "*bases de datos de firma*s".

Dichas bases de datos no sólo contienen largas listas de definiciones de variantes de malware, sino que también ofrecen la posibilidad de identificar una posible amenaza aun no registrada, basándose en los patrones de ejecución y compilación de código de un archivo. Este sistema de prevención avanzada se conoce como *detección heurística*.

Una vez identificada una amenaza, el sistema ofrece las opciones, en base a unos niveles de riesgo y precisión, de notificar, eliminar o redirigir a un entorno de cuarentena el posible archivo infectado con código malicioso.

Sin embargo, como toda solución de seguridad, su eficacia no es ni mucho menos del 100%, sino que dado el increíble dinamismo de la evolución del malware, la eficacia de un sistema antimalware será directamente proporcional a la constante actualización de sus bases de datos. Siendo necesario encontrarse de manera permanente en la última versión publicada

por el fabricante con el objetivo de alcanzar los mayores niveles de efectividad y falsas detecciones positivas.

Al igual que ocurriera con la definición de malware, existen diferentes productos disponibles en el mercado, siendo posible encontrarlos de manera independiente o como una solución conjunta, tales como antivirus, antispyware, antiadware, etc.

Dentro de los sistemas Antimalware podemos encontrar dos variantes de despliegue, enfocadas cada una de ellas a diferentes sectores. La primera de ellas estaría compuesta únicamente de la instalación de un software cliente, el cual ejecutará de manera local, en la máquina instalada, los procesos de protección configurados por el usuario o predefinidos por el fabricante. Esta solución se encuentra principalmente orientada a usuarios domésticos y pequeñas empresas, con una infraestructura reducida.

La segunda de las opciones de despliegue disponible, sería a través de la instalación de un sistema cliente-servidor, o sistema centralizado. En dicho sistema, la mayor parte de la configuración de la política de seguridad definida se encontrará en un servidor dedicado a tal fin, el cual previo establecimiento de la comunicación a través de un puerto pre-configurado con los equipos de usuario, gestionará de manera distribuida el conjunto de equipos cliente registrados en su Base de Datos, desplegando las nuevas políticas de seguridad y distribuyendo las nuevas bases de datos de firmas a través de la red local.

Para poder realizar dicha gestión, será necesaria la instalación de una versión más ligera del software, orientada a equipos cliente. Esta versión cliente, normalmente podrá ser instalada y administrada de igual modo que un software antimalware tradicional, o por el contrario, instalada de manera distribuida a varios equipos simultáneamente a través del despliegue de paquetes de instalación en red, pudiendo el administrador incluso configurar la opción de *auto instalación silenciosa*, la cual ni siquiera requeriría la interacción del usuario, con la consecuente agilización del proceso.

Esta opción sería la elegida en la mayoría de los casos por medianas y grandes empresas, donde las tareas de administración de la TI (Tecnologías de Información) corporativas, requieren la necesidad de economizar esfuerzos debido al elevado número de dispositivos participantes en la red.

Si bien los sistemas antimalware suponen el elemento más económico dentro de las soluciones de seguridad planteadas habitualmente, su presencia se considera indispensable en todos los entornos donde los sistemas de información tengan cualquier tipo de contacto con el exterior, ya sea a través de Internet, correo electrónico o incluso soportes de almacenamiento portable USB o tarjetas de memoria.

5.1.2. **Sistemas de Control de Acceso**

Los sistemas de control de acceso, dotan al resto de sistemas de seguridad perimetral de la posibilidad de establecer agrupaciones y diferenciaciones entre unos u otros usuarios, además de proporcionar los valores de identificación necesarios para conceder o denegar el acceso a los servicios corporativos.

La existencia de diferentes protocolos, tanto estándar como propietarios de algunos fabricantes, destinados a unos u otros propósitos de validación en el ámbito de las infraestructuras de red, ofrece numerosas posibilidades a la hora de diseñar las políticas de seguridad y de utilización de recursos.

Algunos de los más populares de estos protocolos son RADIUS (Orientado a aplicaciones de acceso a la red o movilidad IP), TACACS (protocolo propietario de Cisco, orientado a la validación de acceso a equipos de red) y LDAP (orientado a la validación de usuarios en el uso de recursos compartidos).

5.1.3. **Sistemas Firewall**

Si anteriormente se mencionaba la necesidad imperativa de disponer de algún tipo de sistema antimalware presente en cualquier infraestructura de seguridad de red, la presencia de un sistema cortafuegos se situaría al mismo nivel, o superior, que esta última.

Aunque es posible encontrar numerosas soluciones software de cortafuegos personales, enfocadas en su mayoría al uso doméstico, dado que el funcionamiento de las

soluciones dedicadas abarca un abanico más amplio de funcionalidades se centrará el análisis en este sentido.

Los sistemas Firewall (del inglés, **cortafuegos**), establecen la primera barrera lógica en la comunicación de una red local con Internet. Su funcionamiento básico se basa en el control de las comunicaciones, tanto de salida como de entrada, a una infraestructura de red, así como el control de estas entre las diferentes zonas de seguridad definidas, realizando un análisis del tráfico en diferentes capas según sea la política y tipo de cortafuegos empleado.

Pese a que pueden ser identificadas un gran número de zonas de seguridad, existen al menos 3, cuya utilización se muestra presente en la gran mayoría de los casos.

- **LAN:** Siglas de la definición en inglés Local Area Network (Zona de Area Local), se utiliza para hacer referencia a una o varias zonas internas o confiables de la red. En esta zona se ubican los recursos internos de la red, tales como repositorios de información, servidores internos y equipos de usuario, siendo todos ellos la parte más vulnerable y cuyo acceso desde el resto de zonas requiere mayor control.

- **WAN:** Siglas de la definición Wide Area Network (Red de Área Extensa), utilizadas para definir al conjunto de redes externas o no confiables y cuyo control de accesos hacia el interior de la red local ha de ser más exhaustivo. Esta zona se utiliza comúnmente también, para localizar al tráfico proveniente de la mayor de las redes no confiables, Internet.

- **DMZ:** En español, zona desmilitarizada (Demilitarized Zone). Dicha zona se utiliza para ubicar aquellos elementos de la red que se encuentran constantemente expuestos al exterior, como puedan ser servidores de correo electrónico, frontales web o servidores de resolución de nombres (DNS). El objetivo de esta zona suele ser el de permitir el acceso a ella tanto desde el exterior (WAN) como desde el interior (LAN), denegando sin embargo el acceso desde esta hacia la red local. De este modo, se consigue aislar estos recursos públicos cuya seguridad puede llegar a quedar comprometida, del resto de elementos de la red interna.

La siguiente figura muestra un ejemplo de implantación lógica en un diagrama de red. Esta misma imagen será empleada en apartados posteriores para ofrecer una visión completa de la implantación de diferentes dispositivos de seguridad en una misma infraestructura lógica.

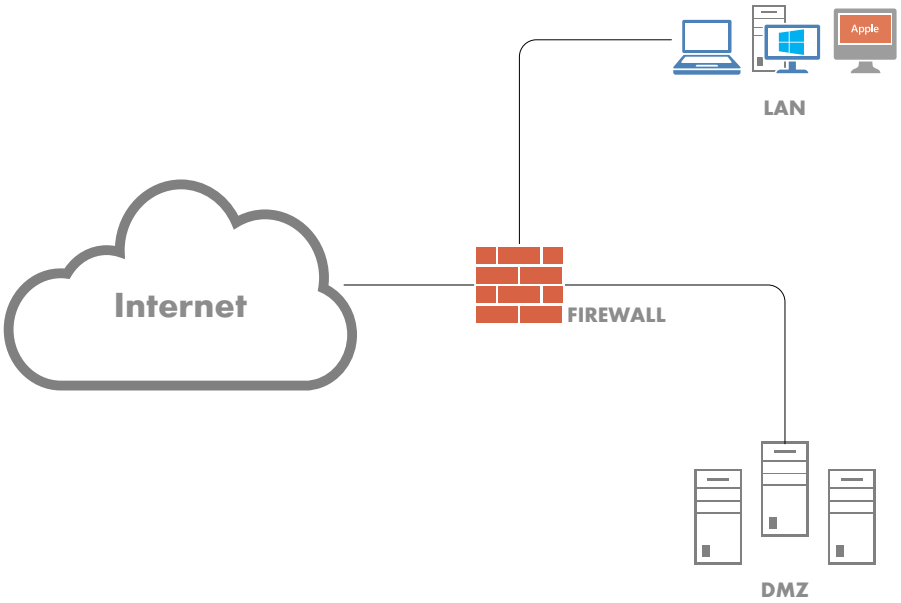

Fig. 37 Ubicación de un sistema Firewall en el diagrama de una red

Desde su aparición hasta hoy, pese a que los dispositivos o sistemas firewall han ido evolucionando en gran medida, integrando diferentes mejoras y funcionalidades, además de crecer junto con la constante evolución capacitiva de todos los sistemas informáticos, en lo que a recursos hardware se refiere, es posible diferenciar entre principalmente dos tipos de firewall según su funcionamiento.

El primero de ellos sería, los firewall de filtrado de paquetes, también conocidos como firewall de red o de ***nivel 3***, haciendo referencia dicho nivel a la tercera capa, de la pila de protocolos del modelo de Interconexión de sistemas abiertos (OSI)[44]. Estos equipos realizan un análisis de los paquetes recibidos a través de cada una de sus interfaces, recogiendo la

[44] Definición de las siete capas del modelo OSI http://support.microsoft.com/kb/103884/es

información contenida en sus cabeceras referente a direcciones IP y puerto, origen y destino. Una vez toda esa información se encuentra disponible, el cortafuegos puede contrastarla con los parámetros definidos en su política de seguridad, y permitir o bloquear el establecimiento de una conexión o simplemente el tráfico de red entre las diferentes zonas de seguridad definidas.

Dichas políticas, se dividen en reglas de acceso, organizadas con un orden de secuencia numerado, las cuales serán procesadas en orden descendente visualmente, y donde será necesaria la coincidencia, de los valores obtenidos de un paquete, con todos los parámetros especificados en de dicha regla para definir la acción de bloqueo o autorización programada.

Cada una de las reglas de filtrado deberá especificar, por tanto, una parte o la totalidad de los siguientes elementos:

- Zona de red o Interfaz origen
- Zona de red o Interfaz destino
- Dirección IP o dirección de red origen
- Dirección IP o dirección de red destino
- Puerto o servicio destino
- Tipo de protocolo (TCP, UDP, o ICMP)
- Acción

Seq.#	Source	Destination	Service	Action
wan1 -> internal (6)				
33	IP_193.145.230.6	IP_193.144.101.191	HTTP TCP_1521 TCP_8080	✓ ACCEPT
34	host_86.109.111.91	IP_193.144.101.132 IP_193.144.101.134 IP_193.144.101.136	ANY	✓ ACCEPT
35	all	all	ANY	⊘ DENY

Fig. 38 Reglas de acceso de una política de firewall

Este tipo de cortafuegos, no necesitan de gran capacidad de recursos y su funcionamiento es prácticamente transparente para los usuarios en cuanto tiempo de retardo introducido en el flujo de la transferencia de datos.

En segundo lugar, se encuentran los firewall de nueva generación o firewalls de aplicación. Con un nivel de granularidad mucho mayor en cuanto las posibilidades ofrecidas, de cara a la definición de las políticas de seguridad. Estos equipos son definidos de dicho modo por ser capaces de gestionar la información contenida en un paquete dentro la séptima y última capa de la pila de protocolos del modelo OSI, la capa de aplicación.

Fig. 39 Pila de protocolos del modelo OSI

Ofreciendo también las funcionalidades disponibles en un firewall de filtrado de paquetes, añaden la posibilidad de controlar el flujo de datos perteneciente a ciertas aplicaciones y protocolos como pueden ser la navegación web, la transferencia de ficheros (FTP) o el tráfico DNS, que discurre a través de ellos. Pudiendo evaluar la correcta asociación entre dichos protocolos, la utilización de puertos estandarizados o el uso no autorizado o inseguro de alguno de ellos.

Permiten además la integración con diferentes sistemas de control de acceso, de modo que es posible definir diferentes niveles de permisividad, en cualquiera de las políticas definidas, según sea el usuario o grupo de usuarios que se encuentran detrás de una conexión.

5.1.4. **Sistemas antispam**

Los sistemas de filtrado antispam, tal y como su nombre indica, ofrecen diferentes funcionalidades, mediante las cuales reducir y controlar la recepción de correo electrónico no deseado, por parte de los usuarios finales.

Al igual que ocurre con las soluciones firewall, en el caso de los sistemas antispam es posible encontrar diferentes soluciones, según sea el entorno donde estas van a ser aplicadas. En el caso de entornos domésticos, la solución mayoritaria consiste en la utilización de software diseñado para trabajar exclusivamente en un equipo cliente. Mientras que en entornos corporativos, esta solución pasa por la implementación de sistemas dedicados, orientados a analizar todo el volumen de entrada a un servidor de correo electrónico.

En la primera de las opciones, el software de filtrado se integra con el cliente de correo del usuario, ya sea a través de una aplicación web, o de un software instalado en el PC de este. El sistema analiza el correo a la entrada en el sistema evaluando, según diferentes criterios, las posibilidades de que este sea legítimo o no deseado. En este último caso el mecanismo de filtrado tiene la opción de bloquear y rechazar el correo automáticamente, o bien pasarlo a un estado de cuarentena, donde será eliminado si no es liberado tras un periodo de tiempo.

Para analizar la segunda opción, es necesario, en primer lugar, conocer el funcionamiento a grandes rasgos de un sistema corporativo de correo electrónico. En este caso, a diferencia de lo que ocurre en los servicios de correo de públicos ofrecidos por grandes empresas, donde millones de usuarios llegan a compartir los mismos servidores de correo electrónico, en los entornos privados, las compañías disponen de sus propios dominios de correo, administrados por servidores dedicados e implementados en su propia infraestructura de red. Empleando la nomenclatura utilizada en el campo de los dominios de Internet, estos servidores ejercerían el papel de los llamados servidores MX (Mail eXchange record, en español "registro de intercambio de correo"), siendo estos quienes recibirían el correo electrónico de la compañía y quienes lo distribuirían a los usuarios.

Los sistemas antispam, aparecen en estos entornos ocupando la posición pública de los servidores de correo, de modo que resulten ser un intermediario entre estos e Internet. Dicho de otro modo, en la instalación de un servidor antispam, este será definido como

servidor MX de un dominio, recibiendo todo el volumen de correo, procesándolo y reenviando aquellos mails que hayan superado el filtrado al servidor real.

El siguiente diagrama de red, muestra un ejemplo de arquitectura donde ha sido implementado un servidor antispam. Como se ve en la figura, el sistema antispam se sitúa por detrás de la posición del firewall, recogiendo el tráfico permitido por este y devolviéndolo una vez analizado.

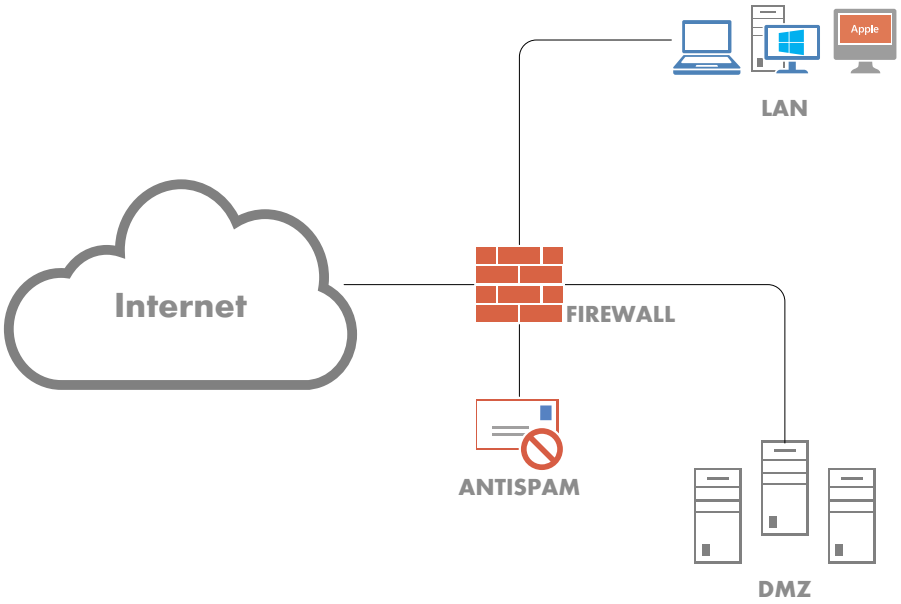

Fig. 40 Ubicación de un sistema antispam en un diagrama de red

Existen diferentes mecanismos a través de los cuales un sistema de filtrado de correo electrónico evalúa los emails procesados:

Filtrado por contenido: en este sentido, los motores de análisis de pueden inspeccionar tanto el contenido en texto de un correo electrónico, como el de los archivos adjuntos a este.

Empleando el análisis del contenido en texto, el sistema trata de localizar palabras clave como pueden ser “sex” o “viagra” o enlaces a páginas consideradas maliciosas, todo ello

a partir de diferentes bases de datos de reputación cuyo contenido es actualizado periódicamente.

En el análisis de archivos adjuntos, ya sean documentos en diferentes formatos, archivos comprimidos o imágenes, el sistema trata de localizar patrones de código de virus y otros tipos de malware, pudiendo también detectar, a partir de la suma de ambos análisis casos de estafas y phishing.

Filtrado por origen: En el filtrado por origen o reputación, el sistema analiza las cabeceras del correo electrónico, de cara a obtener la dirección IP, el dominio del remitente e incluso su ubicación geográfica. Esta información es contrastada con las denominadas listas de reputación, a partir de las cuales el sistema puede conocer la calificación asignada al remitente.

Un determinado dominio o dirección IP, puede pertenecer, según sea su reputación, a una lista negra, si el sistema de firmas global o local le considera como reconocido spammer, una lista gris, si su reputación está en entredicho, o una lista blanca si el administrador ha decidido excluirle del análisis y confiar de manera inequívoca en él.

Ambos sistemas de filtrado, no sólo pueden funcionar de manera automática si no que pueden ser empleados por el administrador del sistema para configurar la política de seguridad del equipo. Pudiendo, por ejemplo, bloquear el envío o recepción de correos que, aun siendo confiables, tengan como origen, o no, determinados dominios o bloquear aquellos correos que contengan un determinado tipo de archivo adjunto, sin necesidad de proceder con su análisis.

Una vez un correo ha sido evaluado según cada uno de los filtros definidos por el administrador, este recibirá una puntuación final, la cual será quien que defina la reputación del mismo y por tanto su consideración como deseado, sospechoso, o no deseado.

Adicionalmente, y como herramienta de protección de la información, los sistemas antispam más recientes disponen de técnicas adicionales de control de contenido, empleadas generalmente en el envío de correos procedentes de de la propia organización. Una de estas técnicas, la cual es empleada no sólo en sistemas antispam sino también en sistemas de control de aplicaciones web, es la denominada **Data Leak Prevention (DLP),** que en español sería prevención de fuga de datos.

A través de las técnicas de DLP, los sistemas pueden prevenir el envío de información considerada confidencial o personal, por parte de los usuarios, los cuales de manera negligente deciden enviarla a través de medios no seguros como puede ser un correo electrónico o un sistema de mensajería instantánea.

Las herramientas de DLP, disponen de patrones y mecanismos para reconocer cadenas de texto, como puede ser números de tarjetas de crédito, números de DNI, etc.

5.1.5. **Sistemas IDS**

De las siglas en inglés *Intrusion Detection System* (Sistemas de detección de intrusiones), los sistemas IDS, presentes en el mercado tanto como soluciones software como en forma de servidores dedicados o módulos adicionales a elementos de red como routers o firewalls, suponen un paso más en cuanto al uso de herramientas de seguridad para la detección de amenazas de red.

El funcionamiento de los sistemas IDS se basa en el análisis de un determinado tráfico de red, con el objetivo de detectar y reportar posibles amenazas o actividades no controladas provenientes del exterior de un sistema. La metodología que estos sistemas pueden emplear para su funcionamiento puede dividirse en:

- ***Host-Based*:** donde el análisis del tráfico y la búsqueda de actividad maliciosa se realiza sobre la información obtenida de un único host.
- ***Network-Based:*** el sistema se sitúa en un determinado segmento de la red, generalmente al mismo nivel que el sistema firewall, y analiza todo el conjunto del tráfico que atraviesa dicho segmento.
- ***Knowledge-Based:*** la interpretación que el sistema realiza del tráfico se ejecuta empleando el conocimiento almacenado en Bases de Datos compartidas y distribuidas en forma de patrones de firmas, de forma similar a la empleada por los sistemas antimalware.
- ***Behavior-Based:*** *el sistema analiza el tráfico buscando la coincidencia con los patrones de comportamiento habituales en cada tipo de comunicación y observando aquellas posibles variaciones que puedan suceder.*

La autonomía con que funcionan habitualmente estos sistemas y el escaso mantenimiento necesario una vez realizado el despliegue inicial, les convierten en una potente y útil herramienta capaz de proporcionar información de gran relevancia, al responsable de seguridad de una red, tal como la dirección IP origen de un ataque o el momento exacto en que se ha registrado.

Un sistema IDS, captura, procesa y es capaz de responder ante ciertas amenazas detectadas con la particularidad de que para ello trabaja empleando una copia del tráfico analizado, el cual evalúa a partir del uso de firmas, en vez de trabajar sobre el flujo real. Este método de funcionamiento se conoce como "*promiscuo*" y ofrece la ventaja que no afecta en absoluto a la latencia del flujo de datos.

Sin embargo, las desventajas de esta forma de funcionamiento suponen que, por un lado para posibilitar el análisis del tráfico, sea necesaria la incursión de al menos una parte de este en la red, y por otro que, el hecho de trabajar con una copia, impida la detención de numerosas intrusiones de manera autónoma, requiriendo en la mayoría de ocasiones de la utilización de otros dispositivos de red como router o firewalls para controlar una intrusión.

La siguiente imagen muestra la ubicación en un diagrama de red que ocuparía este sistema.

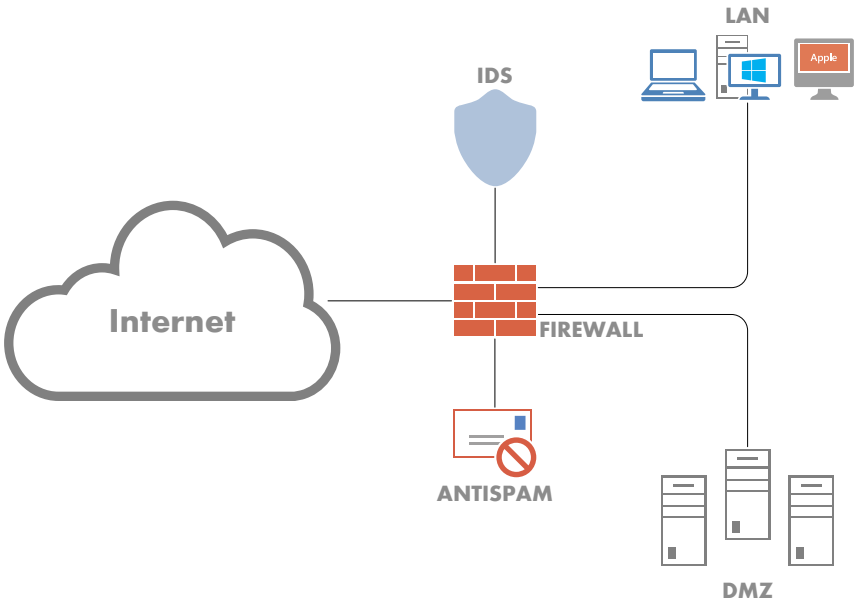

Fig. 41 Ubicación de un sistema IDS en un diagrama de red

5.1.6. **Sistemas IPS**

Mientras que los sistemas IDS emplean una réplica del tráfico analizado, los sistemas de Prevención de Intrusiones (en inglés Intrusion Prevention System), trabajan en línea (inline) sobre el flujo real de datos. Este hecho acarrea como consecuencia directa un ligero retardo en las comunicaciones inversamente proporcional a la capacidad de procesado del sistema.

Al igual que los anteriores, es posible encontrarlos tanto en soluciones software como en forma de módulos adicionales a elementos de control de red o servidores dedicados.

Sin embargo, a diferencia de estos, los sistemas IPS no permiten la entrada del tráfico intrusivo en la red, sino que realizan la supervisión de los paquetes recibidos mediante diferentes sensores y monitores desde la capa 2 a la 7 del modelo OSI. Esto permite un análisis más exhaustivo, y por tanto un mayor nivel de precisión a la hora de categorizar la naturaleza del flujo de datos registrado.

Por otro lado, mientras que un IDS funciona, en la mayoría de las circunstancias como un elemento pasivo, cuya finalidad es la detección y notificación de las intrusiones detectadas, el objetivo principal de los sistemas IPS, atiende más a un comportamiento reactivo, detectando y actuando de manera inmediata, mediante una serie de mecanismos totalmente autónomos que permiten ejecutar una respuesta activa con el fin de mitigar la amenaza y generando una alerta únicamente cuando esto sea explícitamente definido.

La siguiente figura muestra la ubicación de un sistema IPS en un diagrama de red.

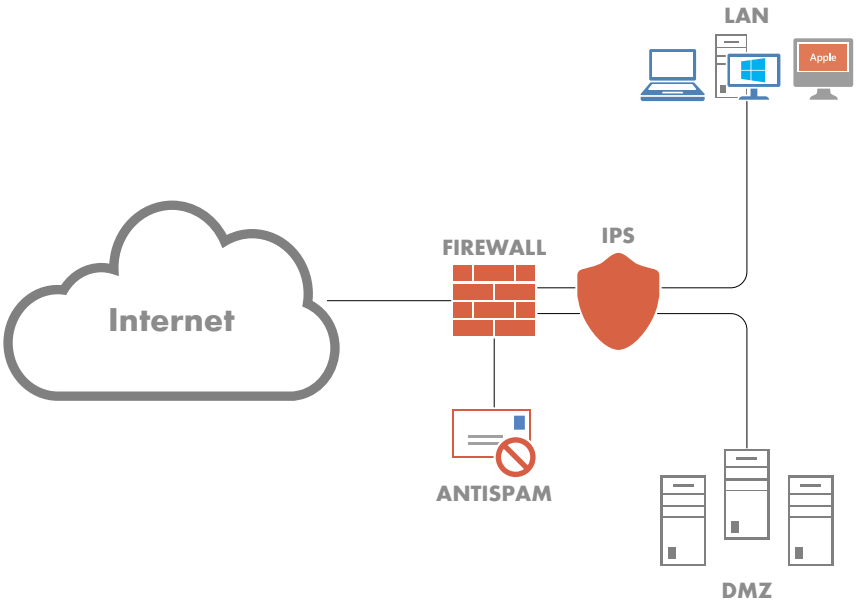

Fig. 42 Ubicación de un sistema IPS en un diagrama de red

Al igual que los sistemas firewall, tanto IDS como IPS, permiten la implementación de políticas personalizadas de seguridad, en este caso con el fin de corregir comportamientos predefinidos por el sistema tales como falsos positivos o a bloquear tráfico directamente no deseado. Sin embargo, a diferencia de estos, ambos sistemas anti intrusiones disponen de mecanismos de auto aprendizaje que les dotan de una capacidad muy superior de reconocimiento de alertas.

Uno de estos métodos de auto aprendizaje consiste en el empleo de los llamados sistemas ***Honeypot*** (del inglés tarro de miel). Este método consiste en la presentación de un servidor, físico o virtual, cuyo servicio o características atraigan la atención del posible atacante, desviando las acciones de este de los elementos reales de la red. El atacante emplea sus recursos contra el sistema Honeypot, desvelando a los sistemas de detección los métodos empleados e incluso permitiendo su identificación. De esta manera, gracias a la información recogida, es posible elaborar patrones de comportamiento y de ejecución de código malicioso que permiten optimizar la política de detección de intrusiones.

5.1.7. **Sistemas proxy**

Partiendo del hecho del funcionamiento de Internet basado en el modelo Cliente-Servidor, concretamente en el caso de la navegación web, esto sucede de modo que un usuario (cliente) realiza una o varias peticiones de ficheros de contenido a un servidor, el cual, a partir de los datos obtenidos a de dicha petición, entre otros versión del sistema operativo, navegador y sobre todo dirección IP origen, devuelve una respuesta al equipo cliente con la información solicitada.

De este modo, un usuario que se encuentra navegando de manera convencional por la web, se muestra constantemente compartiendo información explicita de su sistema y, como consecuencia, exponiéndose directamente a todo tipo de amenazas.

Los sistemas web proxy (en español, intermediario), actúan como una entidad intermedia entre el equipo cliente y el servidor web al que este desea acceder, de modo que cuando un usuario realiza un intento de conexión, es el sistema proxy quien envía su propia información al servidor web, recogiendo la respuesta emitida por este y almacenándola en memoria, para posteriormente reenviarla al equipo cliente. Con ello, además de obtener una velocidad de navegación superior, dado que el contenido web se encuentra almacenado en el propio sistema proxy como si del servidor web se tratara, se consigue haber dejado en un segundo plano al equipo cliente, dejando su información privada oculta al exterior. Este tipo de diseño de funcionamiento es conocido con la denominación de "**proxy directo***".*

Un sistema web proxy, puede actuar interviniendo en el proceso de navegación del usuario, con el fin de disminuir los riesgos a los que este se expone en la Red, utilizando diferentes métodos tanto de manera conjunta como aislada.

NAT: Siglas en inglés del método *Network Address Translation* (Traducción de Dirección de Red) para referirse al sistema empleado por diferentes dispositivos de red para enmascarar o modificar la dirección origen o destino de un paquete TCP/IP.

En este caso, los servidores web proxy modifican la dirección IP origen de de uno o varios equipos cliente, sustituyéndola por su propia dirección IP, de modo que un servidor remoto sea incapaz de identifica el origen real de la conexión.

En ocasiones, algunos sistemas proxy no emplean este método, participando en la navegación únicamente de manera pasiva, estos sistemas son conocidos como sistemas proxy transparentes.

Filtrado de Navegación: Debido a la capacidad de analizar los paquetes de datos, no sólo a nivel 3(Nivel de Red) sino también en las capas superiores, incluida la de aplicación, los sistemas proxy pueden evaluar y en consecuencia permitir o denegar, a través de la política de seguridad expresamente definida por el administrador, según sus criterios de confiabilidad, la navegación de un usuario hacia determinados sitios web en base a diferentes variables.

***Filtrado por Contenido**:* Utilizando bases de datos dinámicas, el sistema categoriza cada uno de los sitios web accesibles según su contenido principal. De este modo, es posible controlar el acceso de los usuarios a sitios como webs pornográficas, redes sociales, paginas de juegos online, de contactos, etc.

La siguiente captura muestras las categorías más comúnmente usadas por los sistemas de filtrado por contenido.

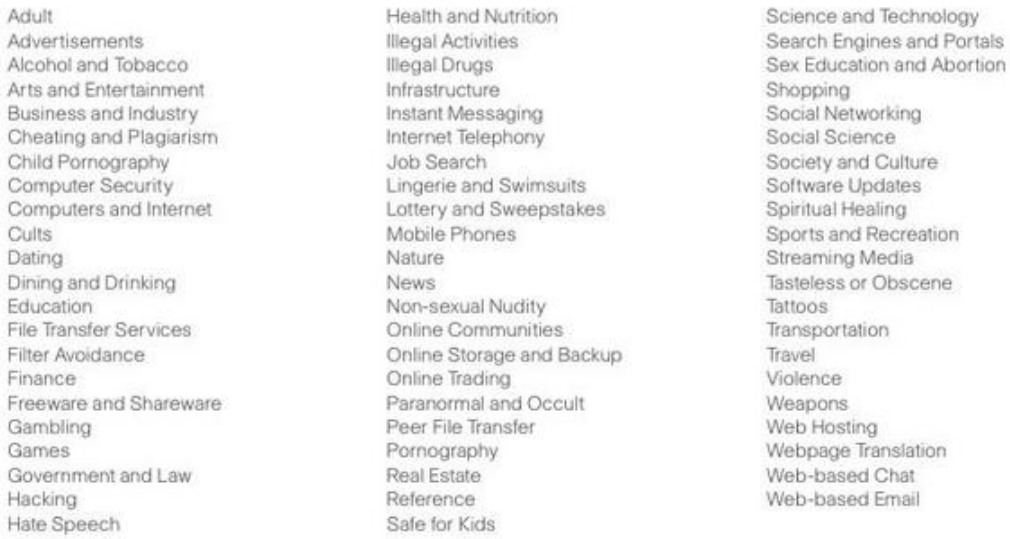

Fig. 43 Listado de las 65 categorías de filtrado web más utilizadas

Filtrado por URL: A diferencia del caso anterior, este método analiza la cadena de caracteres contenida en la dirección URL (siglas en inglés de *Uniform Resource Locator)* escrita en el navegador para acceder a un determinado sitio web, pudiendo bloquear o permitir el acceso a determinados sitios cuya dirección web contengan una cadena o expresión de caracteres concreta, como pudiera ser "xxx" (habitualmente contenida en webs de pornografía).

Filtrado antimalware: Además de los sistemas de protección anteriores, los sistemas proxy más recientes disponen también de sistemas de detección basados en firmas, del mismo modo que los tradicionales sistemas antimalware, contra diferentes formas de malware, como adware o spyware presentes en numerosos sitios web, y en cuyo caso como identificación de forma positiva el acceso al sitio puede ser igualmente bloqueado.

Filtrado de contenido: Orientado principalmente a prevenir la descarga de ficheros potencialmente maliciosos, como por ejemplo paquetes autoinstalables, este sistema emplea el reconocimiento de los tipos más comunes de archivos utilizando su información descriptiva, de modo que permite el bloqueo, o autorización si así se indica, de la transferencia de determinados archivos según sea la naturaleza de estos.

Por otro lado, basándose en un concepto similar pero en sentido contrario, es decir estableciendo el sistema proxy como intermediario entre el servidor e Internet, pero igualmente como gestor de contenido a través del almacenamiento caché, se encuentran los llamados sistemas *reverse proxy* o **proxy inverso.** Dichos sistemas, establecen una barrera de seguridad frente a uno o varios servidores web, mostrándose como objeto destino de la comunicación y sirviendo directamente al usuario el contenido solicitado, el cual previamente ha sido solicitado al servidor real y almacenado en memoria.

Todo esto lleva a considerar a los sistemas proxy como una importante medida de seguridad contra las amenazas existentes en la navegación web.

El siguiente esquema muestra la ubicación de un sistema proxy directo en el diagrama de red empleado como ejemplo.

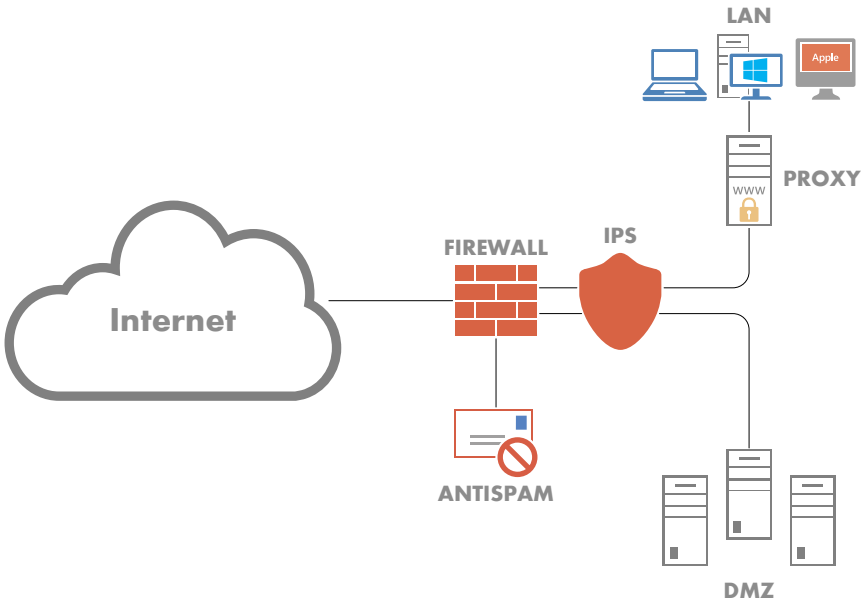

Fig. 44 Ubicación de un sistema Proxy en un diagrama de red

5.1.8. **Sistemas Balanceadores de carga**

Pese a que el principal objetivo de un sistema balanceador de carga reside en la ejecución de algoritmos de distribución de la carga, diseñados para distribuir de manera eficiente el número de peticiones enviadas a dos o más servidores web o ftp, que funcionan de forma conjunta para ofrecer un mismo servicio, la implantación de estos sistemas en el diagrama de red supone además una forma de protección física empleada para la mitigación de ataques realizados contra servidores Web.

Un sistema de de balanceo de carga o de servicios se sitúa en la infraestructura de red de manera que desarrolle el papel de intermediario entre Internet y el servidor final que atenderá la petición. El funcionamiento de este sistema, básicamente se desarrolla de forma que cuando un usuario realice un intento de acceso a un determinado servicio, a través de la dirección IP o URL con que este se encuentra publicado en la red, esta petición se realice contra el propio sistema balanceador, el cual redistribuirá la sesión a uno de los servidores disponibles.

El sistema balanceador dispondrá para ello de un sistema de configuración en el que se definan una serie de elementos denominados "*virtual server*", para aludir a la relación entre dirección *IP:Puerto* públicos de un servicio y una serie de nodos con direccionamiento privado los cuales harán referencia a cada uno de los servidores web redundados.

Multiplicando de este modo el número de peticiones que puede atender un mismo servicio de manera simultánea, y lo que es más importante en nuestro caso, su capacidad de procesamiento ante un posible ataque de Denegación de Servicio por conexiones simultáneas, debido a las posibilidades ofrecidas por los diferentes algoritmos de distribución, los cuales pueden ser empleados para impedir la sobrecarga de un sistema final a través de monitores de recursos disponibles, o redirigir todas las peticiones basadas en un mismo patrón a un mismo sistema, liberando la carga del resto , de modo que estos puedan seguir ofreciendo servicio sin que la calidad de este se vea afectada.

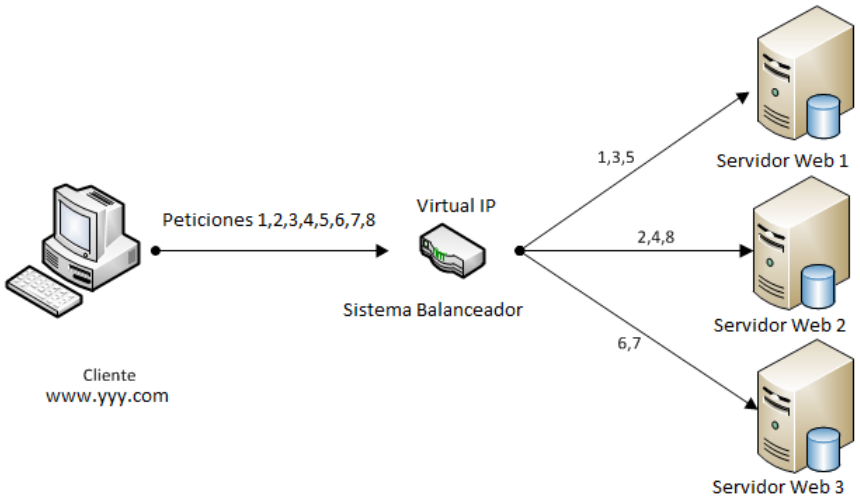

Fig. **45** Esquema de funcionamiento de un sistema de balanceo de carga

Por otro lado, el simple hecho de que las peticiones remotas sean atendidas por el equipo balanceador y no por el servidor final, supone una barrera de protección de cara a un posible intento de escalado de privilegios, por parte de un atacante, el cual supondría estar accediendo directamente al servidor real.

Igualmente, un gran número de peticiones, o ejecuciones de código malicioso, intentando explotar una vulnerabilidad web, serán directamente desechadas debido a la imposibilidad de su ejecución remota.

5.1.9. **Equipos UTM**

Utilizados sobretodo como alternativa común por la pequeña y mediana empresa, con el objetivo de reducir costes en la implantación de una solución de seguridad a su infraestructura de comunicaciones, los sistemas o firewall UTM (del inglés, Unified Threat Management) engloban varias soluciones de mitigación y prevención en un único sistema.

Esta nueva generación de equipos de seguridad, permiten englobar en un solo equipo dedicado, servicios de antimalware, IDS, IPS, firewall, proxy e incluso otras soluciones como balanceo de carga, antispam o gestión de ancho de banda, estas últimas en el menor de los casos. Todo ello llevado a cabo mediante, el denominado sistema de análisis de tráfico multicapa, que permite realizar una inspección en detalle del flujo de datos de la red. Esto da la posibilidad a un único administrador de red, de controlar de manera sencilla un alto porcentaje de la política de seguridad, y por tanto de efectuar un manteniendo de la misma mucho más ágil y controlado.

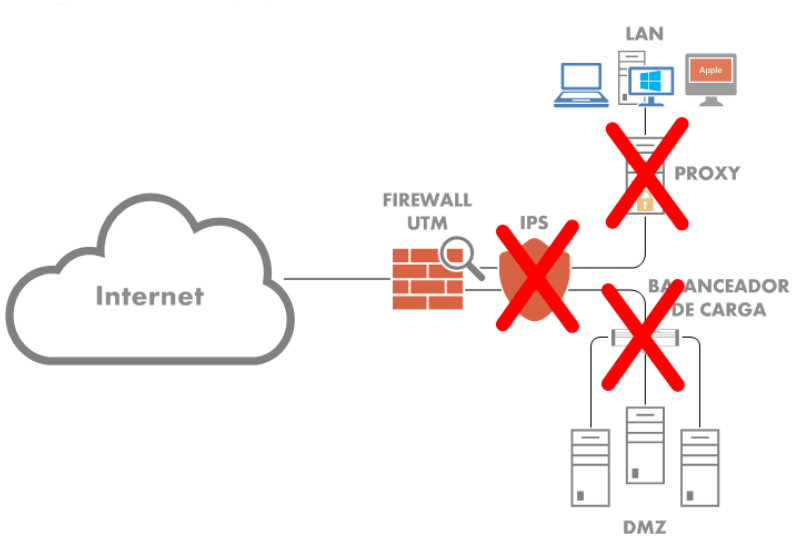

Fig. 46 Sustitución de un equipo UTM por el resto de soluciones de seguridad

Obviamente, el uso compartido de recursos hardware y un menor abanico de posibilidades de configuración que el ofrecido por las soluciones específicas en cada campo, hace que la efectividad y potencia de estos equipos se vea mermada significativamente. Sin embargo, el importante ahorro económico que supone para las empresas el hecho de tener gran parte de su infraestructura de seguridad concentrada en un mismo equipo, hace que esta sea una de las soluciones más elegidas en entornos no tan críticos, con resultados más que aceptables.

5.1.10. **Sistemas de correlación de eventos**

Si bien hasta ahora se ha comentado la existencia de diferentes sistemas de seguridad tanto activa como pasiva aplicables a una infraestructura de red. Con el objetivo de tener una visión global de la red y del estado real de la seguridad, todas estas soluciones habitualmente requieren de la revisión, por parte de la figura del administrador, de la información volcada en forma de log o registros de eventos, que estos equipos almacenan de manera local o envían a un servidor definido.

Esto presenta un importante y a la vez complejo reto que afrontar debido a que:

- El volumen crudo de eventos enviado por un único dispositivo puede alcanzar cantidades ingentes, y es necesaria la adopción de medios de evaluación de cara a, únicamente fijar la atención en aquellas entradas relevantes.

- La ausencia de eventos enviados por un dispositivo, puede suponer, de igual modo, tanto la no detección de problemas reportables como el mal funcionamiento o fallo de configuración de este. Esto supone la necesidad de un sistema de monitorización que garantice la correcta disponibilidad de los sistemas.

- Mientras que una serie de eventos enviados por parte de un dispositivo pueden carecer de toda importancia, o no resultar significativos como para requerir atención, este hecho puede cambiar de manera drástica al analizar el conjunto de toda la información reportada por los diferentes sistemas. Esta práctica es conocida como correlación.

- Sin embargo, el flujo continuo de eventos enviados y el volumen de estos, requiere de sistemas de alta velocidad de procesado para permitir dicho análisis, y la detección de una posible amenaza o problema en tiempo real.

- La criticidad de un evento no es un valor inmutable, sino que depende de factores de contexto. Un mismo evento en circunstancias diferentes puede variar en su nivel de importancia.

- Las acciones a adoptar ante la detección de un evento también difieren según el momento en que suceden o el histórico del mismo. Puede haber procedimientos distintos para el día o para la noche, para un caso aislado o reincidente, según cuál sea el impacto real desde el punto de vista de las operaciones de una organización y sus necesidades

Todo esto abunda en la necesidad de un sistema de gestión y correlación de eventos de mayor o menor nivel de sofisticación, más o menos alcance y una u otra capacidad de integración con los sistemas de la información y los procedimientos de gestión de la infraestructura de seguridad.

De igual modo, estos sistemas dotan de una excelente visibilidad temporal de la red, ofreciendo la posibilidad de generar y presentar informes detallados, tanto históricos como en tiempo real, y de integrarse tanto con soluciones específicas de gestión de dispositivos (firewalls, IPS, antimalware, etc.), como con los sistemas de gestión interna de la organización.

5.1.11. **Sistemas contra ataques DDoS**

A pesar de contar con grandes recursos de procesado de tráfico, tanto los sistemas firewall como el resto de sistemas de seguridad, dada la necesidad de estos cumplir con su principal cometido de aplicar un tratamiento de control a dicho tráfico y de tener que analizarlo en profundidad siguiendo las diferentes políticas de seguridad, en ocasiones, cuando el objetivo de un ataque no son los sistemas que protegen sino directamente ellos, se encuentran con que sus recursos no son suficientes para soportar las nuevas formas de ataques DoS o DDoS y por tanto pueden ser llevados al colapso, provocando con ello caídas en el servicio y, en muchas ocasiones, dejando el camino libre a los ciberdelincuentes para conseguir perpetrar las intrusiones en el sistema pretendidas inicialmente, donde el colapso de los sistemas de seguridad simplemente era el primer paso necesario.

Los sistemas contra ataques DDoS aparecen en este sentido como una herramienta dedicada y complementaria tanto para los propios sistemas de seguridad como para servidores Web, DNS, etc., con el objetivo de centrar su cometido únicamente en la mitigación de las diferentes formas de estos ataques.

La base de su funcionamiento consiste en el empleo de diferentes Bases de datos de firmas junto con patrones de flujo de tráfico, a partir de las cuales se evalúa y califica a cada una de las conexiones entrantes al sistema, así como a la dirección o direcciones IP identificados como fuente de dicha conexión.

A partir de esta calificación asignada, cuyo valor va siendo modificado dinámicamente a medida que la información recogida denota uno u otro comportamiento del emisor, el sistema considerará si la reputación del origen de la conexión es suficiente como para permitir el correspondiente flujo de datos o por el contrario es considerada como potencialmente maliciosa y por tanto relegada a un segundo nivel de evaluación, donde podrá ser dirigido a un estado de cuarentena y si se estima necesario finalmente bloqueado.

El sistema permite además la opción, en lugar de responder con el bloqueo de la conexión y el consiguiente mensaje de rechazo (*reject*) recibido en el origen, de descartar el tráfico malicioso, con lo que el posible atacante no recibiría ningún tipo de indicio de que su

conexión ha sido descartada y por tanto mantendría, sin ningún tipo de efecto, su ataque activo.

Esta nueva herramienta, de reciente aparición, se coloca como el único elemento de seguridad perimetral cuya ubicación lógica en la red se recomienda establecer por delante de los sistemas firewall, es decir, interponiéndose entre estos e Internet y ocupando el papel de primera línea de defensa en la red.

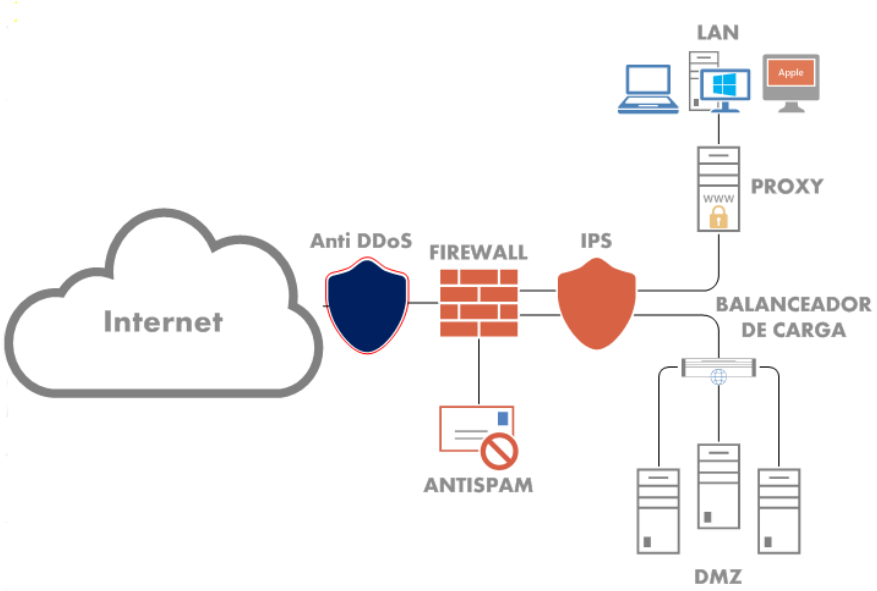

Fig. 47 Ubicación de un sistema anti DDoS en un diagrama de red

5.1.12. **Auditorias de Seguridad**

Otra de las medidas de seguridad, en este caso del tipo preventivo, más eficaces que un administrador de red puede tomar, ya sea de manera autónoma, o a través de la externalización de estos servicios a empresas especializadas, es la de realizar, de manera periódica, diferentes procesos de auditoría de seguridad, cuyo alcance ocupe la totalidad de cada uno de los elementos que integren la infraestructura de TI de la que sea responsable.

La constante evolución de las amenazas existentes, o el descubrimiento de nuevas vulnerabilidades en los sistemas, así como la respuesta emitida por los fabricantes de cara a aparición de nuevas soluciones y/o mejoras de los sistemas existentes a través de la

publicación parches o nuevas versiones de software, hacen necesario mantener al día todos los sistemas.

Practicas como la ejecución de test de intrusión o análisis de vulnerabilidades a través de las diferentes herramientas disponibles en el mercado, las cuales no sólo emiten un informe detallado como resultado del análisis, sino que acompañan dicha información con las soluciones publicadas en cada caso, pueden desvelar importantes fallos de seguridad, hasta ese momento totalmente desconocidos, y que habrían estado exponiendo la integridad y la seguridad de la red ante posibles amenazas.

5.2 Acuerdos gubernamentales

Pese a la constante persecución contra los cibercriminales y el amplio abanico de sistemas de seguridad existentes en el mercado, una de las principales vías de lucha contra el cibercrimen reside en la educación y concienciación tanto por parte de los usuarios como de la de los gobiernos, en cuanto al uso de las TIC, siendo estos últimos quienes juegan el papel más relevante en este sentido y de quienes realmente dependerá el curso seguido por la lucha contra la ciberdelincuencia.

En un estado de concienciación creciente, aunque aun por debajo del nivel necesario, los estados realizan notables esfuerzos por plantar cara al mundo del cibercrimen y solventar las diferentes barreras existentes para poder combatir con eficacia una nueva modalidad de delincuencia que durante años siempre ha ido varios pasos por delante.

Una de estas barreras, y quizá la más complicada a la vez que imprescindible de superar, es la limitación transfronteriza a la que se enfrentan las fuerzas del orden a la hora de emprender acciones legales o investigaciones. En un mundo donde el crimen organizado distribuye a sus miembros a lo largo y ancho de toda la superficie del planeta, resulta una tarea realmente complicada ejecutar la aplicación de las leyes pertinentes, más aun cuando estas difieren en su interpretación de un mismo delito, dependiendo de la nación en que este se plantee. Esto supone una enorme ventaja para los ciberdelincuentes, quienes, tal y como

ocurre habitualmente en muchos otros ámbitos de la delincuencia, recurren a la búsqueda de todo tipo de vacios legales para poder eludir a la justicia.

Ante esta situación, y comenzando desde el, ya mencionado anteriormente en este documento, "Convenio sobre cibercriminalidad" de 2001, donde se trataba de establecer un marco común en cuanto al tratamiento de los ciberdelitos por parte de los estados miembros, y al cual han ido uniéndose numerosos países desde su creación, donde fueron 30 los estados participantes[45], han sido varios los intentos de establecer métodos de actuación común

En Mayo del 2003, los miembros del entonces denominado G8 (aludiendo al grupo de los 8 países situados a la cabeza de la economía mundial), estableció una serie de recomendaciones dirigidas a todos los estados, en la búsqueda por avanzar en una estrategia de coordinación internacional y, citando textualmente[46]: "*con el fin de proteger eficazmente las infraestructuras críticas de la información y asegurarlas contra los daños y ataques. Dicha protección efectiva, incluye la identificación de las amenazas junto con la reducción al mínimo tanto la vulnerabilidad de las infraestructuras como el tiempo de recuperación, así como la identificación de la causa del daño o de la fuente del ataque para su posterior análisis por los expertos o las autoridades. Una protección eficaz requiere también la comunicación, la coordinación y la cooperación nacional e internacional entre todas las partes interesadas de la industria, la academia, el sector privado, entidades y gobiernos, incluida la protección de las infraestructuras y las fuerzas del orden. Tales esfuerzos deben llevarse a cabo teniendo en cuenta la seguridad de la información y la ley aplicable en materia de asistencia judicial y protección de la privacidad."*

Dicho documento, titulado G8 "***Principles for Protecting Critical Information Infrastructures***" (en español, principios para la protección de las infraestructuras de información crítica, en adelante **ICC**) contiene las siguientes recomendaciones:

[45] Un total de 30 países firman la primera convención internacional contra el Cibercrimen. http://www.elmundo.es/navegante/2001/11/26/esociedad/1006766268.html

[46] G8 Principles for Protecting Critical Information Infrastructures http://www.cybersecuritycooperation.org/documents/G8_CIIP_Principles.pdf

1. Los países deben tener un sistema de redes de advertencias sobre vulnerabilidades, amenazas e incidentes cibernéticos.

2. Los países deben incrementar la concientización para facilitar y ayudar a comprender a las partes interesadas la naturaleza y el alcance de las ICC y el papel que estas juegan en la protección de ellas.

3. Los países deben analizar sus infraestructuras y las dependencias entre las mismas con objeto de mejorar sus estrategias de coordinación y protección.

4. Los países deben promover alianzas entre el gobierno, el sector privado y público para analizar las IIC con el fin de prevenir, investigar y responder a los daños o ataques sufridos por estas infraestructuras.

5. Los países deben crear y mantener redes de notificación y comunicación ante crisis así como comprobarlas frecuentemente, para asegurarse de su seguridad y estabilidad ante situaciones de emergencia.

6. Los países deben asegurar las políticas de disponibilidad de los datos tomando como base la necesidad de proteger las IIC.

7. Los países deben facilitar el seguimiento de los ataques a las IIC y, si fuera necesario, la revelación de la información requerida a otras naciones.

8. Los países deben desarrollar ejercicios y entrenamientos necesarios para mejorar su capacidad de respuesta, y así comprobar los planes de continuidad y contingencia en caso de producirse un ataque contra las IIC, y además debe animar a las partes interesadas a participar en actividades similares.

9. Los países deben adecuar las regulaciones y legislaciones, siguiendo lo establecido en el Convenio sobre cibercriminalidad del 23 de Noviembre de 2001 y, así mismo, deben entrenar al personal necesario para investigar y perseguir los ataques a las IIC y coordinar las investigaciones con otros países cuando así se requiera.

10. Los países deben participar, cuando sea necesario, en la cooperación internacional para asegurar las IICC, incluyendo el desarrollo y la coordinación de los sistemas de alerta, y compartiendo y analizando la información relacionada con vulnerabilidades, amenazas e incidentes así como coordinando las investigaciones sobre los ataques a este tipo de infraestructuras de acuerdo con la legislación local.

11. Los países deben promover la investigación y el desarrollo tanto nacional como internacional así como fomentar la aplicación de tecnologías de seguridad, certificadas de acuerdo a los estándares internacionales.

En esta línea de ideas, los gobiernos de todo el mundo han querido mostrar su implicación con la seguridad tecnológica a través de la fundación y desarrollo de diferentes grupos de lucha contra la ciberdelincuencia y los ciberataques.

Prueba de ello, ha sido el nacimiento durante estos últimos años de diferentes equipos de respuesta ante emergencias informáticas, también conocidos como **CERT** (Computer Emergency Response Team).

En el caso de España, son ya varios los grupos formados en este sentido, encontrándose entre los más importantes el perteneciente al Instituto Nacional de Tecnologías de la Comunicación (INTECO) **INTECO-CERT** y sobre todo, tanto por su antigüedad como por su colaboración en el marco de los acuerdos europeos, a través del Cuerpo Nacional para la Protección de las Infraestructuras Críticas (CNPIC), el **CNN-CERT.**

Utilizando textualmente la descripción del sitio web de la organización (https://www.ccn-cert.cni.es/)

"El CCN-CERT es el Equipo de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó a finales del año 2006

como el CERT gubernamental/nacional, y sus funciones quedan recogidas en la Ley 11/2002[47] *reguladora del Centro Nacional de Inteligencia (CNI), el Real Decreto 421/2004*[48] *de regulación del CCN y en el Real Decreto 3/2010* [49]*, de 8 de enero, regulador del Esquema Nacional de Seguridad.*

De acuerdo a todas ellas, el CCN-CERT tiene responsabilidad en ciberataques sobre sistemas clasificados y sobre sistemas de la Administración y de empresas pertenecientes a sectores designados como estratégicos. La misión del CCN-CERT es, por tanto, contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a las Administraciones Públicas y a las empresas estratégicas, y afrontar de forma activa las nuevas ciberamenazas. Para ello cuenta, entre otros, con servicios de:

- *Soporte y coordinación para el tratamiento de vulnerabilidades y resolución de incidentes*
- *Investigación y divulgación de mejores prácticas (Guías CCN-STIC)*
- *Formación al personal de la Administracion especialista en ciberseguridad*
- *Información sobre vulnerabilidades, alertas y avisos de nuevas amenazas sobre los sistemas de información*

Como CERT Gubernamental ofrece la información, formación, recomendaciones y herramientas necesarias para que las Administraciones Públicas puedan desarrollar sus propias capacidades de respuesta a incidentes, siendo su coordinador a nivel público estatal."

Siguiendo con esta misma filosofía, aunque ya en Octubre de 2012, el Ministerio del Interior y el Ministerio de Industria, Energía y Turismo firmaron un convenio de colaboración con el objetivo de mejorar la lucha contra la ciberdelincuencia y el Ciberterrorismo, en el que

[47] BOE núm. 109 Martes 7 mayo 2002 .
https://www.ccn.cni.es/images/stories/normas/pdf/ley_11_2002_reguladora_cni.pdf

[48] BOE núm. 68 Viernes 19 marzo 2004.
https://www.ccn.cni.es/images/stories/normas/pdf/rd421-2004centrocriptologiconacional.pdf

[49] Real Decreto 3/2010, de 8 de enero https://www.ccn-cert.cni.es/publico/ens/BOE-A-2010-1330.pdf

se recogía la colaboración, con el objetivo de mejorar la protección de las infraestructuras críticas, del CNPIC, las Fuerzas y Cuerpos de Seguridad del Estado y el INTECO.

Sin embargo, pese a que este tipo de documentos y convenios suponen grandes avances, todavía existirá una importante carencia en lo que se refiere a la homogeneidad legislativa internacional mientras los países sigan intentando actuar de manera independiente.

5.3 Grupos de lucha

Además de los ya mencionados CERT, o Equipos de Respuesta a incidentes de Seguridad, existen en la actualidad un gran número de grupos organizados para combatir y perseguir la ciberdelincuencia y a quienes la practican. Cada país cuenta con grupos independientes o divisiones de sus propias fuerzas de seguridad, los cuales participan de manera activa y especializada en este ámbito, pudiendo llegar en a requerir de la colaboración internacional de sus homólogos en otras naciones.

A continuación se detallan algunos de estos grupos y fuerzas del orden cuya importancia ha sido considerada relevante en este estudio.

Grupo de Delitos Telemáticos (GDT): Fundado dentro de la Unidad Central Operativa de la Guardia Civil, y dividido en los llamados Equipos de Investigación Tecnológica (EDITE) en cada una de las provincias de España, tiene como objetivo principal la investigación de todos aquellos delitos cometidos por medio de las redes y sistemas de información.

El GDT destaca además por sus constantes esfuerzos enfocados al fomento del uso seguro de las nuevas tecnologías, así como a la difusión, a través de las redes sociales, de información de ayuda y prevención al internauta, relacionada con todo tipo de noticias y consejos de actuación ante nuevas amenazas y estafas en la red.

Fig. 48 Captura de la cuenta de Twitter del GDT

Preocupado además de mantener una presencia constante en seminarios y conferencias internacionales, actualmente el grupo es miembro y participa activamente en los Grupos de Trabajo de Interpol de Europa y Latinoamérica, en el Foro internacional del G-8 para el cibercrimen, y en Grupo de policía europeo, Europol.

Brigada Investigación Tecnológica (BIT): Perteneciente al Cuerpo Nacional de Policía, y encuadrada dentro de la unidad de Delincuencia Económica y Fiscal junto con el GDT, esta unidad participa de manera conjunta a este último en la investigación y persecución de delitos cometidos mediante el uso de las tecnologías de la información.

Igualmente se encarga de la difusión de contenidos a través de la web y las redes sociales y muestra su participación activa en los foros internacionales de cooperación policial y colaboración ciudadana.

Centro Europeo de Ciberdelincuencia (EC3): Formado como división tecnológica de la oficina europea de Policía, Europol, e inaugurado en Enero de 2013, el EC3 se presenta con la intención de convertirse en el punto focal en la lucha de la Unión Europea contra la ciberdelincuencia, a través de la creación de capacidades operacionales y analíticas para la investigación y la cooperación de los estados miembros como a través de un único marco común.

El hecho de formar parte de Europol, le otorga las capacidades y la infraestructura de esta de cara a la aplicación de la ley en todo el territorio europeo, hecho que supone un importante avance legislativo en los problemas transfronterizos existentes hasta ahora, en lo que a la persecución y puesta a disposición judicial de los ciberdelincuentes se refiere.

Grupo Europeo de Ciberseguridad (ECSG): A diferencia de las anteriores, pertenecientes todas ellas a diferentes cuerpos de seguridad, el recién formado (Mayo de 2013) ECSG, se sitúa como una de las fuerzas independientes más grandes de Europa en este campo.

Liderado por la empresa de seguridad española S21sec, en asociación las empresas CSIS (Dinamarca), Fox IT (Holanda), y Lexsi (Francia), el grupo, que cuenta con la suma de más de 600 expertos, se presenta como firme candidato del nivel de las estadounidenses McAfee, IBM, HP y Symantec, para asesorar y colaborar con los gobiernos de los distintos países, así como proveedor de servicios CERT para la Unión Europea en la lucha contra el Cibercrimen internacional.

Internet Crime Complaint Center (IC3): Sin dejar de mencionar a los servicios de seguridad estadounidense, como la CIA o el FBI, como incuestionables fuerzas contra la lucha contra el Cibercrimen, merece la pena mencionar al Internet Crime Complaint, como un organismo fundado en asociación entre el Centro Nacional de Delitos de Cuello Blanco (NW3C) y la Oficina Federal de Investigaciones (FBI), con el objetivo de presentarse al usuario como el mejor método para denunciar ante las autoridades cualquier caso de Cibercrimen del que hayan sido víctimas.

5.4 Últimos hitos

Para finalizar con este capítulo, a continuación se muestran algunas de las noticias de mayor relevancia publicadas recientemente en diferentes medios de información.

El cierre de la red de spam Rustoc hace caer un tercio del correo basura en el mundo

El cierre de la red mundial de spam Rustock, que enviaba 13.820 millones de correos electrónicos no deseados al día, hizo caer este tipo de ciberdelincuencia un tercio, según el informe de Messagelabs Intelligence del mes de marzo realizado por la multinacional de seguridad Symantec.

El informe señala que desde el desmantelamiento de este llamado botnet (pastor que controla remotamente e ilegalmente ordenadores) que se ha producido este mes, han aumentado las actividades para aprovechar el vacío dejado y está ocupando su lugar Bagle.

Symantec explica en una nota de prensa que entre el 15 y el 17 de marzo, tras las acciones legales contra Rustock, el spam a nivel mundial cayó un 33,6 %.

Fuente: Diario Hoy Tecnología (Edición Online) 30/03/2011.

http://www.hoytecnologia.com/noticias/cierre-spam-Rustoc-hace/295163

Asalto a farmacias online

La operación de la INTERPOL, Pangea6, se ha convertido en un ejemplo de la buena cooperación internacional. El asalto simultáneo de la policía en 100 países concluyó con 58 arrestos, el cierre de 9.000 páginas web y la confiscación de 9,8 millones de paquetes que contenían drogas peligrosas y que se vendían sin prescripción médica a través de farmacias online. Estas sustancias podrían haber causado un gran daño ya que suelen ser fármacos falsos o que se utilizan erróneamente. Además, estos negocios farmacológicos suelen ser la tapadera de otros tipos de empresas del cibercrimen.

Fuente: Kaspersky Labs (Blog online) Jul. 2013

http://blog.kaspersky.es/lucha-contra-el-cibercrimen-exitos-internacionales

Detenido en Barcelona el responsable del mayor ciberataque de servicios DDOS

Agentes de la Policía Nacional han detenido en Granollers (Barcelona) al activista holandés Sven Olaf Kamphuis, de 35 años, como responsable del mayor ciberataque de denegación de servicios DDOS de la historia, que el pasado mes de marzo colapsó internet en todo el mundo.

La portavoz de la Policía Nacional, María Buyo, ha explicado que las investigaciones se iniciaron en Holanda después de que en marzo se detectaran una serie de ataques informáticos contra una compañía anti-spam, que también afectó a los Estados Unidos y el Reino Unido.

Considerado el mayor ciberataque del mundo, colapsó internet por los intentos de hacerse con el control de los servidores afectados.

Fuente: RTVE (Online) 28/04/2013

http://www.rtve.es/noticias/20130428/detenido-barcelona-responsable-del-mayor-ciberataque-servicios-ddos/652120.shtml

El GDT desarticula una red dedicada a la prostitución infantil y corrupción de menores en Internet

El Grupo de Delitos Telemáticos (GDT) de la Guardia Civil en el transcurso de la operación GUARDADOR llevada cabo en la Comunidad de Madrid, ha detenido a seis personas como presuntas autoras de varios delitos de prostitución y corrupción de menores. Los adultos detenidos contactaban y captaban a sus víctimas a través de las redes sociales, ofreciéndoles dinero y regalos, con la única finalidad de mantener relaciones sexuales con ellos, a sabiendas de la minoría de edad de los mismos.

Fuente: GDT (Sitio Online) 22/08/2013

https://www.gdt.guardiacivil.es/webgdt/popup_noticia.php?id=1228

Capítulo 6. **Conclusiones**

Como último punto del documento, este capítulo dedica su contenido a realizar un breve repaso sobre el cómputo general de las ideas comentadas hasta ahora. Intentando establecer una serie de conclusiones, como resultado final del estudio realizado.

Sin lugar a dudas, la ciberdelincuencia supone una nueva visión de lo que hasta ahora había sido considerado como acto delictivo. En un mundo donde la población se encuentra las 24 horas del día conectada a la red, los delincuentes han encontrado un nuevo lugar, lleno de posibilidades, donde acechar y cometer sus delitos.

Al igual que ocurriera con la delincuencia tradicional, el ciberdelincuente no es una figura encasillada dentro de un único perfil, sino que es posible diferenciar numerosos tipos según sea su metodología, sus objetivos personales o su papel en una estructura criminal organizada.

Tanto organizaciones, como gobiernos y, como no podía ser de otra forma, los ciudadanos se encuentran expuestos a todo un abanico de delitos y estafas en la red, aunque no siempre jugando únicamente el papel de víctima. En ocasiones, la sensación de anonimato y libertad obtenida de Internet, lleva a algunos a "descuidar" la atención sobre donde se encuentra el límite entre lo legal y lo ilegal.

En cuanto a los métodos y técnicas empleados por los ciberdelincuentes para alcanzar sus objetivos, se puede definir este análisis según sea la motivación primordial por la que estos se ven guiados. Siguiendo esta idea, se encuentran en primer lugar aquellos cuyo objetivo principal es el de obtener una rentabilidad económica como fruto de sus actos. Estos métodos aparecen principalmente en forma de estafas o robos de información y sus principales medios de acceso a las víctimas han pasado de ser el correo electrónico y los sitios web, para ir dejando paso a las omnipresentes redes sociales y los terminales móviles de nueva generación.

A continuación, aparecen los denominados ciberdelincuentes sociales, cuyo objetivo no tiene nada que ver con el anterior, sino que se trata de individuos cuyos delitos afectan directamente a las personas, tanto en su integridad física como psicológica.

Por último, y aquí es donde aparecen los mayores grupos organizados, se presenta la llamada ciberdelincuencia ideológica. Fruto de las nuevas herramientas que nos ofrece nuestra era, aquellos que se enfrentan a las ideas impuestas por gobiernos y grandes empresas, muestran su han recurrido al uso de la tecnología y los conocimientos informáticos para desacreditar a sus víctimas y mostrar sus ideales. Los gobiernos, ante algunos de estos actos de rebeldía y amenazas, no dudan en colgar el cartel de Ciberterroristas a aquellos que atentan contra sus sistemas, ponen en entredicho su reputación o infringen las leyes y derechos que restringen el uso y acceso libre a determinados tipos de información.

En un repaso por la historia, se ha podido ver como la aparición de aquellos primeros jóvenes curiosos que decidieron saltarse las normas para investigar, fueron, a la vez, los principales decisores del curso que seguirían los avances tecnológicos desde entonces hasta hoy en día. Dejando lugar a la duda, de qué habría pasado, si los sistemas informáticos y las

redes de la información hubieran permanecido siempre protegidos y regulados por sus creadores como dictaba la ley.

Una vez analizado el pasado, el presente y futuro de la ciberdelincuencia sitúa sus objetivos en el ciberespionaje, la ciberguerra, el crecimiento de infecciones en terminales móviles y redes sociales y el aumento de ataques a los nuevos servicios en la nube.

Identificada la gravedad y dificultad que supone el desarrollo del cibercrimen, se plantea el análisis de las diferentes soluciones y medios existentes para combatir el problema desde diferentes puntos de vista.

En primer lugar y más importante, la educación ciudadana y la concienciación sobre el peligro potencial que supone la falta de celo en el manejo de información confidencial, supone una medida básica de prevención y a su vez de lucha contra la ciberdelincuencia. Teniendo en cuenta que un ciberdelincuente basa gran parte de sus argumentos y métodos en la ingeniería social y el engaño, esta tarea se vuelve mucho más complicada si las víctimas a las que se enfrenta ya se encuentran preparadas.

La aparición de acuerdos como el ”Convenio sobre cibercriminalidad”, firmado en Budapest en 2001, marcó un antes y un después en la lucha por parte de los gobiernos, y dejó clara la necesidad de establecer acuerdos internacionales, como medida fundamental para garantizar la efectividad de las fuerzas del orden en su objetivo de mantener la seguridad de los ciudadanos y las organizaciones así como en el de castigar a aquellos que la pongan en entredicho. No cabe duda sin embargo, de que aún queda mucho camino por recorrer y recursos que invertir, a pesar de que, desde entonces han sido numerosos los acuerdos surgidos en la misma línea y los estados son conscientes de que para que sus esfuerzos sean efectivos, deben trabajar en un marco común y remar en el mismo sentido.

En tercer lugar, la instalación y adopción de medidas de seguridad se establece como la opción a seguir tanto por parte del los usuarios como de las organizaciones, para solventar la vulnerable posición que presentan los sistemas de la información y las comunicaciones, en un entorno que con el paso del tiempo se ha ido volviendo cada vez más peligroso y donde no caer en alguna de las innumerables estrategias de los ciberdelincuentes se ha convertido en una tarea prácticamente imposible.

Estas medidas han conseguido que, poco a poco, los esfuerzos vayan dando sus frutos y que, cada vez con mayor eficacia, sea posible igualar la balanza en la lucha contra la ciberdelincuencia.

Capítulo 7. **Bibliografía y referencias**

[1] Convenio sobre cibercriminalidad, Budapest 23/11/2001 [en línea]

http://conventions.coe.int/Treaty/en/Treaties/Html/185-SPA.htm

[2] Cybercrime is a Global Problem; Increasingly Social and Mobile (2012 Norton Cybercrime Report) [en línea]

http://www.symantec.com/connect/blogs/cybercrime-global-problem-increasingly-social-and-mobile-2012-norton-cybercrime-report

[3] McAfee. Informe sobre Criminología Virtual 2009. [en línea]

http://www.mcafee.com/mx/resources/reports/rp-virtual-criminology-report-2009.pdf

[4] Panda Security. Los profesionales del Cibercrimen [en línea]

http://cybercrime.pandasecurity.com/blackmarket/cybercrime_professions.php?lang=es

[5] Entrevista completa Jose María Alonso. Mayo 2013 [en línea]

http://www.marketingdirecto.com/marketing-directo-tv/ponencias/clubm-by-maxus-con-chema-alonso-hacker-love-your-hackers/

[6] Norton Cybercrime Report 2012[en línea]

http://nowstatic.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

[7] Ontsi. Uso de Internet de individuos [en línea]

http://www.ontsi.red.es/ontsi/es/indicador/individuos-que-usan-frecuentemente-internet

[8] Trustwave Global Security Report 2013 [en línea]

http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf

[9] Encuesta sobre el uso de Tecnologías de la Información y las Comunicaciones (TIC) y del Comercio Electrónico en las empresas 2011/12[en línea] http://www.ine.es/prensa/np718.pdf

[10] Inform “China’s Cyber Espionage Units” [Artículo] http://intelreport.mandiant.com

[11] Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa [en línea] https://www.gdt.guardiacivil.es/webgdt/media/Legislacion/Protocolo_adicional_convencion_cibercrimen.pdf

[12] Brigada de Investigación Tecnológica [en línea] www.policia.es/bit/index.htm

[13] Panda Security. Informe Q1 2013. [En línea]

http://prensa.pandasecurity.com/wp-content/uploads/2010/03/Informe-Trimestral-Q1-2013-ES.pdf

[14] Web de Internet World Stats [en línea] http://www.internetworldstats.com/

[15] Kaspersky Security Bulletin: Spam Evolution 2012 [en línea]

http://www.securelist.com/en/analysis/204792276

[16] Kaspersky spam in Q3 2012 [en línea]

http://www.securelist.com/en/analysis/204792251/Spam_in_Q3_2012

[17] Informe sobre las amenazas para la seguridad de los sitios web 2013 [en línea]

https://www.symantec-wss.com/campaigns/14385/es2/int/assets/symantec-WSTR2-ES.pdf

[18] Web de Wikileaks [en línea] wikileaks.org

[19] Julian Assange biography. [En línea] http://www.biography.com/people/julian-assange-20688499

[20] NSA fears Snowden saw details of China spying. [Artículo]

http://www.usatoday.com/story/news/nation/2013/07/11/nsa-snowden-espionage-china-microsoft/2510623/

[21] Iran 'building copy of captured US drone' RQ-170 Sentinel [Artículo]

http://www.bbc.co.uk/news/world-middle-east-17805201

[22] EEUU desclasifica PRISM al tiempo que se filtra su herramienta de catalogación de datos [Artículo]

http://es.engadget.com/2013/06/09/eeuu-desclasifica-prism-catalogador-boundless-informant-filtrado/

[23] El Parlamento Europeo investigará el espionaje electrónico de PRISM en los países de la Unión [Artículo]

http://es.engadget.com/2013/07/04/parlamento-europeo-investigara-espionaje-eeuu-prism/

[24] Declaración Universal de los Derechos Humanos [en línea]

http://www.un.org/es/documents/udhr/

[25] Diario El Mundo.es La red social Ask.fm toma medidas contra el ciberacoso tras el suicidio de una joven [Artículo]

http://www.elmundo.es/elmundo/2013/08/19/navegante/1376937003.html

[26] Video de Amanda Tood [en línea]

http://www.ciberbullying.com/cyberbullying/2012/10/17/el-video-con-el-que-amanda-todd-luchaba-contra-el-ciberbullying-subtitulado-al-espanol-por-pantallasamigas/

[27] Original article, "The Conscience of a Hacker". [Artículo]

http://www.phrack.org/issues.html?issue=7&id=3&mode=txt

[28] Advisory CA-1989-04 WANK Worm on SPAN Network. [Artículo]

http://www.cert.org/advisories/CA-1989-04.html

[29] History of Guy Fawkes [en línea] http://www.bbc.co.uk/history/people/guy_fawkes

[30] Película V de Vendetta [en línea] http://wwws.warnerbros.es/vforvendetta/

[31] Anonymous ataca la web de la Policía Nacional [Artículo]

http://www.cadenaser.com/espana/articulo/anonymous-ataca-web-policia-nacional/csrcsrpor/20110612csrcsrnac_2/Tes

[32] Using hastags on Twitter [en línea] https://support.twitter.com/articles/49309#

[33] Explicación de la abreviatura LOL [en línea] http://www.frikipedia.es/friki/LOL

[34] Associate of Hacking Group LulzSec Indicted for Conspiracy to Conduct Cyber Attacks. [Artículo]

http://www.fbi.gov/losangeles/press-releases/2012/associate-of-hacking-group-lulzsec-indicted-for-conspiracy-to-conduct-cyber-attacks

[35] Historia de la Blue Box. [en línea] http://www.ionlitio.com/hackers-capitulo-i/

[36] McAfee. Una gran década para el Cibercrimen. 2011[en línea]

http://www.mcafee.com/es/resources/reports/rp-good-decade-for-cybercrime.pdf

[37] Stuxnet y el nacimiento de la ciberguerra [Artículo]

http://www.theqore.com/articulos/6560/Stuxnet-y-el-nacimiento-de-la-ciberguerra

[38] Securitybydefault. Recopilación de los ataques a Sony [Artículo] 2011

http://www.securitybydefault.com/2011/05/recopilacion-de-los-ataques-sony.html

[39] Tendencias de ciberdelincuencia para 2013 [en línea] abril 17, 2013 by CristinaSanz

http://itercriminisblog.com/index.php/tendencias-ciberdelincuencia-2013/

[40] Trustwave global security report 2013 [en línea]

https://www2.trustwave.com/2013GSR.html

[41] How a remote town in Romania has become cybercrime central [Artículo]

http://www.wired.com/magazine/2011/01/ff_hackerville_romania/all/1

[42] Sophos Security Trheat Report 2013 [en línea]

http://www.sophos.com/en-us/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf

[43] Cisco Security Applied Intelligence for a Risky World [en línea]

http://www.cisco.com/en/US/solutions/collateral/ns1015/ns1238/info_graphics_c82-727889.pdf

[44] Definición de las siete capas del modelo OSI [en línea]

http://support.microsoft.com/kb/103884/es

[45] Diario El Mundo. Un total de 30 países firman la primera convención internacional contra el Cibercrimen. [Artículo]

http://www.elmundo.es/navegante/2001/11/26/esociedad/1006766268.html

[46] G8 Principles for Protecting Critical Information Infrastructures [en línea]

http://www.cybersecuritycooperation.org/documents/G8_CIIP_Principles.pdf

[47] BOE núm. 109 Martes 7 mayo 2002 [en línea]

https://www.ccn.cni.es/images/stories/normas/pdf/ley_11_2002_reguladora_cni.pdf

[48] BOE núm. 68 Viernes 19 marzo 2004 [en línea]

https://www.ccn.cni.es/images/stories/normas/pdf/rd421-2004centrocriptologiconacional.pdf

[49] BOE. Real Decreto 3/2010, de 8 de enero [en línea]

https://www.ccn-cert.cni.es/publico/ens/BOE-A-2010-1330.pdf

[50] Sitio web del CCN CERT [En línea] https://www.ccn-cert.cni.es/

[51] Sitio web del CNPIC [En línea] http://www.cnpic-es.es

[52] Defense Security Service website [en línea] http://www.dss.mil/

[53] Sitio web de la compañía Corero Networks [en línea] http://www.corero.com/es/

[54] Sitio web de la compañía Fortinet [en línea] http://fortinet.com

[55] Sitio web de INTERPOL [en línea] http://www.interpol.int/es/

[56] Sitio web de Centro Europeo de Ciberdelincuencia [en línea]

https://www.europol.europa.eu/ec3

[57] European Cibersecurity Group website [en línea] http://www.cybersecuritygroup.eu/

[58] Internet Crime Complaint Center website [en línea] http://www.ic3.gov/default.aspx

[59] Sitio web de Protocolo Ciberbullying [en línea] http://www.protocolo-ciberbullying.com/

[60] Sitio web de Disidents Team [en línea] http://www.disidents.org/

[V04] Dan Verton. Blackice. La Amenaza Invisible del Ciberterrorismo, Ed. McGraw Hill, 2004

[FT07] Javier Gustavo Fernandez Teruel. Cibercrimen: Los delitos cometidos a través de Internet, 2007

[R08] David Rice. Geekonomics: The Real Cost of Insecure Software, Ed. Addison Wesley, 2008

[T08] Carlos Tori. Hacking Ético. Autoedición ,2008

[FT11] Javier Gustavo Fernandez Teruelo. Derecho Penal e Internet. Ed. Lex Nova, 2011

[RC11] Carlos Garcia Romero Casabona. Cibercrimen. Ed. Comares, 2011

[RY12] Alejandro Ramos, Rodrigo Yepes. Hacker Épico. Ed. Informatica 64, 2012