UNIVERSIDAD DE EXTREMADURA

Escuela Politécnica

Grado en Ingeniería Informática

En Ingeniería del Software

Trabajo Fin de Grado

Análisis de la privacidad en las redes sociales

ESCUELA POLITÉCNICA

UNIVERSIDAD DE EXTREMADURA

Escuela Politécnica

Grado en Ingeniería Informática

En Ingeniería del Software

Trabajo Fin de Grado

Análisis de la privacidad en las redes sociales

Autor: Marta Sanabria González

Tutor: Rafael Martín Espada

1 ÍNDICE GENERAL DE CONTENIDOS

2 ÍNDICE DE FIGURAS

3 ÍNDICE DE TABLAS

4 INTRODUCCIÓN

Hoy en día no cabe ninguna duda de que la sociedad actual se desarrolla sobre lo que se conoce como Internet en sentido amplio, esto es, una infraestructura que transciende la funcionalidad primaria de soporte a sistemas de comunicación para modificar los propios modos de vida del siglo XXI en todos sus aspectos. Y dentro del "ecosistema" Internet nada ha tenido un impacto tan vertiginoso como las redes sociales, que soportan un sinnúmero de relaciones humanas con el objeto de asociar intereses de lo más diverso: deportivos, musicales, científicos, afectivos, etc... (1) Y esto conlleva a los usuarios a compartir información personal relevante con consecuencias que trascienden la mera intención inicial.

Cada vez es mayor el número de personas que las utilizan (2), almacenando en su seno infinidad de datos personales explícitos e implícitos (a través de su uso, conformando los metadatos) que se vuelven objetivo de los negocios lícitos e ilícitos; y por ello se han convertido en un objetivo perfecto de usuarios maliciosos para realizar ataques con diferentes propósitos, principalmente para obtener algún beneficio tangible, tal como información personal, números de cuentas bancarias, hábitos, etc., pero también para dañar la reputación de marcas.

Si bien se está abordando intensamente un debate acerca de la privacidad y de los riesgos inherentes a la falta de ella, el debate está lejos de estar cerrado. Se cifra de más de 550 millones de variantes de malware, a razón de 390.00 nuevos programas malignos diarios. (3) Como se puede entender, estas cifras resultan escalofriantes hasta para los más acostumbrados a los guarismos de Internet.

Pero si habitualmente estamos convencidos de utilizar aplicaciones confiables, al menos hasta cierto punto, y en unas condiciones normales de uso, ¿cómo se propaga esta verdadera epidemia por la red? Es habitual encontrar en la red, listas de oquedades por las que penetran este software malicioso, como la siguiente:

- El usuario hace clic en un email de phishing, o un email de *spear* phishing adaptado específicamente, que lleva a un sitio web que contiene malware, como el recibido muy recientemente por la Universidad de Extremadura.

- El usuario abre un documento que contiene un enlace que lleva a un sitio web que contiene malware.
- El usuario hace clic en un enlace en una **red social (como Facebook o Twitter)**, que lleva a un sitio web que contiene malware.
- El usuario hace clic en un enlace contenido en un sitio web de confianza (como un sitio de noticias), que lleva a un sitio web que contiene malware.
- Operadores malignos infectan un sitio web de confianza, programándolo para entregar malware a los visitantes, incluso cuando estos no hagan clic en ningún enlace.
- Operadores malignos intervienen una red de distribución de contenido, herramientas de monitorización de usuarios u otros componentes del sitio web, programándolos para entregar malware a los visitantes.

Como se puede adivinar de la lista anterior, independientemente de la gravedad e impacto de los ataques, es evidente que la forma de propagarse está directamente relacionada con la expansión del medio de propagación y en este caso, las redes sociales son únicas en cuanto a capilaridad y poca preparación de los usuarios, lo que las convierte en el mecanismo preferido de los usuarios maliciosos.

A pesar de todos estos informes, nuestra relación con los medios informáticos hace que nos resistamos a creer que nos encontramos en un escenario de vulnerabilidad constante. El uso de palabras de paso y los mecanismos de autenticación, la personalización, el entorno controlado, etc., nos impregna de un ambiente equivocadamente seguro, en la confianza de nuestra relación personal y rutinaria con estos mecanismos que hace que no advirtamos absolutamente nada de lo que ocurre con nuestros datos hasta que se desencadena un malfuncionamiento de los sistemas. (4)

En este proyecto nuestro objetivo ha sido ofrecer una visión aún más detallada de las existentes acerca de la privacidad y la facilidad de obtención de datos privados y públicos, para, debidamente correlacionados, establecer vectores de ataque que ya ni siquiera deben seguir el mundo informático. Y es que la información no solo tiene

valor en el mundo virtual, sino que establece fuertes vínculos con nuestra forma de vida e la influye inevitablemente, de forma que delitos clásicos se ven ahora reforzados por uso de medios electrónicos.

Para realizar este estudio se han analizado las redes sociales más extendidas, los ataques más frecuentes, las medidas de seguridad que aportan las plataformas, mucho más concienciadas en los últimos tiempos y se han realizados pruebas experimentales con herramientas de correlación de datos que, estando a disposición de todo el mundo para objetivos de defensa, también permiten el uso malicioso. Y es que, efectivamente, herramientas como NMAP, Maltego, Wireshark, etc... Son formidables para el análisis de la red y la seguridad, pero también esa misma información que ofrecen resulta ser la ganzúa de los malhechores.

Más concretamente, el proyecto parte de la idea original de intentar caracterizar aquellos perfiles de redes sociales que llevan a sitios web maliciosos, detectando aquellos usuarios delincuentes que permanentemente despliegan sus perfiles a la búsqueda de usuarios incautos, del mismo modo que los terroristas actuales se encubren tras perfiles inocentes para captar acólitos (5). Si bien las principales redes sociales han implementado medidas para evitar la propagación de materiales poco aceptables para los estándares morales, incluso con exceso de celo, aún queda un largo trecho por recorrer.

4.1 USO DE LAS REDES SOCIALES

Parece una obviedad afirmar que las redes sociales han sido el revulsivo más importante de la expansión de la tecnología. Y es que, si bien las redes sociales como tal se analizan y estudian desde prácticamente los orígenes de la sociología (por ejemplo, la teoría de los Seis Grados de Separación data de 1930) bien es cierto que la tecnología acorta espacio y tiempo y transforma las relaciones de una forma definitiva. Este hecho y la necesidad del ser humano de pertenecer a un grupo, la creación de identidades, etc. han reforzado el uso y la necesidad imperiosa de disponer de tecnologías que faciliten la intercomunicación entre individuos.

En efecto, según un estudio realizado en el año 2016 (6) sobre internet y las redes sociales, se concluye que de los más de 7.395 millones de habitantes del planeta, 3.419 millones tienen acceso a internet y casi una tercera parte utilizan regularmente las redes sociales, la mayoría de ellas utilizan su teléfono móvil para acceder a las redes sociales.

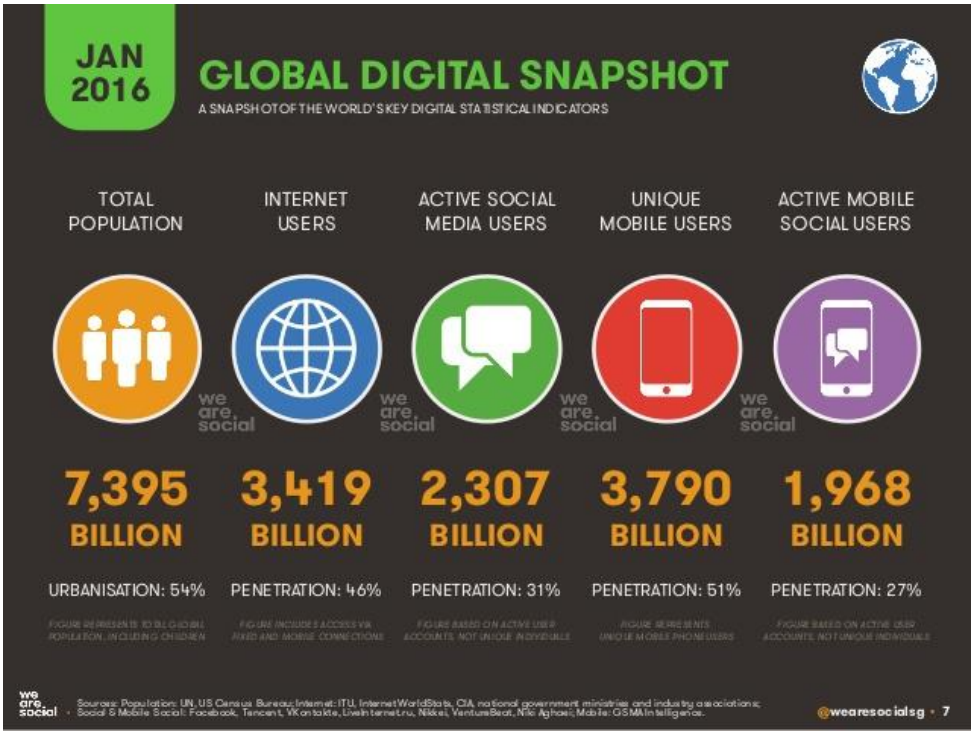


Ilustración 1. Usuarios de internet en 2016 Fuente: www.wearesocial.com

En cuanto a España, de los 46,5 millones de habitantes, 35,7 son usuarios de internet (77%) y 22 millones cuentan con perfiles en las redes sociales (47%). Esto quiere decir que una parte importante de la población utiliza las redes sociales, comenzando a ser más extraño el no estar que el estar en ellas. Otro dato que conviene resaltar es que los usuarios españoles pasan casi dos horas diarias utilizando las redes sociales, lo que nos indica que no sólo se está en ellas sino que se conversa, se disfruta de la música, vídeos, etc. convirtiéndose prácticamente en el nuevo escritorio de los dispositivos conectados.

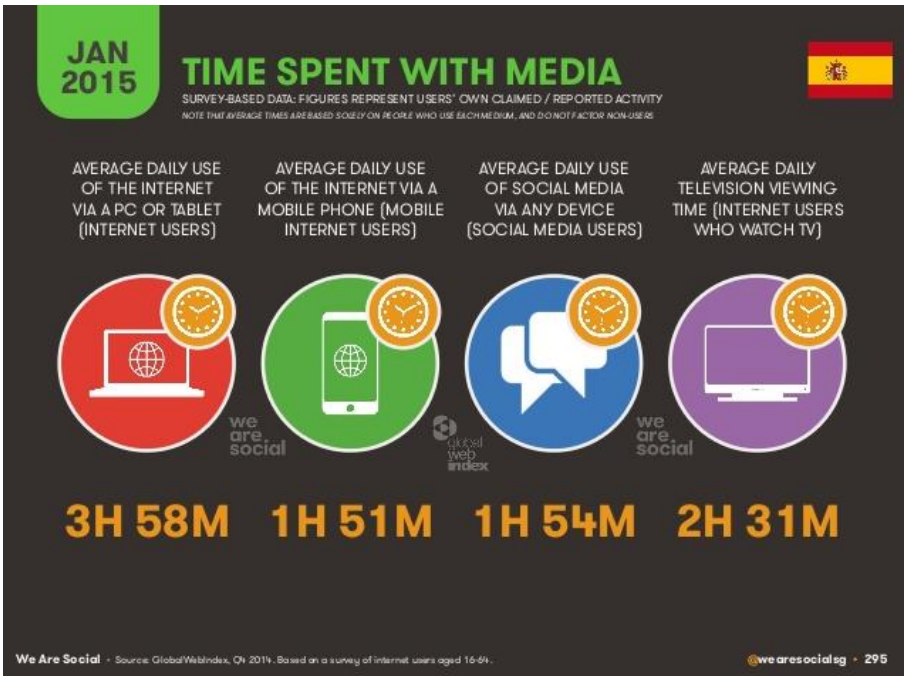


Ilustración 2. Usuarios de interet en España Fuente: www.wearesocial.com

Como podemos presuponer, cada usuario no realiza las mismas actividades en las redes sociales, ya que algunos lo dedican principalmente a ver qué hacen sus contactos y otros lo dedican a publicar en ellas, pero en cualquier caso ya no existe una diferenciación funcional entre los que publican y los que consultan, propia del internet original o la Web 1.0, sino que el mismo usuario puede ser consumidor de contenidos y publicador. A continuación se muestra un gráfico obtenido de una encuesta del *wearesocial* (2)

Ilustración 3. Actividades de los usuarios en las redes sociales Fuente: (2)

Como se puede apreciar en el gráfico anterior, la estadística indica que el uso principal es la mensajería, aunque el visionado de vídeos y escuchar música es muy demandado por los usuario y creciendo (7). Destaca también la información acerca de los contactos, cuestión que se ha convertido en una verdadera práctica habitual en todos los ámbitos, la de obtener información inespecífica sobre las personas, hecho este último muy controvertido, desde el momento en que la información se dispone de forma estática, perenne, evidenciando las contradicciones de las personas en su desarrollo vital y haciendo florecer nuevos problemas de índole práctico. (8)

En cuanto a las redes sociales más utilizadas en España durante el año 2016, en primer lugar nos encontramos Facebook seguida de Twitter, Google+ e Instagram. En las últimas posiciones de entre las más conocidas nos encontramos con LinkedIn y Pinterest. (2)

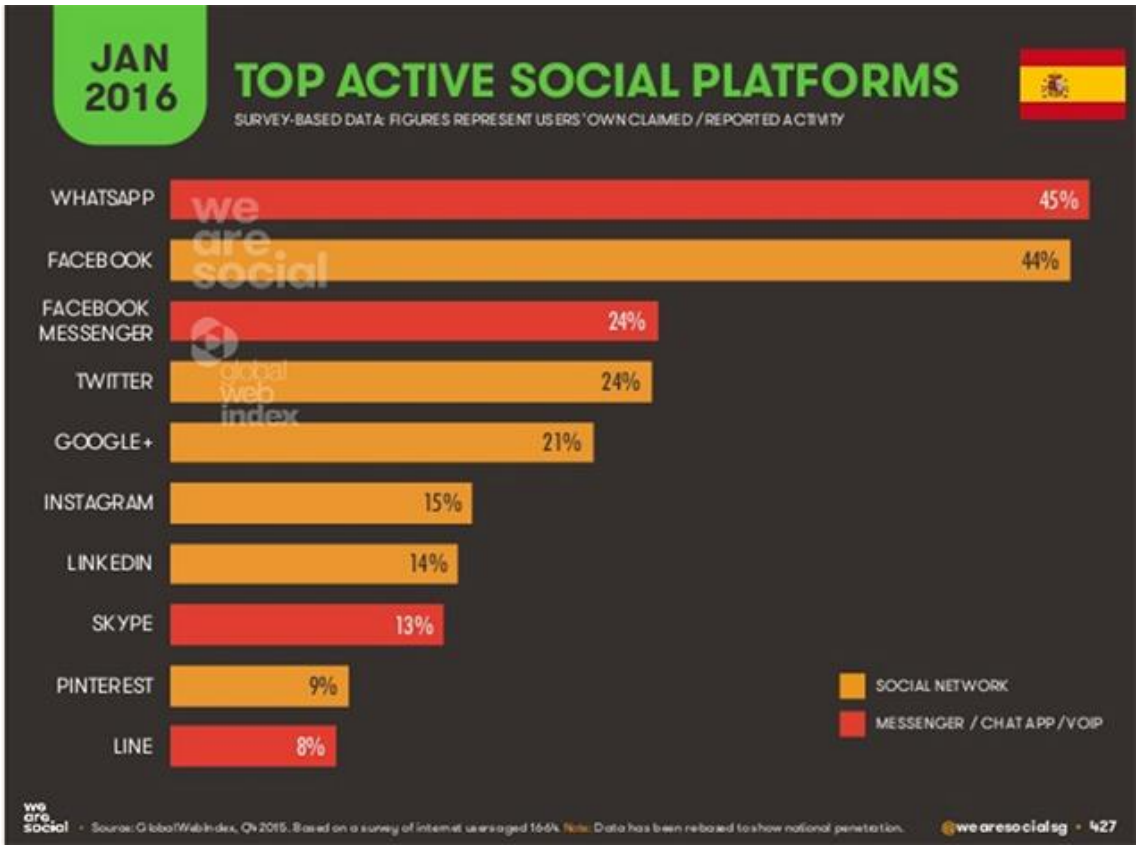


Ilustración 4 .Uso de las redes sociales Fuente: www.wearesocial.com

El número de usuarios que utilizan las redes sociales es un factor importante, puesto que exhibe la amplitud del mercado para los malhechores, agravado por el hecho de que un gran número de ellos no toman las medidas de protección adecuadas. Esto nos indica claramente que cuantos más usuarios tenga una red social, más probabilidad hay que se convierta en el escenario de un ataque, como demuestra la alta vulnerabilidad de Facebook en estos momentos (9).

A modo de ejemplo que evidencia la vulnerabilidad de las redes sociales, en agosto de 2016 aconteció uno de estos fallos (10), permitiendo a los malhechores cambiar la contraseña de cualquier cuenta. El problema se localizaba en el sistema de recuperación o cambio de contraseñas, ya que al solicitar una nueva contraseña, Facebook envía un código formado por 6 dígitos al propietario de la cuenta mediante un SMS o un email. Esto quiere decir que existe un máximo de un millón de combinaciones posibles hasta que se empiecen a repetir códigos. Si un hacker utiliza un programa para generar números aleatorios (combinando identificadores y

códigos) y realiza un ataque masivo al servidor de Facebook, podría llegar a modificar la contraseña de cualquier cuenta y hacerse con el control de Facebook.

Como se comentaba anteriormente, el uso de internet y de las redes sociales aumenta muy rápidamente; concretamente, más de la mitad de la población utiliza internet y un tercio está registrada en al menos una red social; esto hace a un grupo amplio de la población especialmente vulnerables a los ataques cibernéticos. Si bien el fin más habitual de un ataque cibernético no es perjudicar a unos usuarios concretos directamente sino a los nodos centrales de una organización, con el propósito de dar o destruir su reputación, éstos se ven afectados de forma colateral, puesto que al introducir su información personal en los sistemas que sustentan la aplicación de red social hace que se conviertan en las principales víctimas de un robo de datos.

Con este TFG se quiere realizar una auditoría a las redes sociales para hallar perfiles sospechosos, que puedan estar ayudando al malware a reproducirse y propagarse, encubiertos bajo la apariencia de enlaces a aspectos de su perfil que redirijan a webs con contenido malicioso.

Esta forma de ataque se está extendiendo de forma paralela al uso de las propias redes sociales, pues invitan a los usuarios a ser partes activas del visionado de webs que intentan captar información relevante de la que sacar un provecho ilícito y, lo que es peor, los usuarios se encuentran ávidos de ver contenidos cuando están en modo “ocio”, esto es, cuando disfrutan de forma pasiva de los contenidos que se le ofrecen.

4.2 ESCENARIO TÍPICO DE ATAQUE

Un escenario típico a la hora de realizar un ataque, ilustra este extremo: éste podría ser el robo de credenciales o datos de una red social, en la que, en primer lugar, el atacante elige a su víctima que puede ser tanto una empresa como una persona objetivo.

A continuación empieza a recabar información acerca de dicha víctima, mediante la monitorización de sus datos en las redes sociales, por ejemplo, identificar los hashtag que utiliza con frecuencia o las palabras que más utiliza. En definitiva, datos públicos que quedan registrados en los sistemas y en las aplicaciones.

El siguiente paso es la suplantación de la identidad del individuo o empresa mediante la creación de perfiles falsos, que habitualmente se detectan por los sutiles errores ortográficos o imágenes similares por provenir de traducciones automáticas y deficientes.

Si la cuenta creada tiene tráfico, es decir, los usuarios amigos del verdadero perfil añaden a su lista de amigos al perfil falso, se comienza a crear sitios web falsos para intentar un ataque phishing[1] o enlaces con malware para intentar otros tipos de ataque. Si este ataque tiene éxito, la víctima quedará desconcertada y los atacantes aprovecharán esta ventaja para hacerse con el control de más cuentas de la red social. A continuación se muestra una imagen a modo de breve resumen. (11)

Ilustración 5.Anatomía de un ataque a una red social Fuente: (11)

[1] Phising: Phishing o suplantación de identidad es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña, información detallada sobre tarjetas de crédito u otra información bancaria). El cibercriminal, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas (Fuente: Wikipedia)

5 OBJETIVO Y MOTIVACIÓN

El objetivo de este TFG es realizar una auditoría a las redes sociales para poder determinar la reputación de perfiles públicos, identificando el nivel de confianza sobre la base de unos determinados parámetros que habremos definido previamente. Para este fin, analizaremos el perfil de una red social en primer lugar con Maltego, herramienta especializada en minería y obtención de información a través de la recolección de metadatos. Además obtendremos información de otros sitios web con la misma herramienta para comprobar la amplia conexión de los datos en el universo Internet.

Un objetivo adicional consiste en la catalogación de las vulnerabilidades de las redes sociales, con lo que queremos especificar los tipos de ataques que se llevan a cabo frecuentemente en estos entornos y cómo intentar evitarlos.

Otro, objetivo, no menos importante, es la investigación de un perfil determinado. Concretamente determinaremos si se trata de un perfil social falso o no, esto es, si corresponde a una persona determinada o se trata de un señuelo específicamente diseñado para un fin espurio. Posteriormente, procederemos a analizarlo y categorizarlo para determinar su reputación.

Una de las principales motivaciones que subyacen en este trabajo es la de estudiar la seguridad en las redes sociales desde una perspectiva global, puesto que se trata de una herramienta de comunicación profusamente utilizada a diario tanto por mayores como por jóvenes y que se está convirtiendo en la vía de entrada predilecta para difundir malware en los dispositivos, del mismo modo que hace ya algún tiempo eran los gusanos insertados en programas difundidos por plataformas web o adjuntados en correos electrónicos. Sin duda, hoy las redes sociales representan el escenario de una fascinante disputa entre los agentes maliciosos y los elementos de seguridad de la información.

6 SEGURIDAD EN LAS REDES SOCIALES

Las redes sociales nos permiten realizar multitud de acciones, como comunicarnos con personas con las que hemos perdido el contacto, crear nuevas amistades, publicitar productos, difundir noticias, etc... Todo un sinfín de acciones con la comunicación de colectivos como base. Por esta razón, la mayoría de las personas crean perfiles en las redes sociales, como acción básica para participar en ellas, donde exhiben sus datos más personales, como el estado civil, sus estudios, lugar de trabajo, lugares que frecuentan e incluso fotografías propias y de familiares que pueden ser utilizadas por los malhechores para las más innovadoras formas de acciones maliciosas.

Como ya se ha explicado anteriormente Facebook es la más popular entre los usuarios, pues atesora más de 1.900 millones de usuarios, según el estudio de Trece bits (12). Le sigue a gran distancia LinkedIn, que cuenta con 500 millones de usuarios activos según (13), habiéndose situada en el ámbito de lo profesional, mientras que la primera se identifica como una aplicación de ocio y de contacto personal.

Actualmente en España 25,4 millones de personas utilizan internet, de las cuales un 81% de ellas utilizan las redes sociales, datos del segmento de edades comprendidas entre 16 y 55 años. (14)

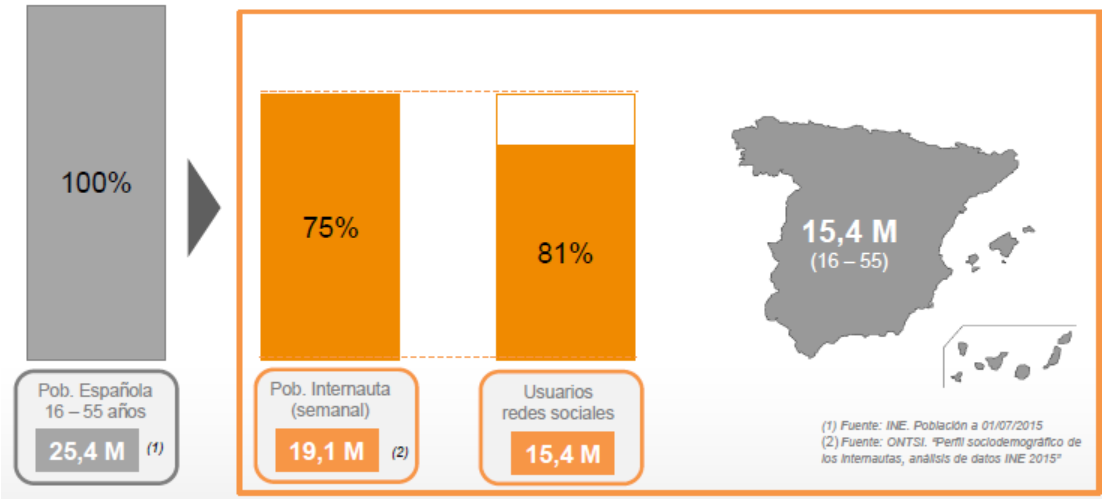


Ilustración 6.Uso de las redes sociales en España Fuente: IAB

Obviamente, no todos los usuarios tienen el mismo conocimiento sobre las tecnologías y su uso y esto lleva a un importante grupo de ellos a despreocuparse a la hora de configurar la privacidad de su perfil y tomar unas medidas de seguridad de la información mínimas adecuadas. Al no hacerlo correctamente, pueden sufrir algún tipo de ataque, por ello desde INCIBE se están creando campañas para concienciar a todos los usuarios de la necesidad de aumentar la privacidad de sus cuentas en redes sociales.

En efecto, si un perfil es consultado por alguna vía no deseada, un atacante o *hacker* puede obtener datos relevantes para configurar de forma definitiva un ataque malicioso, que no tiene por qué ser estrictamente informático, sino que simplemente pueden utilizar la información para conocer la hora de ausencia del hogar o eventos significativos de los usuarios objetivo por el que lograrían someterlos a cierto control.

Un ejemplo muy sencillo que revela la facilidad de lo anteriormente expuesto consistiría en ofrecer la amistad con un perfil falso, diseñado con características afines a las aficiones u ocupación laboral del usuario objetivo, de forma que una vez establecida la amistad, se desencadenen una serie de ataques con enlaces a descargas o información con malware inserto.

Por ello, antes de afrontar un análisis detallado de los ataques y sus posibles defensas, debemos tener en cuenta en primer lugar las tres dimensiones básicas de la seguridad de la información en cuanto a redes sociales se refiere (15):

- Confidencialidad: requiere que la información sea accesible únicamente a las entidades autorizadas. Es de vital importancia en las redes sociales porque un mal uso de la información podría traer graves consecuencias en la vida de las personas.

  Este aspecto es sumamente complejo en el mundo digital, puesto que la información, una vez difundida en un entorno, aunque sea limitado, puede ser objeto de nuevas redifusiones, perdiendo el control de la información original. La utilización de certificados digitales y tokens pueden limitar este

extremo, pero siempre se podrá limitar la capacidad de hacerlo y por tanto, dejar de ser objetivo de actividades ilícitas.

- Integridad: la información sólo puede ser modificada por las entidades autorizadas.
- Autenticación: posibilidad de un usuario de demostrar ser quién realmente dice ser.

Respecto a la privacidad de los usuarios, conviene resaltar que la confidencialidad de los datos y el anonimato de los propietarios son partes integrales de ella con lo que nadie debería poder acceder a la cuenta de otro usuario. Dicho esto, conviene decir que esto no es completamente cierto en la actualidad, debido a los virus u otro tipo de ataques que tiene con fin el robo de credenciales u otra información personal privada.

Uno de los primeros problemas que se vislumbran al acceder al universo de las redes sociales es el de la autenticación. En efecto, la certificación de la identidad es una cuestión de vital importancia cuando hablamos de seguridad en sentido amplio. La acreditación de la identidad de un individuo se realiza de distintas formas en cada país, pero siempre se deben buscar elementos (certificado de nacimiento, libro de familia, etc...) que certifican que un individuo es quien dice ser. En el mundo digital, la identidad digital se certifica en la actualidad en nuestro país con el certificado electrónico o DNI digital basado en la identidad real obtenida como se mencionaba anteriormente (16). En España, el proceso de obtener la identidad digital requiere el suministro por un organismo público que dispone de nuestra identidad real del certificado que establece la correspondencia de la identidad real y la digital. Un cuestión importante por el que debe velar la gobernanza de Internet es ésta; en efecto, siendo una red global, supraestatal, ¿son todos los certificados expedidos por cualquier país válidos para los propósitos de la red?

En cualquier caso, en las redes sociales no existe de momento ningún tipo de acreditación formal de los usuarios particulares ni de los entes jurídicos, esto es, ni los nombres, ni los datos ni los accesos acreditan que una persona es quien dice ser. Desde esta perspectiva, se puede adivinar el espacio de inseguridad caótica del que

hablamos: la red social se convierte en un juego de cartas en el que todos falsean sus jugadas, pero dónde se requiere confidencialidad para no revelar el farol y que el juego sea entretenido. Y es aquí donde los malhechores gozan de su espacio natural, explorando los espacios de conexión con la realidad de los usuarios.

Por ello, no es de extrañar que uno de los principales tipos de ataque aproveche estas vulnerabilidades para romper la privacidad, despojando a un usuario de su identidad mediante la creación de un perfil falso que no corresponde al usuario original o apropiándose del perfil original y privando a su usuario legítimo de toda la comunicación social con él.

De aquí en adelante, centraremos nuestra atención en la información que puede ser rastreada en las redes sociales, esto es, aquella información que sin ser pública se puede conseguir de forma indirecta. La razón para ello es que desde el punto de vista de la exposición de los datos, no parece existir una privacidad restrictiva, lo que hace que estos sean muchos más fáciles de ser sustraídos de lo que la aplicación inicialmente presume.

Aunque las redes sociales ofrecen una configuración de la privacidad acorde a los deseos del usuario, los datos son fáciles de rastrear desde el momento en que el grado máximo de protección que permiten no es muy fuerte, pudiendo fácilmente un atacante robar datos con intenciones espurias. Es decir, en el corazón de las redes sociales, nos encontramos diferentes lenguajes que son utilizados para aportar seguridad y privacidad a las redes sociales, aunque no aseguran completamente la red social ante un ataque. Uno los lenguajes utilizados para almacenar datos es XML (*eXtensible Markup Language* o *Lenguaje de Marcado Extensible*), este lenguaje carece de las medidas mínimas a la hora de gestionar la privacidad de los datos, pero existe un conjunto de estándares que tratan de gestionar la privacidad, llamados P3P (*Platform for Privacy Preferences*) que son utilizados por Facebook entre otros, aunque existen herramientas que consiguen saltarse estos estándares de privacidad y obtener datos privados con lo que no aseguran una privacidad total de los datos.

En efecto, las redes sociales contienen datos de valor inestimable, por lo que estos perfiles son utilizados, entre otras cosas, para orientar los anuncios a unos usuarios determinados con un claro objetivo comercial de tipo invasivo, especialmente grave cuando se trata de menores y adolescentes, que pueden ser afectados por estas prácticas. Obviando este último problema, no por su alcance ni por su gravedad, sino por ser objeto de otras consideraciones fuera del alcance de este documento, la propia utilización comercial de los datos hacen que su privacidad no pueda ser restrictiva.

Además, han surgido numerosas controversias al respecto de los usos comerciales de las redes sociales, principalmente debido a que algunas agencias utilizan dichos datos para emprender actividades ilegales, como traspaso de datos entre compañías, etc. También conviene destacar que, por el contrario, en otros casos como en los Países Bajos, las redes sociales han sido utilizadas para investigar la delincuencia organizada.

6.1 CIBERSEGURIDAD O SEGURIDAD DE LA INFORMACIÓN

En la actualidad, ha aumentado exponencialmente el número delitos que se cometen en la red según un estudio sobre *cibercriminalidad* realizado en España en el año 2015, en el cual se realizaron 60 mil delitos informáticos, entre los que se encuentran: fraude informático, falsificación, delitos sexuales, amenazas, etc. (17)

Esto ha hecho que la red haya ocupado un lugar preferencial en los intereses de los servicios de seguridad, la policía y los servicios de seguridad de los estados, ante el vertiginoso crecimiento del número de ataques que están afectando drásticamente a la seguridad de los usuarios en internet. De este extremo, de la seguridad de los usuarios, se encarga la ciberseguridad, que de acuerdo con ISACA (Information Systems Audit and Control Association) podemos decir que es:

"La protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados"

Por lo tanto la ciberseguridad tiene como foco la protección de la **información digital** que está presente en los sistemas interconectados, es decir, en todos los sistemas que permanecen conectados a internet. La ciberseguridad se refiere generalmente a la capacidad de controlar el acceso a las redes, sistemas de información y todo tipo de recursos de información.

Los principales objetivos de la ciberseguridad son: prevenir, detectar, responder y recuperarse frente a un ataque, aunque el más importante es prevenir que un ataque pueda realizarse con éxito.

En general, se podría decir que la ciberseguridad se refiere a métodos de uso, procesos y tecnologías para prevenir, detectar y recuperarse de daños a la confidencialidad, integridad y disponibilidad de la información en el ciberespacio.

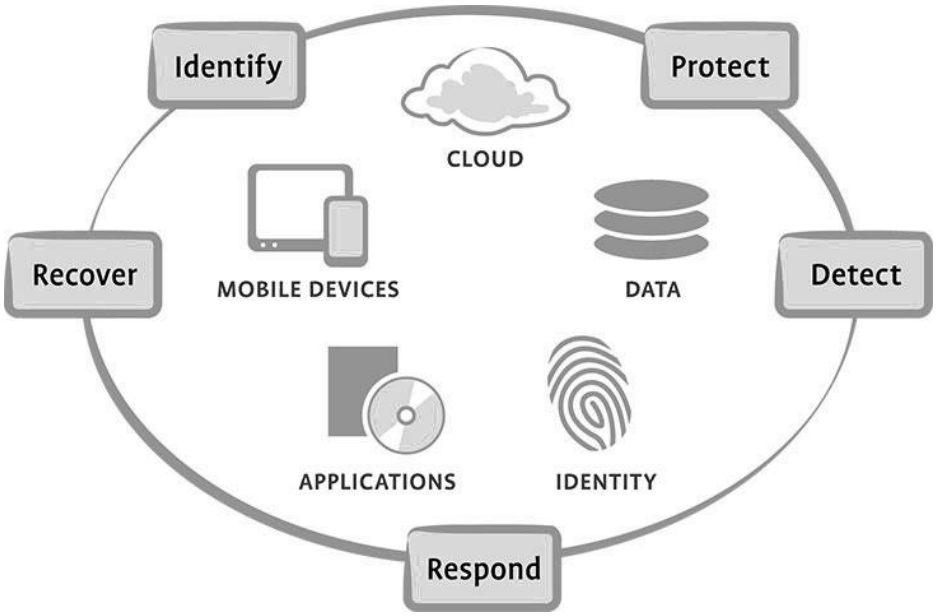


Ilustración 7.Dimensiones de la ciberseguridad

En cuanto a la seguridad de la información en las empresas, se puede decir que su propósito es el de reducir los riesgos ante actividades maliciosas, es decir, la Seguridad de la Información, según la **ISO27001**, se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan, estos pueden ser:

- Electrónicos
- En papel
- Audio y vídeo, etc.

La principal diferencia respecto a la ciberseguridad, es que no solo se encarga de la protección de la información en formato digital, sino también en los aspectos físicos, por lo que su alcance es mayor. Por lo tanto, sin importar los límites de cada concepto, el objetivo principal es de la seguridad de la información es proteger la información, independientemente de que ésta pertenezca a una organización o si se trata de información personal.

En resumen, hoy en día todos los organismos públicos y privados, a través de las normativas ISO, ENS, LOPD, etc. y un sinnúmero de leyes estatales y europeas están intentando crear un ecosistema confiable de tratamiento de la información, que al disponer las redes sociales en el centro de los intercambios informacionales, se quiebra de forma definitiva, siendo éste el motivo del fracaso de las redes sociales como herramientas oficiales de tramitación o comercialización y limitándose a funciones de ocio y entretenimiento.

Pero la interconexión de Internet hace el nivel de seguridad lo marque exactamente el punto más débil y convirtiéndose por ende, las redes sociales, en el talón de Aquiles de los sistemas de información. De ahí la importancia del estudio detenido del binomio seguridad-redes sociales.

6.2 ¿Y LA CIBERDEFENSA?

La ciberdefensa es un subconjunto de la ciberseguridad que se podría definir como: “La capacidad de asegurar y salvaguardar la prestación de los servicios, confidencialidad, integridad y disponibilidad, proporcionados por los Sistemas de Información y Comunicaciones en la fase de operación de los sistemas en producción, en respuesta a posibles inminentes acciones maliciosas originadas en el ciberespacio” según el Manual de Seguridad de las Tecnologías de la Información y Comunicaciones CCN-STIC- 400. (18)

En definitiva la ciberdefensa se encarga de hacer frente a los ataques, pero para ello es necesario que estos sean previamente analizados y procesados a una velocidad que permita tomar decisiones y actuar de una forma rápida. En cuanto a esta, tiene unas capacidades que se clasifican en tres tipos:

1. **Defensa**, medidas para la detección, reacción y recuperación frente a un ataque.
    a. Obtención de datos
    b. Procesado de datos
    c. Detección de actividades maliciosas y malware
    d. Análisis de actividades maliciosas
    e. Restauración de la información
2. **Inteligencia**, medidas en cuanto al análisis de los datos, recopilación de información.
    a. Obtención de la información de fuentes abiertas
    b. Análisis de malware
3. **Respuesta**, medidas y acciones ante una amenaza o para mitigar los efectos de un ataque.
    a. Prevención y eliminación de ataques malware
    b. Respuesta al ataque
    c. Hacking ético
    d. Defensa activa

Resumidamente, la ciberdefensa es la encargada de contrarrestar, proteger y mitigar los efectos de un ataque.

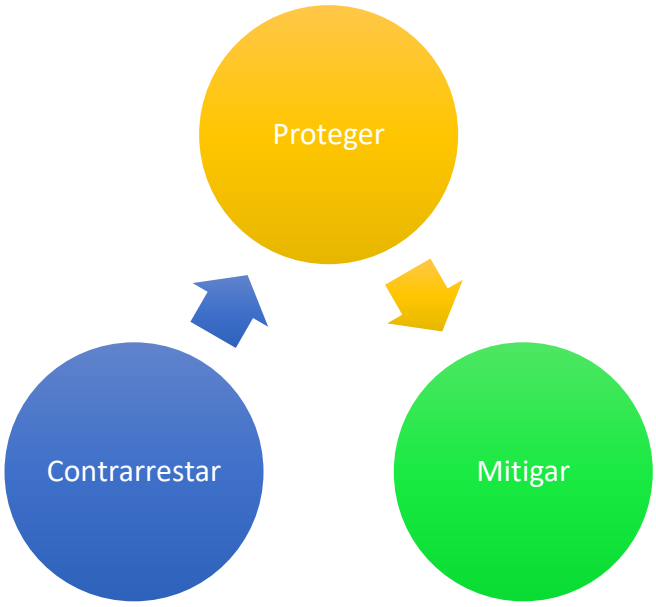


Ilustración 8.Funciones de la ciberdefensa. Fuente: slideshare

Anteriormente se nombraron las capacidades de la ciberdefensa, y una de las actividades que se realizan es precisamente la obtención de información de fuentes públicas. En el caso de la ciberdefensa se realiza para plantear un plan de defensa, pero las herramientas de defensa también pueden ser utilizadas para realizar un contraataque. En efecto, antes de proceder a un contraataque se debe obtener toda la información posible, normalmente, se obtiene la pública con herramientas especializadas en ello ya que dicha información puede ser consultada por cualquier usuario.

En el apartado 10 en el cual trataremos Maltego, se realizarán una serie gráficos en el cual se mostrará la información obtenida acerca de los mensajes peligrosos que se localizan en algunos perfiles.

7 TIPOS DE ATAQUES Y MALWARE EN LAS REDES SOCIALES

Anteriormente hemos hablado de la ciberseguridad y de la seguridad en las redes sociales, ya que para mitigar el malware en las redes sociales, debemos intentar eliminar su propagación entre los usuarios. Por ello, en este apartado nos centraremos en los principales tipos de ataques que existen a las redes sociales y cómo se nos presentan los diferentes tipos de malware en éstas.

En un primer análisis, dependiendo de la finalidad del ataque, estos se pueden clasificar en ataques lógicos y ataques físicos (19). Los primeros provocan amenazas a la información de los usuarios y al software, mientras que los ataques físicos presentan amenazas a los medios físicos, tales como servidores, ordenadores, etc.

Profundizando más en esta clasificación, dentro de los ataques lógicos tenemos: monitorización, que consiste en el robo de los datos a través de una herramienta software sin que el usuario lo note; ataques de autenticación, que consiste en la suplantación de la identidad a través del robo de credenciales, a este tipo de ataques pertenecen el DDoS (Denial of Service) y Man in the Middle.

Los ataques físicos se clasifican en desastres naturales, amenazas ocasionadas por los seres humanos tales como incendios y disturbios, sabotajes externos e internos.

Como se ha indicado en el párrafo anterior hay una forma de obtener datos de una red social sin atacarla directamente que se realiza recolectando datos, para ello se rastrean las listas de perfiles públicos, puesto que no requieren ninguna cuenta para acceder y son rastreadas rutinariamente por los motores de búsqueda. Por tanto, se trata de una operación habitual, no invasiva, pero que ofrece una riqueza de información suficiente para iniciar un ataque.

Uno de los principales bugs de seguridad de Facebook a través del cual se podría rastrear la ubicación de los usuarios que se comunicasen con nuestra cuenta se localiza en el uso de una Extensión de Google Chrome que trazaba las ubicaciones de los usuarios con los que la cuenta se intercambia mensajes. (20)

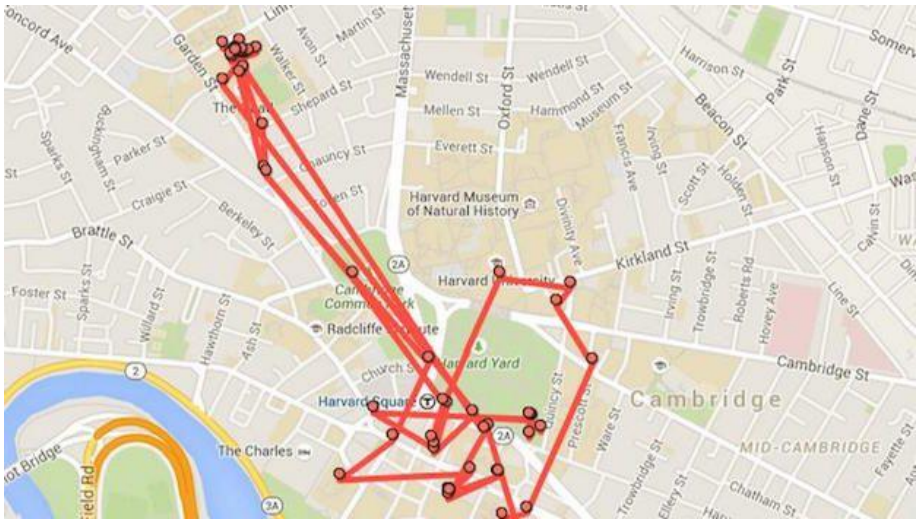


Ilustración 9.Noticia sobre un fallo en la privacidad de Facebook. Fuente: ComputerHoy

Otra forma de extraer datos de las redes sociales es atacar directamente a la red social desde dentro. Se pueden distinguir varios tipos:

- Ataques de violación de la privacidad
- Marketing Viral
- Ataques estructurales de la red
- Ataques Malware

En los siguientes apartados se describen con detalle este tipo de ataques y algunas noticias en las que se nos informa del alcance de ellos, para observar la dimensión que adquieren en la actualidad.

7.1 ATAQUES DE VIOLACIÓN DE LA PRIVACIDAD

En cuanto a los ataques directos a redes sociales en primer lugar explicaremos los ***privacy breach attacks*** que son los llamados ataques de violación de la privacidad. Este tipo de ataques se produce porque las llamadas terceras personas acceden a datos de usuarios. Nos encontramos con cuatro tipos distintos, dependiendo de quién o quienes lo realizan.

- Proveedores de servicios
- Terceras personas (usuarios)
- Aplicaciones terceras

En cuanto a los ataques realizados por los proveedores de servicios, podemos decir que estos ataques se realizan aprovechándose del poder que tienen de acceder a toda la información de los usuarios, y sobre todo los utilizan para orientar la publicidad, es decir, no es en sí mismo un ataque aunque desarrolla un efecto no deseado explícitamente para el usuario como puede ser incluirle en campañas publicitarias y venta de comportamientos comerciales no consentidos o consentidos de forma no conscientes por los usuarios.

Uno de los métodos de obtención de datos utilizado en la mayoría de las redes sociales es mediante los *tracking cookies*, estas almacenan las páginas que el usuario visita, las búsquedas, los gustos del usuario, etc. De esta forma se personaliza la publicidad al usuario, con lo que las redes sociales generan un beneficio por el hecho de almacenar datos de usuarios.

Desde el gobierno de España y, en general, en toda Europa, se está intentando disminuir el número de usuarios afectados por este problema. Para ello el gobierno promulgó en 2002 la Ley 34/2002, de 11 de julio de Servicios de la Sociedad de Información y Comercio Electrónico, conocida como la LSSI, encargada de regular el comercio electrónico online, y con ello la publicidad que se preveía entonces.

Según establece el artículo 10.3 de la LSSI, "la publicidad debe presentarse como tal, de manera que no pueda confundirse con otra clase de contenido, e identificarse de forma clara al anunciante" (21). Más concretamente, el artículo 21 de la misma cita en su punto primero "queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica que no hubiera sido solicitado o expresamente autorizada por el destinatario" (21). De esta manera, toda aquella forma de presentar la publicidad que se realice indirectamente es considerada como spam y, por una vía u otra, se está incumpliendo dicha ley, que se encarga de garantizar la seguridad de los usuarios en internet respecto al uso abusivo de la publicidad en internet.

Ya que el mayor problema al que se enfrentan los usuarios respecto a los ataques realizados por proveedores es el uso indebido de los datos para usos publicitarios o para la obtención de un beneficio económico que permita mantener a flote las

plataformas (redes sociales o aplicaciones web). Con esta ley se pretende dotar a los usuarios de una mayor seguridad jurídica a las transacciones realizadas a través de Internet, pero no garantiza la seguridad total de un usuario ante un envío masivo de correos spam, u otros ataques similares.

A continuación, se va a abordar el tema de los ataques realizados por terceras personas, que son aquellos realizados por usuarios externos a las redes sociales, es decir, hay usuarios que aparentemente están registrados en una red social, pero realmente no son los dueños legítimos del perfil, en el cual aparece su foto, así como sus datos, ya que están siendo víctimas de una suplantación de identidad.

Entre los ataques realizados por terceras personas pueden distinguirse varios tipos. El más habitual es la creación de un perfil falso de un usuario determinado, es decir, la clonación de su perfil y la realización de solicitudes de amistad con el fin de obtener información de un grupo de personas. Este tipo de ataques es muy efectivo ya que no hay ningún método de protección contra ellos, pues se accede de forma voluntaria por parte de los usuarios y no hay medida técnica para evitarlos, pues son perfiles como otro cualquiera.

Un ejemplo de ello se ha dado en Murcia, en marzo de 2017, donde dos menores han sido detenidos por la creación de un perfil falso de una menor, con el objetivo de desacreditarla y vejarla ante sus conocidos. (22)

Detenidos dos chicos en Murcia por difundir imágenes sexuales de otra menor por internet

En el ordenador de uno de los arrestados en la localidad de Beniel se habían creado los perfiles falsos de redes sociales donde se subían las imágenes de la chica

LA CRÓNICA Jueves, 23 de Marzo de 2017

G+1 Share 0 Twittear Menéame

Agente de la Guardia Civil trabajando en la 'operación Ninista'

Ilustración 10. Noticia de la falsificación de un perfil. Fuente: Periódico 20 minutos

Otro ataque muy parecido es la creación de un perfil falso de una persona que no existe en una red social, con lo que el atacante se hace con la identidad de la otra persona sin levantar ningún tipo de sospechas. Para ello, el atacante se crea un perfil falso de la víctima en una red en la que ésta no estaba registrada anteriormente y agrega a los usuarios de dicha red social que son amigos reales de la víctima en otra red social, la cual ha sido investigada previamente.

Este tipo de ataques han causado una gran alarma social en los casos en los que delincuentes han emulado perfiles sociales de adolescentes para obtener su amistad y seducirlas con intenciones claramente delictivas.

Actualmente se está incrementando la seguridad en las redes sociales ante el robo de un perfil, ya que existe la doble comprobación de seguridad que consiste en introducir un código que el usuario elige periódicamente. De esta forma, cada vez que el usuario accede a la red social, debe introducirlo, y con ello se evita en gran parte el robo de la cuenta.

En el caso de Facebook se puede configurar la privacidad para que nos envíe alertas cuando se inicie sesión desde un dispositivo nuevo, de forma que podamos controlar el acceso. Así mismo, nos ofrece también la posibilidad de incorporar la activación en dos pasos, de forma que, cada vez que alguien intente acceder a nuestra cuenta, tenga la necesidad de introducir un código que sólo el propietario real de la cuenta conoce.

En definitiva, Facebook intenta aumentar la seguridad y la privacidad de los usuarios y lucha contra el robo de cuentas, aunque apenas logra un difícil equilibrio entre la seguridad y la usabilidad.

Ilustración 11.Configuración de la seguridad en Facebook. Fuente: www.facebook.com

Al igual que Facebook, Twitter presenta mecanismos para ayudar a aumentar la seguridad de sus cuentas y prevenir los ataques cuyo fin es el robo de la identidad de un usuario o empresa.

Uno de estos mecanismos es la verificación en dos pasos, de forma similar al descrito anteriormente, en el que la red social envía un mensaje SMS con un código al usuario cada vez que se intente acceder desde un dispositivo desde el que no se hace habitualmente, es decir, se puede acceder únicamente utilizando la contraseña desde los dispositivos en los que se mantiene la sesión abierta, que normalmente suelen ser el ordenador personal y el dispositivo móvil habitual.

En el caso de otras redes sociales se adolece de mecanismos tan fiables ante este tipo de ataques, aunque se puede frenar su avance alertando a los usuarios del uso indebido de su cuenta.

Otro tipo de ataques que es muy común en nuestras redes sociales son los realizados por aplicaciones externas a la red social, es decir, aplicaciones que poseen acuerdos con las redes sociales para permitir autenticarse en ellas sin la necesidad de un registro previo, utilizando los datos que se han introducido en la red social. Para ello, utilizan los datos de usuario de las redes sociales con las que previamente

han realizado un acuerdo sin restricción alguna, esto es, se establece una concesión directa entre la aplicación y la red social por el que se ceden los datos del usuario.

Un gran porcentaje de los internautas acceden a páginas externas a las redes sociales con las credenciales que han introducido en éstas; en efecto, habitualmente nos encontramos con el típico mensaje: "Inicia sesión con Facebook" u otra red social, entre las que destacan Google+, Facebook y Twitter como medios de autenticación más conocidos.

Cuando el usuario se registra con Facebook, nos aparece una pantalla en la que debemos aceptar los permisos para que se produzca el inicio de sesión, en el caso de Google+ respecto a la misma página web (menéame), pero no se nos informa directamente de los datos que estamos cediendo ni por cuanto tiempo ni si el propósito de los mismos está limitado a la autenticación exclusivamente.

En la imagen siguiente, se muestra el mensaje que Facebook nos muestra al intentar iniciar sesión en una página web con el perfil de esta red social, en este caso la muy conocida *Menéame*. En el caso de pulsar sobre *Continuar como...* El usuario acepta el consentimiento de cesión de los datos.

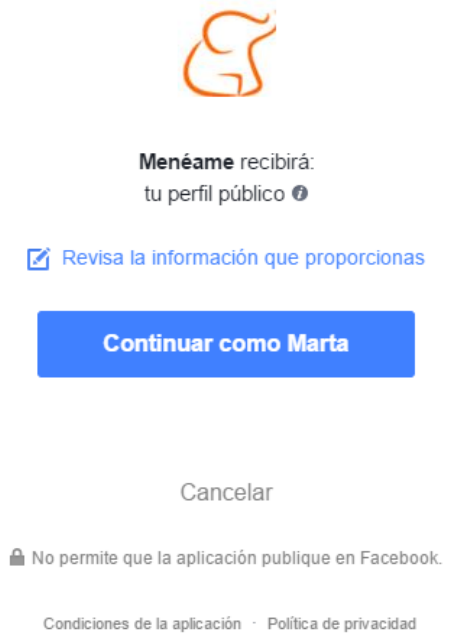


Ilustración 12.Verficación datos cedidos a otras fuentes. Fuente: www.facebook.com

En este mensaje se nos permite ver la información que el usuario proporciona a la aplicación externa. En este caso, estamos ofreciendo nuestro nombre y apellidos, edad, foto, sexo y otra información pública, todo lo cual es absolutamente desconocido para el usuario.

Ilustración 13.Datos cedidos a otras fuentes. Fuente: www.facebook.com

En los siguientes párrafos se va a abordar el caso de Facebook; se explicará de una forma breve algunos de los de detalles de la política de privacidad de ésta a la hora de utilizar el inicio rápido en una aplicación externa a Facebook.

Desde la plataforma *developers* de Facebook se nos indica cómo añadir a nuestra propia página web esta técnica de inicio de sesión y se muestran los datos que el usuario cede a esta página web. Entre ellos se encuentran (23):

- Email
- Perfil público
    - Nombre y apellidos
    - Edad
    - Sexo
    - Localización
    - Identificador de Facebook.
- Fotos del perfil de usuario
- Post realizados por el usuario
- Amigos

En dicha página se nos muestra un mensaje en el que se indica que "La aplicación puede utilizar este permiso sin necesidad de que Facebook lo revise." (23) Por tanto, se nos informa que una aplicación web puede obtener todos los datos cuyo permiso no está revisado por Facebook sin que éste se percate.

Por el contrario, Facebook obliga a todos sitios web a cumplir su política de privacidad, entre los cuales destacan los siguientes artículos (23):

1. *Puedes usar la información de la cuenta de acuerdo con tu política de privacidad y otras políticas de Facebook. Todos los otros datos solo se pueden usar fuera de tu aplicación, luego de obtener el consentimiento explícito del usuario.*
2. *Obtén el consentimiento de las personas antes de utilizar sus datos en un anuncio.*
3. *Protege la información que recibas de nosotros contra el acceso, el uso o la divulgación no autorizados. Por ejemplo, no uses los datos que obtuviste de nosotros para ofrecer herramientas que se usen para la vigilancia.*
4. ***No transmitas, solicites ni recopiles nombres de usuario ni contraseñas de Facebook.***
5. *No transfieras ningún dato que recibas de nosotros (incluidos los datos anónimos, totales o derivados) a redes publicitarias, agentes de datos u otros servicios de publicidad o monetización.*

En los párrafos anteriores se han mostrado algunos artículos que se encuentran la política de privacidad de Facebook, donde nos informa que cuando un usuario inicia sesión en una aplicación externa, ésta no está obteniendo sus credenciales, pero tiene un acceso ilimitado a gran cantidad de datos, tales como sexo, edad, ciudad de nacimiento, que pueden ser utilizados a la hora de realizar un ataque, Y es precisamente este aspecto el que supone un gravísimo problema para los usuarios, ya que no hay una forma de saber si las aplicaciones a terceros están utilizando datos de usuarios de una forma ilegal. Como resultado, estos deben confiar en las aplicaciones para declarar correctamente la información que necesitan.

Además, como no hay forma de supervisar cómo las aplicaciones manipulan los datos personales de los usuarios, se deja la puerta abierta para dichas las aplicaciones abusen de la información.

7.2 MARKETING VIRAL

En cuanto al marketing viral, se sabe que está basado sobre todo en el ***spam*** (correo basura)**,** aunque también nos encontramos con otras formas mucho más sutiles. En la actualidad, sobre todo en lugares como las redes sociales, hay una cantidad ingente de spam, el cual se suele hallar sobre todo en las publicaciones de usuarios que en la red social aparecen en nuestra lista de amigos. Esto hace que mayoría de los usuarios confíen en lo que ven en las redes sociales debido a que es un lugar "de su confianza", es decir, como la mayor parte de las amistades se encuentran presentes en las redes sociales, los usuarios más incautos a la hora de leer publicaciones de estos usuarios en los que confían apenas intuyen que puedan ser víctimas de algún tipo de ataque o que estén siendo *spammeados*.

El problema deviene cuando un usuario hace clic sobre uno de estos anuncios y visita una página que no sabe si realmente es segura o no y cree simplemente que por estar en una red social sí lo es.

Precisamente, la principal motivación por la que se diseñan los banner con spam es conseguir que el mayor número de personas hagan clic, consiguiendo con ello un mayor número de visitas a su página y de esta forma llegar a conectar con más usuario y así hacer llegar más lejos su publicidad. Este es el sistema de medición más clásico del marketing digital, por cuanto cada clic representa una visita y este es precisamente el objetivo del marketing digital y por el que las empresas están dispuestos a abonar grandes sumas de dinero.

En la actualidad el spam ha alcanzado un record de presencia en los emails y las redes sociales. Esta práctica representa ya casi dos tercios (65 %) del volumen total de correo electrónico en el mundo y, de este, entre el 8 % y 10 % pudo clasificarse en 2016 como malicioso, según reveló esta semana la tecnológica Cisco en su Reporte Anual de Ciberseguridad 2017.

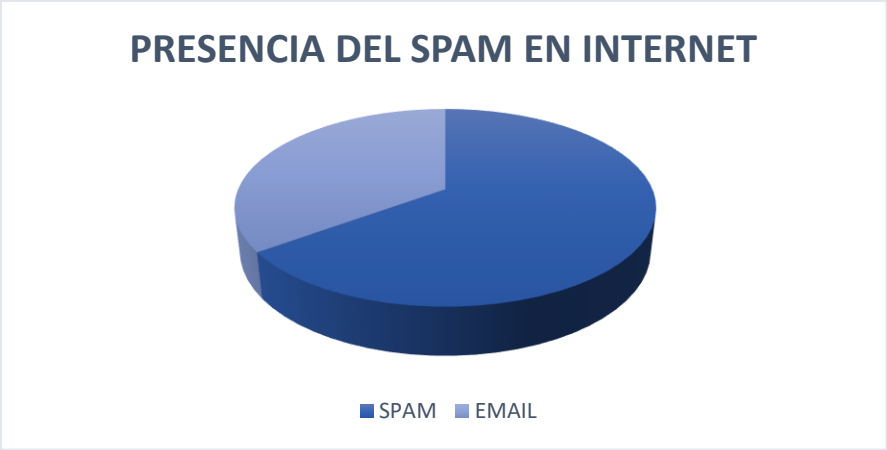


Ilustración 14.Spam en internet. Fuente: Reporte Anual de Ciberseguridad 2017, Cisco

Este aumento es debido a que ha aumentado el número de usuarios inexpertos, es decir, usuarios que todavía no tienen mucho conocimiento sobre internet con lo que no se preocupan de su seguridad. Simplemente se fían de lo que pone en internet y ellos son los que hacen clic en los mensajes de spam con lo que hacen que se propaguen.

7.2.1 Phishing

Un tipo de ataque del catalogado como marketing viral es el ***phishing*** (9)***,*** que consiste en hacer creer a los usuarios que están accediendo a una página cuando en realidad resulta ser una copia de ella, que es utilizada para obtener datos sensibles de los usuarios, tales como contraseñas, números de tarjetas de crédito, etc. Usualmente se trata de un formulario de recuperación o actualización de datos mimetizada con la empresa u organismo real.

Para ello, vamos a determinar el proceso de realización de un ataque phishing:

1. Creación de un sitio web similar al sitio original.
2. Envío del enlace del sitio web falso a un gran número de usuarios.
3. Ingreso de los datos por parte de las víctimas.
4. Robo de la información por parte del atacante.

Ilustración 15.Fases de un ataque Phishing Fuente: (9)

El phishing tiene una dimensión psicológica en la medida en que los atacantes aprovechan limitaciones en el conocimiento técnico o descuidos en las buenas prácticas de seguridad para engañar a los usuarios. Los ataques de phishing suelen iniciarse cuando el usuario hace clic en un enlace de un correo electrónico o una página Web que le lleva a un sitio falso, que normalmente ha recibido para aclarar una cuestión técnica, relato que suele ser convincente.

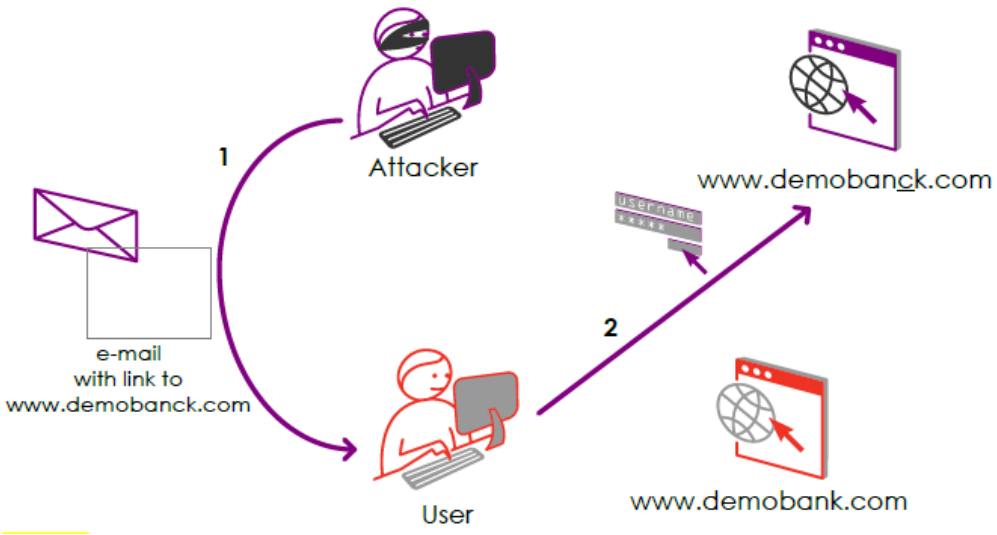


Ilustración 16. Phishing Fuente. www.safelayer.com

En general, a cualquier usuario no especialmente concienciado por la seguridad, le resulta difícil detectar que están intentando engañarle para que revele su credencial.

Por este motivo, es conveniente disponer de mecanismos de autenticación del sitio Web, con los que el usuario pueda reconocer fácilmente que el sitio al que se ha conectado es el legítimo y no una copia. Los certificados de servidor pueden ser una solución, pero la escasa implantación de esta solución y las continuas excepciones que los navegadores nos solicitan para acceder a sitios webs legítimos, hacen que se genere una situación confusa para el usuario.

En cuanto a la presencia del phishing, se puede decir que se localiza principalmente en el email, ya que los receptores se suelen fiar más, aunque en las redes sociales ha aumentado enormemente su presencia, asociada al registro de webs para visualizar vídeos o consultar contenidos específicos. Se pueden encontrar en muchas publicaciones que aparentan ser lo que en realidad no son, como puede ser incluso una página de *login* de una red social que resulta ser fraudulenta.

Al entrar en una página en la que nos pida credenciales debemos comprobar que su link es https: y no http, ya que https cifra los datos que suministremos, con lo que se aumenta la seguridad ante un robo. Ésta no es la única forma de evitar el

phishing, existen muchas otras, como por ejemplo el descrito anteriormente que hacen uso de certificados digitales en los que los sitios web certifican ser quién realmente dice ser. Las páginas fraudulentas carecen de este tipo de certificados y buscan otros servidores en los que apoyar sus fechorías.

En cuanto a las redes sociales es importante que a la hora de realizar un *login* comprobemos si está utilizando el protocolo SSL/TLS (capa de puertos seguros/ seguridad en la capa de transporte). En efecto, este protocolo está diseñado para permitir la transmisión de información sensible entre dos puntos de forma segura. (24). No obstante, determinados estudios de usabilidad confirman que este método no es suficiente, puesto que las técnicas de engaños visuales utilizadas por los atacantes son efectivas incluso para los usuarios más avanzados, es decir, como se explica en el apartado 7.2.1, las técnicas utilizadas para simular las páginas web, en el ejemplo que se muestra en dicho apartado, un engaño visual utilizado es el de cambiar la última "l" minúscula por una "i" mayúscula, así de esta forma simulan, la palabra PayPal, para intentar engañar a los usuarios.

Si cambiamos el tipo de letra utilizado, a la izquierda "Calibri" y a la derecha "Consolas", podemos observar que la palabra no está escrita correctamente, con lo que utilizando esta técnica se intentan realizar engaños visuales a la hora de realizar un ataque phishing.

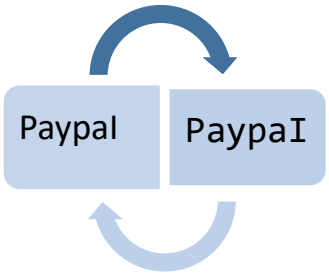


Ilustración 17. Ejemplo engaño visual phishing

En el artículo "Why Phishing Works" (25) se estimó que el 23% de los usuarios no hace caso de las señales de advertencia de los navegadores en la barra de direcciones o la barra de estado, lo cual conduce a decisiones de seguridad erróneas en el 40% de las ocasiones. Con lo que SafeLayer (26) proporciona una solución para los usuarios contra el phising, que consiste en que los usuarios deban elegir una imagen personalizada para que se muestre en el formulario de entrada de credenciales; cabe decir que dicha imagen es única para cada dispositivo y navegador, con lo que el atacante no podrá replicar dicha imagen de forma masiva o automatizada, puesto que esta imagen es distinta para cada usuario.

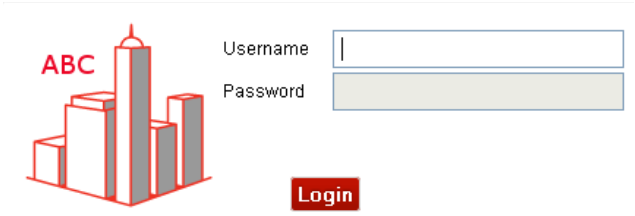


Ilustración 18. Imagen personalizada de Savelayer. Fuente: www.safelayer.com

En el caso de que un impostor consiga engañar al usuario y sustraer sus credenciales, intentará utilizarlas en un dispositivo diferente al dispositivo que el usuario utiliza habitualmente, con lo que el servicio de autenticación de SafeLayer podrá detectarlo.

Para la identificación de usuario se utiliza un método que utiliza *cookies*. En este método se pueden distinguir dos tipos de identificación:

- Identificación de dispositivo "simple", en la que se utiliza una *cookie estática* y/o una dirección IP para identificar el dispositivo.
- Identificación de dispositivo "compleja", en la que se utilizan cookies de un solo uso y se crea una huella digital (fingerprint) del dispositivo en la que se incluyen características de éste como información de su configuración, dirección IP, geolocalización, etc.

Esta solución permite al usuario registrar un número de dispositivos como propios, lo que significa que dichos dispositivos siempre van estar bajo la vigilancia del usuario, garantizando su identidad.

Como hemos visto en el párrafo anterior, utilizamos las *cookies* para identificar los dispositivos. Con ello combatimos el phishing, pero no así el *pharming*, que es un tipo de phishing más sofisticado y necesita otros métodos de mitigación.

Pharming consiste en un ataque phishing más profesional, en el que el servidor legítimo se ve comprometido y los accesos son redirigidos y capturados por el servidor malicioso, capturando las cookies. La solución de SafeLayer consiste en incorporar una capa de seguridad extra mediante el protocolo **One-time Double-cookie Protocol**, que consiste en el uso de dos cookies en el mismo uso (26), una de las cookies asociada al dispositivo y otra aleatoria generada por el servidor legítimo, temporal y asociada al dominio, para asegurar al usuario en todo momento ya que estas cookies son muy difíciles de imitar.

Un ejemplo de phishing muy conocido se realizó en 2016 engañando a cerca de 10.000 usuarios de Facebook en todo el mundo e infectó los dispositivos desde el que accedieron, después de recibir un mensaje de un supuesto amigo que aseguraba que otra persona lo había mencionado en la red social e hiciera clic para identificarla. (27).

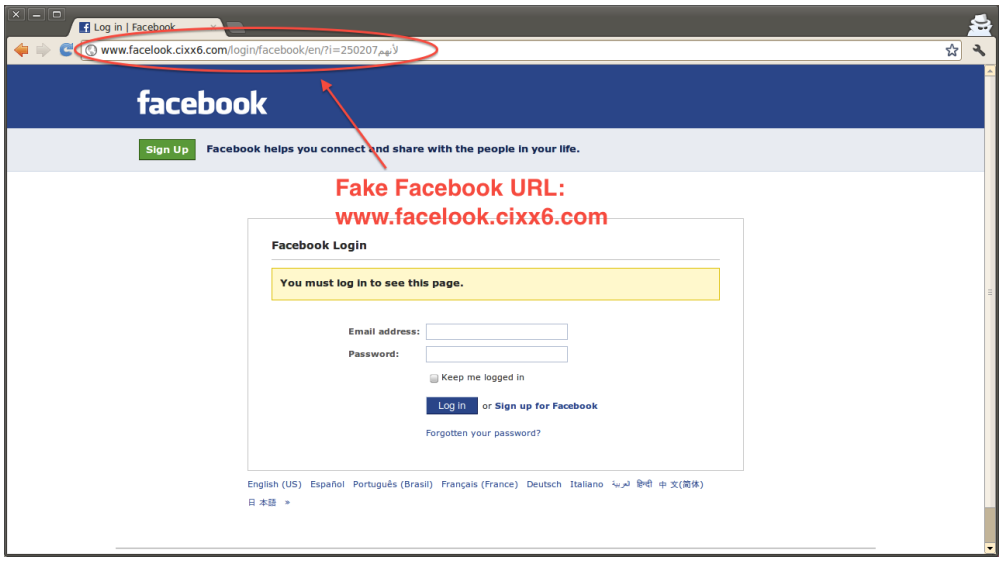


Ilustración 19.Phishing en Facebook. Fuente: Google

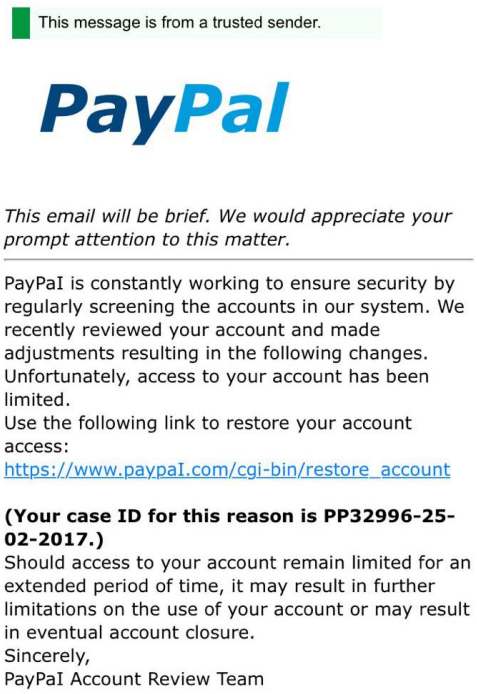
Los dispositivos comprometidos se utilizaron para secuestrar cuentas de Facebook, con el fin de propagar la infección a través de los propios contactos de la víctima y permitir otras actividades maliciosas. Las regiones más afectadas fueron América del Sur y Europa, además de Túnez e Israel.

Profundizando un poco más en dicho ataque, éste consistía en dos etapas. La primera, permitía descargar un troyano en la computadora del usuario que instaló, entre otras cosas, una extensión maliciosa del navegador Chrome. Esto daba paso a una segunda etapa, la toma del control de la cuenta de Facebook de la víctima, cuando ésta iniciaba una nueva sesión en la red social a través del navegador comprometido. Por el contrario, los usuarios de dispositivos móviles Android y iOS fueron inmunes, ya que el malware utilizó bibliotecas que no son compatibles con estos sistemas operativos móviles.

Otro gran ataque del tipo similar se realizó en marzo de 2017, pero, en este caso, el objetivo no era una red social en sí, sino la compañía PayPal. Este ataque consistía en el envío masivo de emails a los usuarios donde se les pedía que verificasen los datos de su cuenta.

A continuación se muestra un correo recibido en el que se ve claramente que dicho email no pertenece a la compañía. Para demostrarlo, vamos a analizar el mensaje para comprobar que efectivamente forma parte de un proceso de ataque y qué deberían realizar los usuarios frente a ellos.

A continuación se muestra una captura del email que muchos usuarios han recibido, entre ellas la que suscribe estas líneas.



This message is from a trusted sender.

PayPal

This email will be brief. We would appreciate your prompt attention to this matter.

PayPaI is constantly working to ensure security by regularly screening the accounts in our system. We recently reviewed your account and made adjustments resulting in the following changes. Unfortunately, access to your account has been limited.
Use the following link to restore your account access:
https://www.paypaI.com/cgi-bin/restore_account

(Your case ID for this reason is PP32996-25-02-2017.)
Should access to your account remain limited for an extended period of time, it may result in further limitations on the use of your account or may result in eventual account closure.
Sincerely,
PayPaI Account Review Team

Ilustración 20. Email phishing PayPal

En primer lugar se puede apreciar que el logo de la empresa tiene la intención de que los usuarios confíen sólo con verlo. Si el usuario continúa leyendo, se puede observar que en el cuerpo del mensaje hay faltas de ortografía referentes a la palabra PayPal, ya que los atacantes han intentado disimularlo cambiado una i latina mayúscula para hacerlo pasar por una l minúscula. Al final del primer párrafo nos indica que el acceso a nuestra cuenta es limitado. Como es de suponer, PayPal tiene todas las credenciales de todos los usuarios, pudiendo hacer uso de ellas, aunque esto no sea legal, con lo que llama la atención que al usuario se le pida que introduzca sus credenciales.

Un detalle importante que conviene resaltar es que aunque el enlace proporcionado es de tipo https, el resto del enlace nos re-direcciona a una página completamente en inglés (PayPal es multilenguaje así que si no fuese un ataque la página debería estar en este caso en español) que no es *paypal.com*.

Si un usuario detecta fallos ortográficos, si el enlace que acaba de abrir no corresponde con la página web en sí, es decir, si un usuario recibe un correo de Facebook, lo abre y en la URL no aparece la palabra Facebook, y sobre todo, el hecho

de que en el correo se indique que vuelva a introducir sus datos, debe borrar el email inmediatamente y bloquear al emisor de dicho mensaje ya que nos encontramos en un caso en el posiblemente se esté realizando un ataque phising. Las empresas y organismos hace tiempo que han abandonado la forma de solicitar aclaración, actualización o modificación de datos a través de correos o enlaces.

7.3 ATAQUES ESTRUCTURALES DE LA RED

Entre los ataques estructurales, esto es, que afectan al funcionamiento mismo de la red, tenemos los ataques ***Sybil*** (9) , en el cual el atacante puede contaminar un sistema distribuido. En este caso la infección se produce por la influencia que puede producir un ordenador con múltiples identidades falsas en un sistema de reputación, por lo que algunos de los nodos de la red pueden sufrir una usurpación de la identidad por el simple hecho de estar conectados a los nodos del atacante.

Este tipo de ataques tienen gran importancia en las redes sociales debido a que muchos usuarios interactúan con otros usuarios que están inmersos en redes P2P (Peer-to- peer), con lo que pueden conseguir que el ataque se propague fácilmente (9). Una forma de infectar una red social es mediante la creación de un número determinado de cuentas falsas y la infección de otras muchas a través de este tipo de ataque, lo que permite al atacante tomar el control las cuentas infectadas.

Las redes sociales suelen disponer de mecanismos para la prevención de estos ataques, ya que, al contrario de las redes peer-to-peer P2P, sólo los usuarios verificados pueden acceder a la red, con lo que pueden controlar adecuadamente este tipo de ataques.

7.4 MALWARE ATTACKS: ATAQUES MALWARE

"El malware (del inglés malicious software), también llamado badware, código maligno, software malicioso, software dañino o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario". Definición de malware. Wikipedia (28)

El malware se puede propagar a través de redes sociales a través de perfiles, interacciones y aplicaciones de terceros. El gusano ***Koobface*** es uno de los gusanos más notorios en las redes sociales. Es el primer malware que tiene un funcionamiento exitoso y continuo que se propaga a través de las redes sociales (9). Ejecuta un ataque automatizando los navegadores de Internet redirigiendo a sitios webs contaminados, para crear cuentas y desde ellas unirse a grupos y publicar mensajes, para así seguir propagando el virus. El objetivo final es conseguir obtener información relevante, como número de tarjetas de crédito.

Un mecanismo que se ha desarrollado para la prevención de estos gusanos se realiza utilizando cuentas en las redes sociales que monitorizan toda la información que pasa por ellas; para ello los propietarios de dichas cuentas deben agregar a un gran número de usuarios para poder monitorizar la mayor cantidad de datos y con ello evitar el ataque de estos gusanos.

En el año 2016 se descubrió un virus catalogado como *ramsomware* que infiltraba código en las imágenes y, posteriormente, estas eran publicadas en Facebook obligando a los usuarios a descargarlas. Cuando esto ocurría, el dispositivo del usuario era infectado por ImageGate (29).

Si bien los descritos hasta este punto son solo algunos ejemplos, se puede aventurar que las redes sociales están llenas de malware que exigen tener mucho cuidado con las publicaciones que se comparten.

El *ramsomware* es un tipo de software malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado y pide un rescate a cambio de quitar esta restricción (30). Algunos tipos de *ransomware* cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate.

En mayo de 2017, se produjo un tipo de *ransomware* llamado “Wannacry” (30), el código malicioso ataca una vulnerabilidad descrita en el boletín MS17-010 en sistemas Windows que no estén actualizados de una manera adecuada, principalmente Windows XP y Windows 7, como se puede ver en la ilustración 21, los sistemas operativos superiores a este como Windows 8, etc. han sido afectados en

menor medida, es decir, el número de ordenador afectados ha sido mucho menor, debido a que muchos de ellos contaban con un parche que no permitía afectar a los dispositivos con este virus.

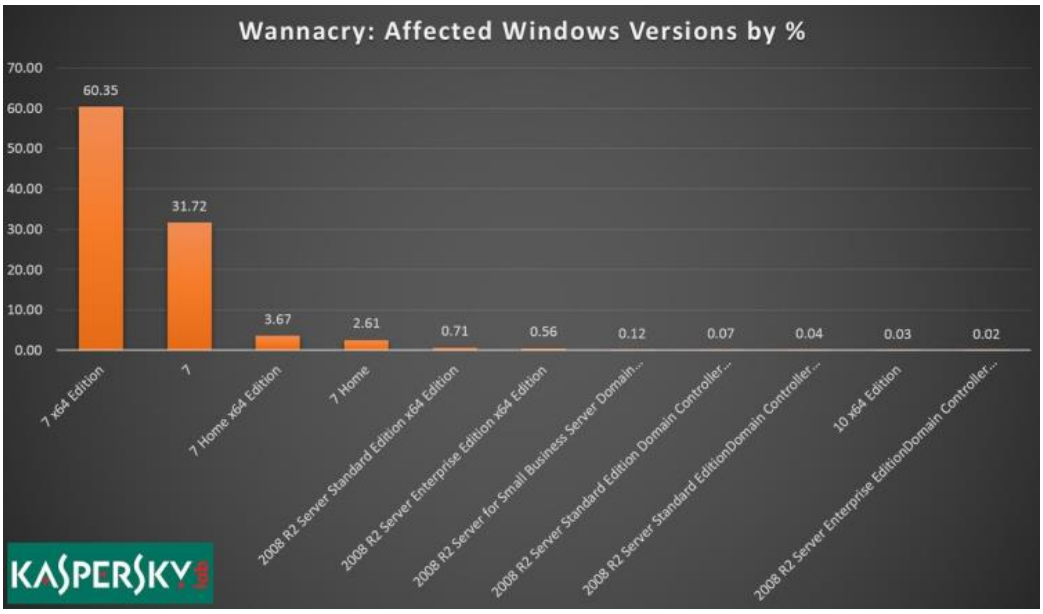


Ilustración 21. Sistemas afectados por Wanna Cry. Fuente: Kaspersky

El ataque provocó el cifrado de datos en más de 75 mil ordenadores por todo el mundo afectando, entre otros, a:

- Rusia: red semafórica, metro e incluso el Ministerio del Interior
- Reino Unido: gran parte de los centros hospitalarios
- Estados Unidos
- España: empresas tales como: Telefónica, BBVA, Gas Natural e Iberdrola

En la ilustración 22, se puede apreciar el alcance de este ataque, que se basaba en encriptar y bloquear los archivos de los dispositivos para posteriormente pedir un rescate. Dicho ataque afectó a gran parte de Europa, Asia y América y tuvo una enorme repercusión en los medios de comunicación.

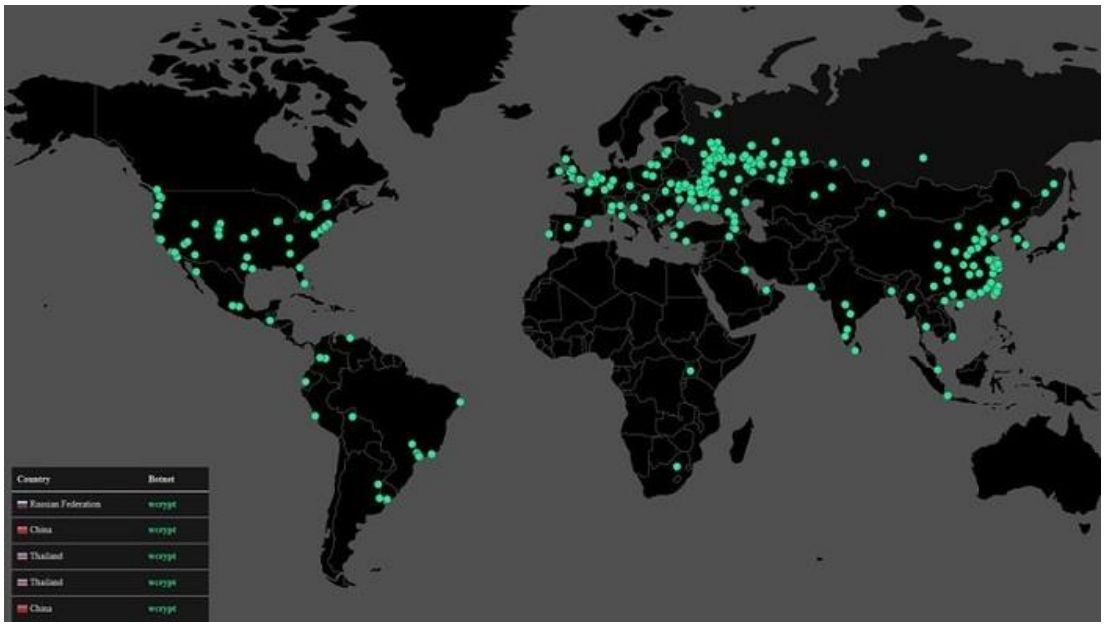


Ilustración 22. Alcance ramsomware mayo 2017. Fuente: applesencia.com

8 PRIVACIDAD EN LAS REDES SOCIALES

En la actualidad, el uso de las redes sociales se encuentra en pleno apogeo y la mayoría de los individuos las conoce o pertenece a alguna de ellas. Según datos del estudio anual de las redes sociales en 2016 del IAB (2), en España, el 81% de las personas que utilizan dichas redes tienen entre 16 y 55 años, aunque la edad no es un factor demasiado importante a la hora de tener en cuenta la privacidad de estos usuarios en dichas redes sociales.

Un factor importante a la hora de determinar la privacidad de una cuenta, es el uso que hace cada usuario de las redes sociales, es decir, un gran porcentaje de los usuarios es seguidor de usuarios famosos, como *celebrities, blogueros, etc.,* en el que lee y realiza seguimiento de sus actividades y publicaciones, los conocidos como *influencers (*personas con mucha influencia en las redes sociales)*,* marcas, tiendas, etc. (2)

Como hemos explicado anteriormente, el factor que marca el nivel de privacidad de un usuario es el uso que hace éste de las redes. El nivel de privacidad recomendado para un usuario cualquiera es el nivel más restrictivo. Con ello evitaremos que se convierta en un objetivo fácil de los hackers, puesto que, de no fijarla en este nivel, se convierte en una víctima potencial, es decir, la mayoría de los perfiles de las redes sociales son llevados por usuarios que no tienen gran conocimiento en informática, por lo que es relativamente fácil que caigan en las trampas de los hackers.

Dependiendo del tipo de perfil que tengamos, deberemos tener una privacidad más restrictiva o menos. Actualmente los *blogueros o bloggers* son personas que se están dando a conocer. Estas personas publican en un blog o tienen un canal en YouTube y generalmente no son muy famosos, con lo que a este tipo de personas no les interesa tener una privacidad restrictiva; antes al contrario, normalmente tienen un perfil público que expone sus intenciones de darse a conocer en las redes sociales.

En la imagen siguiente podemos ver cómo configurar la privacidad en tres redes sociales como Facebook, Twitter y Tuenti, la última de éstas, ha desaparecido como

red social. Comenzaremos examinando la privacidad en Facebook, ya que nos ofrece muchas posibilidades.

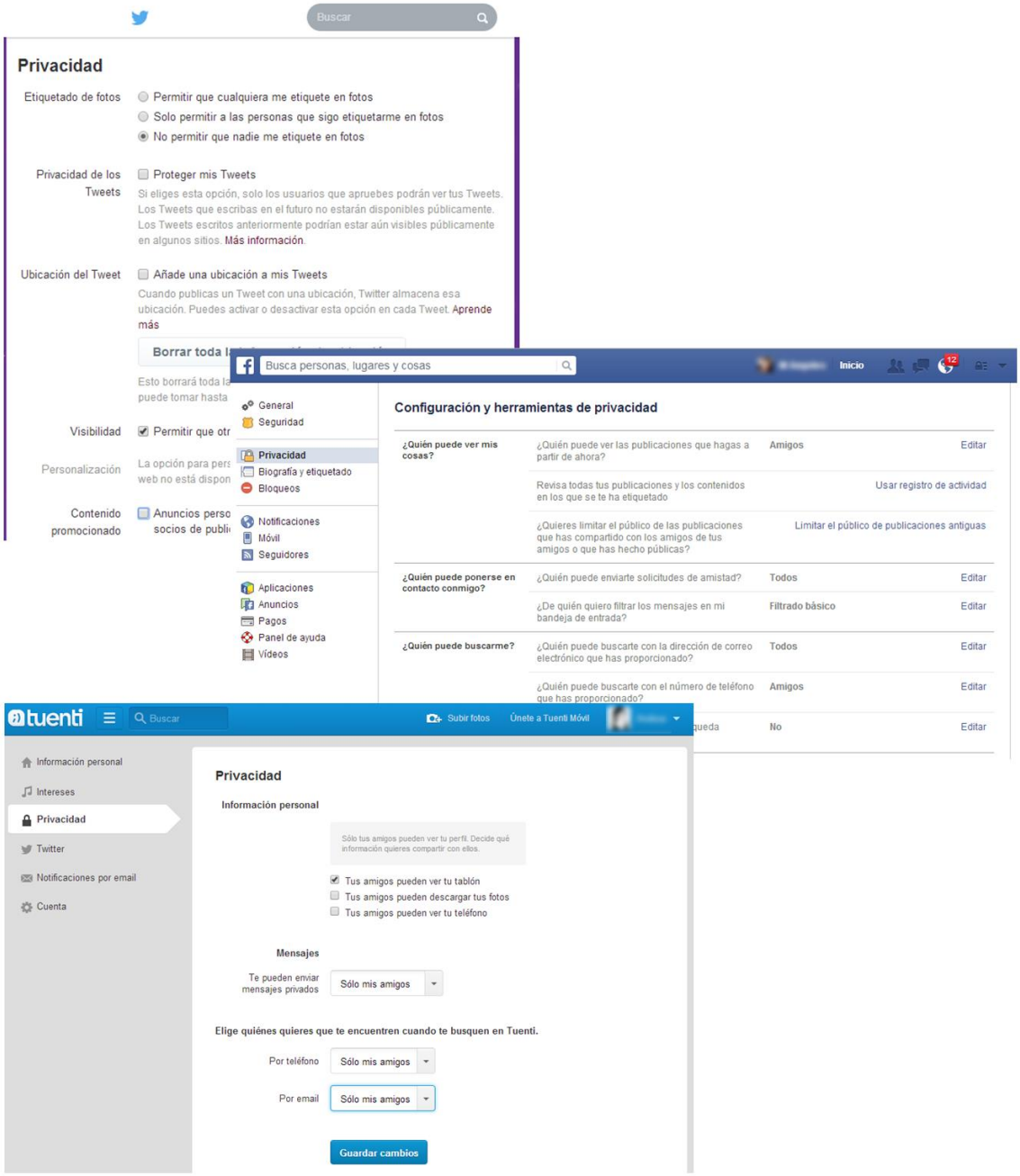


Ilustración 23.Privacidad en redes sociales Fuente: (31)

En primer lugar, en Facebook se nos pregunta quién puede consultar nuestras publicaciones. Si el usuario quiere que sólo sus amigos las vean, restringirá su perfil a sus amigos, es decir, tendrá un perfil privado; por el contrario, si no se restringe en absoluto, el perfil seguirá siendo público por defecto.

La parte más importante para evitar que personas externas a nuestro entorno nos encuentren en Facebook es restringiendo qué usuarios pueden buscar dicho perfil. Para ello la red social ofrece un apartado en el que hay que hacer especial hincapié, concretamente el último apartado de la interfaz de configuración, donde se indica lo siguiente: ***"¿Quieres que los motores de búsqueda fuera de Facebook enlacen tu perfil?"***. Este es el método principal de los malhechores para buscar víctimas, escribiendo un nombre de usuario en un motor de búsqueda y obteniendo su perfil de forma directa. Para evitar este extremo, esto es, ser encontrado fuera del entorno de Facebook, debemos desactivar esta opción, siguiendo siempre la política de utilizar una privacidad restrictiva.

Configuración y herramientas de privacidad

¿Quién puede ver mis cosas?	¿Quién puede ver las publicaciones que hagas a partir de ahora?	Amigos	Editar
	¿Quién puede ver tu lista de amigos? Recuerda que tus amigos controlan quién puede ver sus amistades en sus propias biografías. Si las personas pueden ver tu amistad en la biografía de otra persona, podrán verla en la sección de noticias y en otros lugares de Facebook, así como mediante la función de búsqueda. Si cambias el público a Solo yo, solo tú podrás ver tu lista de amigos completa en tu biografía. Las demás personas solo podrán ver los amigos que tienen en común.	Solo yo	Editar
	Revisa todas tus publicaciones y los contenidos en los que se te etiquetó		Usar registro de actividad
	¿Quieres limitar los destinatarios de las publicaciones que compartiste con los amigos de tus amigos o que hiciste públicas?		Limitar el público de publicaciones antiguas
¿Quién puede ponerse en contacto conmigo?	¿Quién puede enviarte solicitudes de amistad?	Amigos de amigos	Editar
¿Quién puede buscarme?	¿Quién puede buscarte con la dirección de correo electrónico que proporcionaste?	Amigos de amigos	Editar
	¿Quién puede buscarte con el número de teléfono que proporcionaste?	Todos	Editar
	¿Quieres que los motores de búsqueda fuera de Facebook enlacen a tu perfil?	No	Editar

Ilustración 24.Privacidad en redes sociales Fuente: (Oficina de seguridad del internauta, 2017)

En la actualidad la mayoría de las páginas web y algunas aplicaciones móviles nos ofrecen la posibilidad de crearnos un usuario en su plataforma sin la necesidad de registrarnos de la forma tradicional, introduciendo los datos, recibiendo un correo de confirmación con un enlace y haciendo clic para dicha confirmación. Este modo,

aunque se mantiene, se considera lento y tedioso, por lo que se han habilitado otras formas de registro haciendo uso de los datos que introducimos en las redes sociales. Para ello el usuario debe iniciar sesión con los datos de alguna red social, como Facebook, Twitter o Google+. Esto llama especialmente la atención a los usuarios, ya que no necesitan tener una cuenta en cada sitio web, con lo que ahorran tiempo y esfuerzo.

Por el contrario, como contrapartida a la comodidad y rapidez, resulta que las aplicaciones o sitios web pueden tener acceso a nuestros datos fuera de nuestro control directo, ya que en la mayoría de los casos los usuarios no son conscientes de estar facilitándoselos. Es en este punto es donde se detecta que uno de los ataques malware que más se producen en las redes sociales son los realizados por aplicaciones a terceros, es decir, esas aplicaciones a las que precisamente les hemos facilitado nuestros datos.

Para evitar este tipo de ataques se recomienda no utilizarlas a menudo y de forma exclusiva con aquellos sitios en los que tengamos plena confianza. Este sistema se utiliza habitualmente en apps para dispositivos móvil, tales como juegos multiplataforma o apps comerciales, donde se quiere tener los datos sincronizados. Se recomienda un borrado periódico de estas aplicaciones para evitar este tipo de ataques, pues cualquier vulnerabilidad en cualquiera de ellas marcará el destino de las demás, al compartir el sistema de autenticación.

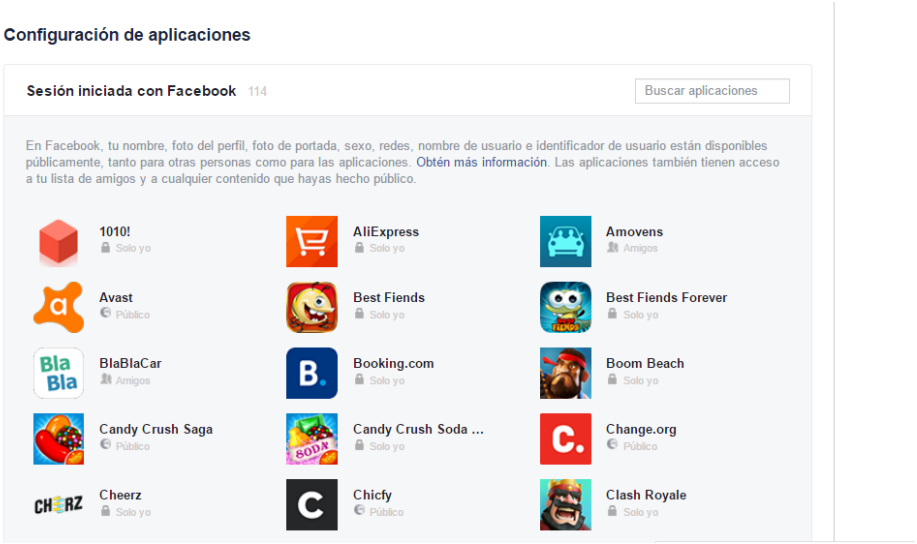


Ilustración 25.Configuración de las aplicaciones externas en Facebook

Precisamente, Facebook, consciente de esta vulnerabilidad, ofrece un panel de control donde podemos eliminar las aplicaciones a terceros que no deseemos que tengan acceso a nuestros datos, así como desactivar por completo esta opción (31).

Como hemos visto anteriormente Facebook ofrece un amplio abanico de posibilidades a la hora de configurar la privacidad de una cuenta. En el caso de Twitter no se quedan rezagados en este aspecto y la red social del "pajarito", conocida así comúnmente por los internautas, nos ofrece las posibilidades que se describen a continuación (32)

En primer lugar, nos ofrece una configuración básica de la cuenta, en la que se incluyen el nombre de usuario y el correo electrónico. A este respecto, se recomienda no poner el nombre y apellidos reales del usuario en cuestión, ya que facilitaría la identificación del usuario en otras redes sociales, haciendo que aumente el riesgo de sufrir un ataque.

Una forma de evitar el uso fraudulento de una cuenta, o ayudar a combatir la suplantación de identidad es incluyendo las iniciales de nuestros apellidos, en lugar de incluir el apellido entero en el perfil, para que las personas fuera del entorno del usuario no puedan obtener sus datos.

Ilustración 26. Privacidad en redes sociales Fuente: (Oficina de seguridad del internauta, 2017)

No sólo la privacidad de la cuenta es importante sino que la seguridad en general nos ayuda a actuar rápidamente ante un ataque. En la configuración de seguridad de Twitter nos encontramos con dos opciones: Verificación de inicio de sesión y restablecimiento de la contraseña. Se recomienda tener activadas ambas opciones.

Ante un intento de robo de nuestra cuenta, teniendo activado el inicio de sesión, en cuanto una persona ajena inicie sesión, el propietario será informado, lo que podría llegar a frenar un ataque generado por algún malware.

En cuanto a la segunda opción, es importante que siempre se nos pida información personal a la hora de recuperar la contraseña, debido a que si no fuera así, cualquier persona que consiga las credenciales de una cuenta podría quitarle todos los privilegios al propietario.

En cuanto a la privacidad, del mismo modo que en Facebook, es recomendable tener la más restrictiva. En este punto conviene destacar que una diferencia muy importante entre Facebook y Twitter es que, en la primera de ellas, los usuarios comparten más contenido digital que en la segunda, siendo este tipo de contenido fotografías personales, vídeos de la familia, etc. Mientras que en Twitter principalmente se escriben sentencias cortas, con lo que implícitamente dispone de una seguridad extra a la hora de hacerse con información personal.

Continuando con lo anterior, Twitter nos ofrece la posibilidad de elegir quién puede añadir una etiqueta o *tag* en las fotos; a este respecto, dependiendo del uso que se le dé, se recomienda que nadie o exclusivamente las personas a las que dicho usuario realiza seguimiento puedan etiquetarle, ya que si elegimos la opción menos restrictiva, que permite a cualquier usuario hacerlo, muchos de los virus que circulan por la red acabarían llegando a dicho perfil.

En cuanto a la privacidad de los Tweets, se recomienda tenerlos protegidos y ante todo, evitar añadir la ubicación asociada a los Tweets, puesto que en muchos de los casos el internauta inexperto ofrece demasiada información a los malhechores para ser utilizada con intenciones delictivas.

Para terminar con la privacidad, la red social nos ofrece la posibilidad de ser visibles a todo Twitter mediante nuestra cuenta de correo electrónico. Esto nos lleva

a determinar que sea recomendable no permitir esta capacidad, porque cualquier hacker puede obtener el email de un usuario por otra red social y realizar una búsqueda del mismo en otra red social, por ejemplo en Twitter, pudiendo desencadenar un ataque directo contra ella.

Ilustración 27. Configuración de la privacidad en Twitter. Fuente: twitter.com

Como se verá posteriormente, orientando las descripciones anteriores a nuestro trabajo, se ha realizado con Maltego una recolección de la información asociada a varias cuentas creadas específicamente para el propósito experimental y comprobaremos que, aunque el nivel de privacidad sea muy restrictivo, se pueden obtener datos que suponemos solo puede ver el usuario propietario de la cuenta.

9 DETECTANDO MALWARE

Las redes sociales son testigo del aumento exponencial de la actividad de los usuarios; esta se cataliza a través de millones de datos por segundo y es de esta característica precisamente de lo que saca provecho el malware para difundirse, poniendo en peligro la reputación de los sistemas y degradando la experiencia de usuario.

Facebook es la mayor red social del mundo, pero no por ello es una excepción en el panorama de los ataques. Recientemente se ha informado de que Facebook se enfrenta a innumerables ataques, con una variabilidad importante, y, a pesar de los reconocidos esfuerzos, no puede por sí sola detener todo el contenido malicioso antes de que llegue al grafo social, es decir, antes de que llegue a todos los usuarios que están interconectados en esta red social.

Facebook es potencialmente una de las redes sociales más lucrativas para las entidades maliciosas, que se aprovechan de las noticias virales para difundir enlaces y propagar rápidamente el malware (33). Prácticamente se puede afirmar que representa el gran mercado donde se pueden ejercer turbias actividades con el menor costo y la mayor repercusión.

Los investigadores en el pasado han estudiado y propuesto técnicas automáticas para identificar las cuentas de usuario maliciosas en las redes sociales. La mayoría de estas técnicas tienen un enfoque restringido en la forma de identificar el contenido malicioso, que se limita a consultar en las base de datos establecidas la pertinencia de determinados mensajes promocionales, envío de mensajes spam masivos, phishing y malware, todos ellos identificados y conocidos.

Sin embargo, con el advenimiento de las redes sociales y la Web 2.0, el alcance de lo considerado como “malicioso” en Internet ha evolucionado. Facebook, por ejemplo, ha establecido normas comunitarias destinadas a proteger a los usuarios contra la pornografía, desnudos, lenguaje que incita al odio, etc., y considera que cualquier entidad que pueda confundir, engañar o defraudar a la gente, como responsable de prácticas abusivas. (34)

En el año 2014 durante la copa de la FIFA un jugador uruguayo hirió a otro jugador con la boca, clavándole los dientes, y esto se hizo viral; los atacantes, aprovechando la gran repercusión que tenía, difundieron enlaces de esta noticia que redirigían a una página de phising en la que los visitantes firmaban una petición en defensa del jugador uruguayo, donde, para ello, debían incluir su nombre, número de teléfono, correo electrónico y país de residencia, con lo que todas esas víctimas acabaron en una lista de *spammailing* (33) de la forma más sencilla imaginable. El vehículo, si bien era conocido, aprovechó la gran capilaridad de las redes sociales, para proyectar su fechoría a escala planetaria.

En el estudio realizado por el Instituto de Tecnología de la Información Indraprastha de Nueva Delhi (India) sobre cómo detectar malware en Facebook se propone definir un conjunto de características basadas en la entidad del perfil, el contenido textual, los metadatos y características de las URL para identificar contenido malicioso en Facebook en tiempo real y 0-day, "desde la hora cero" (estos ataques son los más difíciles de detectar hoy en día, pues no están reportadas las vulnerabilidades y pueden producir un enorme impacto) (33).

Para ello, se propone aplicar técnicas de aprendizaje automático para identificar mensajes maliciosos en Facebook, haciendo uso de la herramienta Weka que contiene una colección de algoritmos de aprendizaje automático en las tareas de minerías de datos.

Estos algoritmos clasifican los datos obtenidos dependiendo de unas características establecidas anteriormente, entre ellos tenemos los siguientes:

- Árbol de decisiones (C4.5), una herramienta que ayuda a tomar una decisión y para ello utiliza un gráfico en forma de árbol o modelo de decisiones.
- Naïve Bayes, una clasificación estadística basada en el teorema de Bayes.

Estos algoritmos ayudan a dar una solución en cuanto a la catalogación de URL maliciosas o malware, aunque también se utiliza con otros fines no relacionados

con la informática. Por ejemplo, Naïve Bayes sigue la siguiente ecuación, para clasificar los datos, dependiendo de sus características.

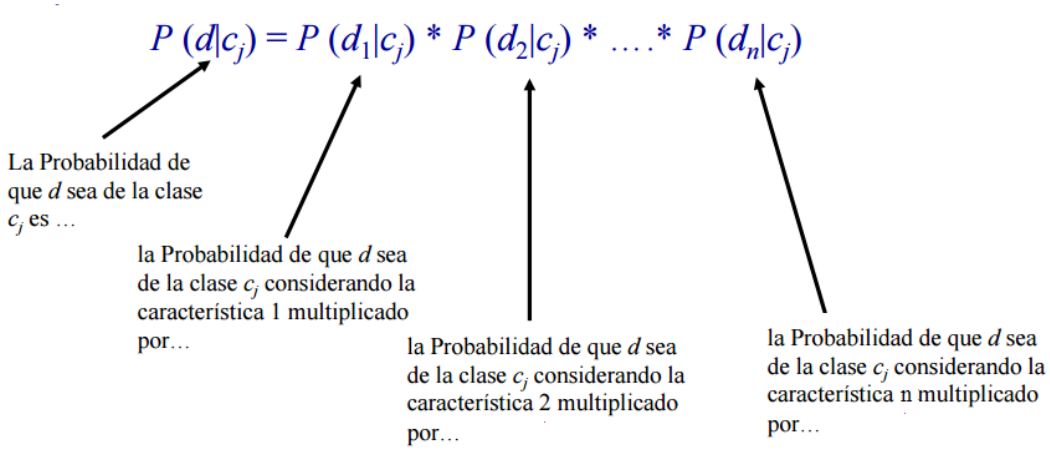


Ilustración 28. Ecuación Naïve Bayes Fuente: campusvirtual.unex.es

De esta forma se han clasificado más de doscientas mil publicaciones como maliciosas de un total de 4,4 millones obtenidas a lo largo de dieciséis meses durante los años 2013 y 2014.

Un detalle que hay que recalcar es que las listas negras han demostrado ser altamente ineficaces inicialmente, debido a que la captura de URL maliciosas 0-day es inferior al 20%. Por esto no parece el recurso óptimo a la hora intentar frenar un ataque desde el inicio, ya que necesita recabar más información.

Por lo expuesto anteriormente, actualmente no se ha encontrado un método 100% efectivo para eliminar el malware desde el minuto cero de su propagación, y este problema se acentúa debido a que normalmente los ataques en redes sociales como Facebook o Twitter se encuentran ocultos bajo una noticia falsa que los usuarios comparten a gran velocidad, aumentando las instancias de dicho enlace, con lo que dificulta aún más el proceso de detección.

Marcamos una URL maliciosa como si contiene uno o más de estos servicios categorizados en el dominio de la URL, como correo no deseado, malicioso, o suplantación de identidad. Para ello utilizamos la herramienta WOT (Web of Trust) que otorga una puntuación de reputación para un dominio dado, permitiendo que

los accesos a ello se puedan categorizar dentro de una estructura de niveles de reputación.

Para la determinación de la reputación, a cada dominio se le asigna un valor en función de varios componentes, uno de ellos es la confiabilidad del dominio. Para ello, el sistema calcula dos valores independientes para cada uno de los dominios, la reputación y una estimación de la confianza en dicha reputación.

Ambos valores juntos indican la cantidad de confianza en el dominio Si los datos de la estimación están por debajo de 60, se califica como insatisfactorio, lo que quiere decir que nos encontramos ante una URL con mala o baja reputación, o lo que es lo mismo, maliciosa y, por tanto, los sistemas deberían inhibir el acceso a éstas.

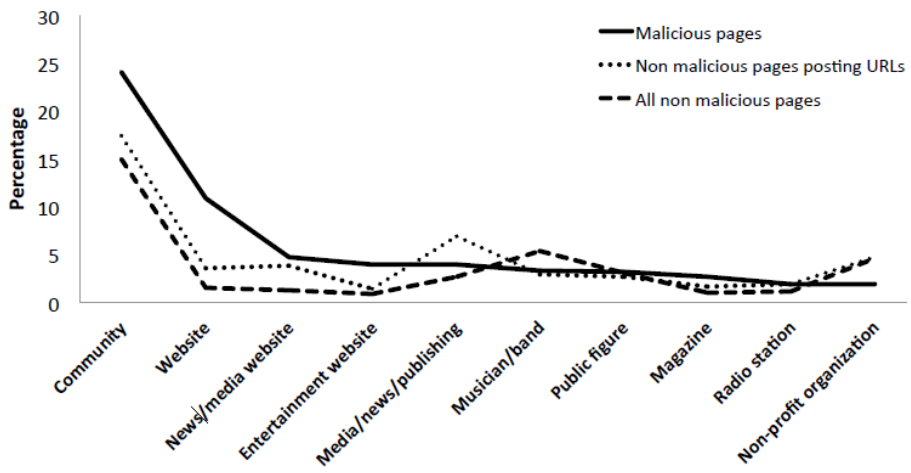


Ilustración 29. Categorías URL con malware en Facebook Fuente: (33)

No obstante, en la ilustración 29 se puede observar que hay una alta similitud entre las páginas maliciosas y las de contenido legítimo. Las categorías que se muestran en la imagen son las destacadas en Facebook debido a su mayor afluencia por los usuarios.

En este momento no hay forma de parar un ataque malware en el momento inicial, esto es, en el origen de su ejecución, pero para los usuarios de las redes

sociales es de gran ayuda la herramienta WOT ya que permite la detección de URL maliciosas.

Ilustración 30.Mensaje WOT Fuente: (33)

En la ilustración 30, se muestra el mensaje que aparece en pantalla cuando un usuario intenta acceder a una URL que ha sido reportada por WOT, el cual se indica que la página que desea visitar no es fiable ya que puede contener spam, malware. Phising u otro tipo de contenido abusivo, ya que como se ha explicado anteriormente la herramienta WOT califica las páginas por el tipo de contenido que poseen, que puede ser, contenido explicito no permitido para menores, etc. O si tienen algún tipo de software malicioso.

Con este trabajo se pretende encontrar una forma de poder asignar la reputación de una cuenta de una red social, o la reputación de una persona en internet, dependiendo de sus redes sociales y otros factores que se describirán.

Para ello se propone una metodología para determinar la reputación de un perfil de una red social. Una forma de poder calcularla en tiempo real si una URL es mediante una API REST que se encargue de calcular mediante unos parámetros, pudiendo ser categorías, la confianza y la reputación de un sitio web de forma similar a como lo hace Web of Trust. Una vez se han analizado todas las publicaciones de dicho perfil con Maltego y la API REST, se procederá a evaluar su reputación.

10 OBTENCIÓN DE DATOS CON MALTEGO

Para este trabajo es necesario obtener los datos del usuario de las redes sociales, para ello utilizamos la herramienta Maltego, que se basa en la obtención de información pública como puede ser una web, una red social, etc.

Maltego es una herramienta de minería y recolección de información utilizada durante la fase de 'Data Gathering', proceso en el cual se trata de obtener el mayor número de información posible sobre un objetivo para su posterior ataque (35). Se encarga obtener información en las fases previas a un ataque, la forma de trabaja de Maltego es mediante peticiones a los servidores, en nuestro caso de Facebook y Twitter, para obtener toda la información posible, dicha información es pública. Ya que Maltego no permite obtener información de perfiles privados.

Por otro lado Maltego permite enumerar información relacionada con elementos de red y dominios así como la información relacionada con personas, como direcciones de email, sitios web asociados, números de teléfono, grupos sociales, empresas asociadas, etc.

Actualmente nos encontramos en el mercado tres versiones: Maltego CE, Maltego classic y Maltego XL (35). La primera de ellas es la versión Comunity, gratuita, mientras que el resto son de pago. En cuanto a la plataforma Kalilinux cabe destacar que también tiene su propia versión de Maltego, llamada Maltego Carbon, dicha herramienta está más enfocada a la realización de un *Pentesting,* aunque este tipo de herramientas tienen siempre dos enfoques, el de atacar y el de defensa ante un ataque.

10.1 ¿PARA QUÉ SIRVE?

Maltego permite establecer relaciones entre entidades (personas, grupos, organizaciones, sitios web, entre otros) usando datos públicos en internet (35), lo que da como resultado una visualización de la entidad objetivo clara, sencilla e intuitiva.

Maltego utiliza "transformaciones", le da este nombre a la operación aplicada sobre una entidad que genera información adicional y cuyos resultados pueden ser

visualizados de varias formas. Estas transformaciones nos permiten indagar en la información y correlar dicha información con otra obtenida por otras vías.

10.2 FUNCIONAMIENTO

En cuanto al funcionamiento interno de la herramienta, se puede decir que es el siguiente:

1. Maltego envía la petición a los servidores de semillas en formato XML a través de HTTPS.
2. La petición del servidor de la semilla se da a los servidores TAS que se transmiten a los proveedores de servicios.
3. Los resultados se envían al cliente Maltego.

Una ventaja adicional que ofrece Maltego es que podemos tener nuestro propio servidor TAS para aumentar nuestra privacidad

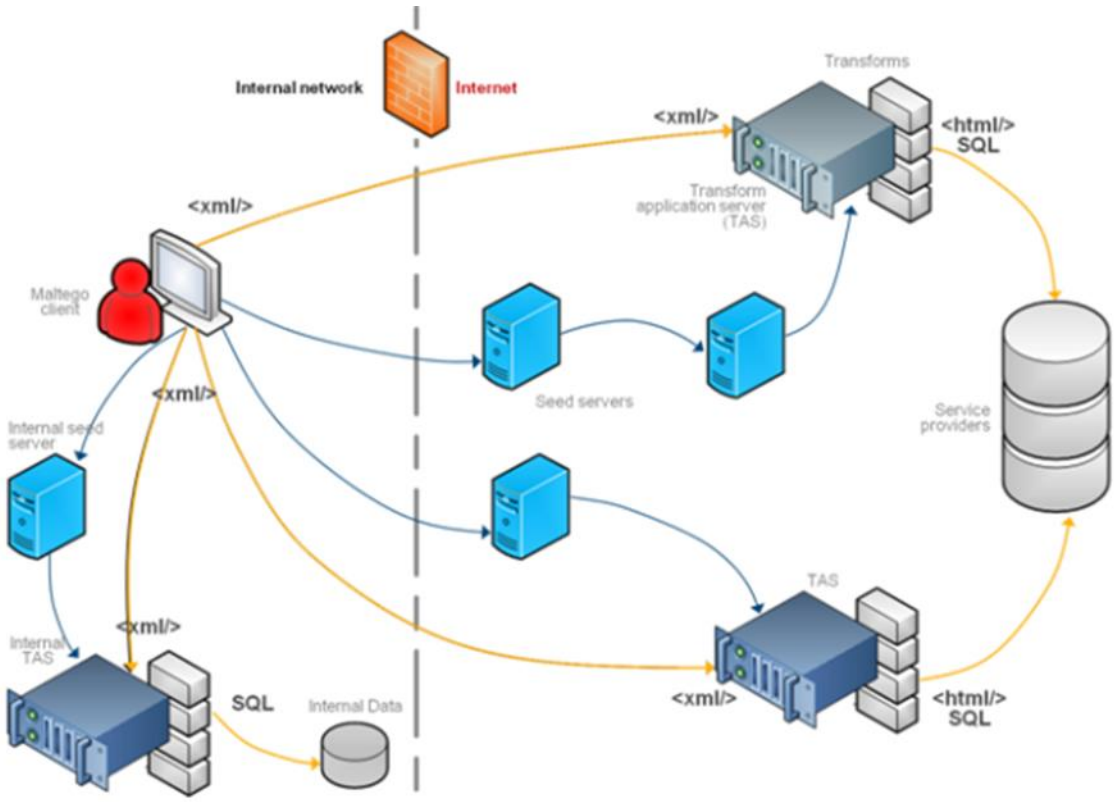


Ilustración 31. Funcionamiento interno de Maltego. Fuente: Paterva.com

10.3 Obtención de datos públicos con Maltego

Como anteriormente se ha explicado, Maltego es una herramienta que se utiliza para la obtención de datos **públicos**, una de sus funciones es aportar información al atacante y también sirve para aportar información acerca de un ataque.

Un detalle para entender mejor el procedimiento realizado es la leyenda de los símbolos que nos permiten un mejor entendimiento de los gráficos obtenidos, a continuación se explican aquellos que van a ser necesarios para nuestro trabajo.

Tabla 1. Iconos útiles para el entendimiento de los gráficos de Maltego

Icono	Leyenda
 Persona	Representa a una entidad persona
 Usuario	Representa a un usuario en Twitter
 Alias	Identifica a una persona por su alias en cualquier red social
 info@paterva.com	Dirección de correo electrónico
 Dominio	Representa un dominio de una página web

URL	Representa la dirección de una página web
Rango de dir. IP	Representa el rango de direcciones de una Red
IP	Representa una dirección IP
Tecnología Utilizada	Indica la tecnología utilizada para el desarrollo de un sitio web
Servidor DNS	Muestra la dirección de un servidor DNS

10.3.1 Ejemplo 1

En este caso se ha procedido a la obtención de datos de una URL, la página web de la universidad, *www.unex.es*, de la cual hemos obtenido una gran cantidad de datos, como IPs, servidores, correos electrónicos, subdominios, localizaciones, etc.

En la ilustración 32 se puede observar de una forma general, la cantidad de datos de datos que ofrece una página web fiable como puede ser la de la universidad, en primer lugar cabe destacar que nos deja a la vista una gran cantidad de correos electrónicos, que podrían incluirse en una lista de Spamming si llegasen a manos de un malhechor.

Otro detalle no menos importante, es que se nos muestra la tecnología utilizada para desarrollar dicha web con lo que nos ayudaría a decidir qué tipo de ataque utilizar si quisiéramos atacarla y por supuesto la dirección IP del servidor donde se encuentra alojada la página.

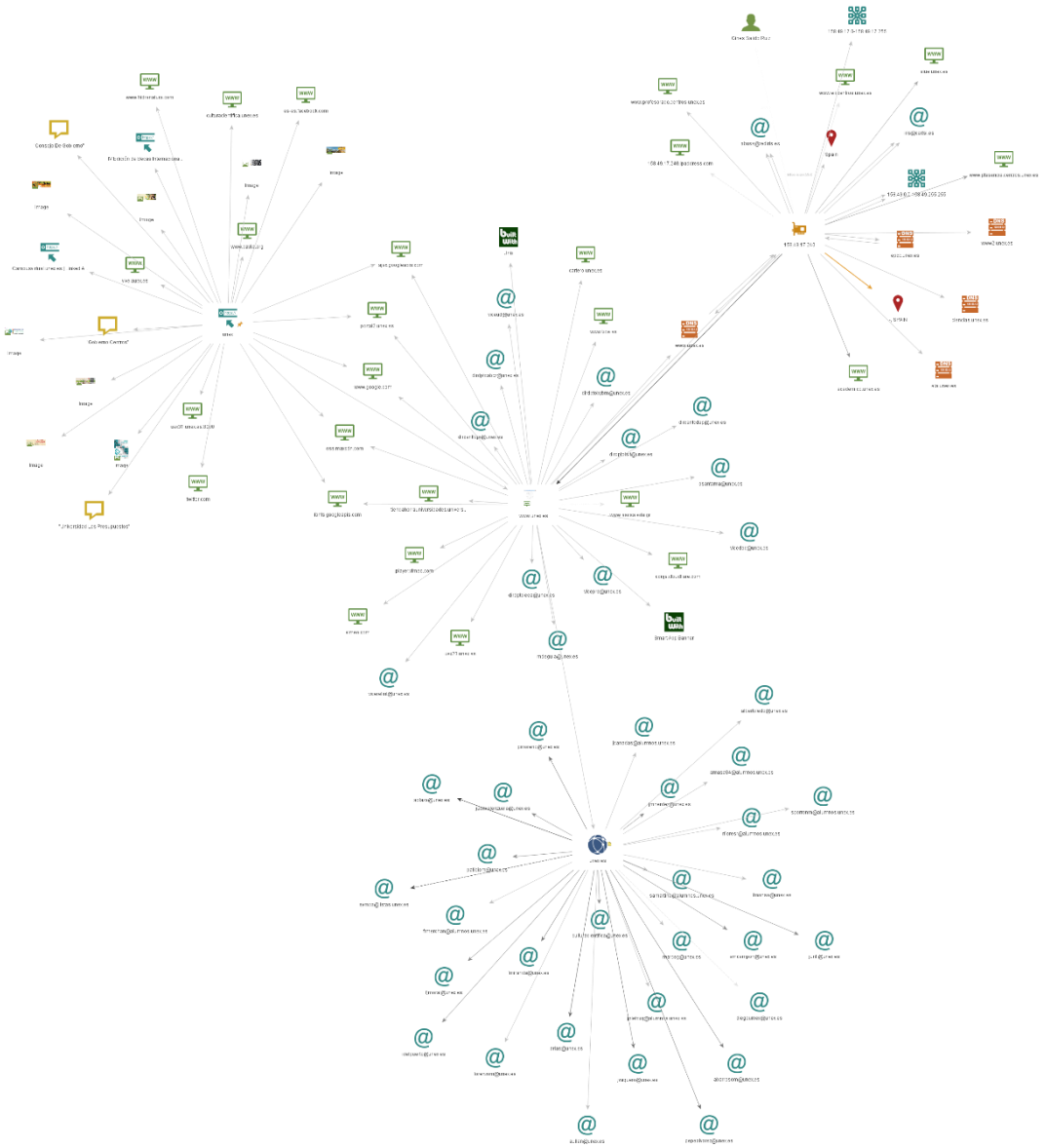


Ilustración 32. Obtención de datos con Maltego de www.unex.es

Dado que la versión gratuita, nos ofrece un número limitado de datos, a continuación se muestran las direcciones de correo electrónico obtenidas, cuyos propietarios son miembros de la Universidad de Extremadura. Si a estas direcciones de correo electrónico le aplicamos más transformadas, podemos correlar datos y

obtener, los datos personales de los usuarios, páginas web que tienen, por ejemplo, cuentas de YouTube, redes sociales en las que están registrados, etc.

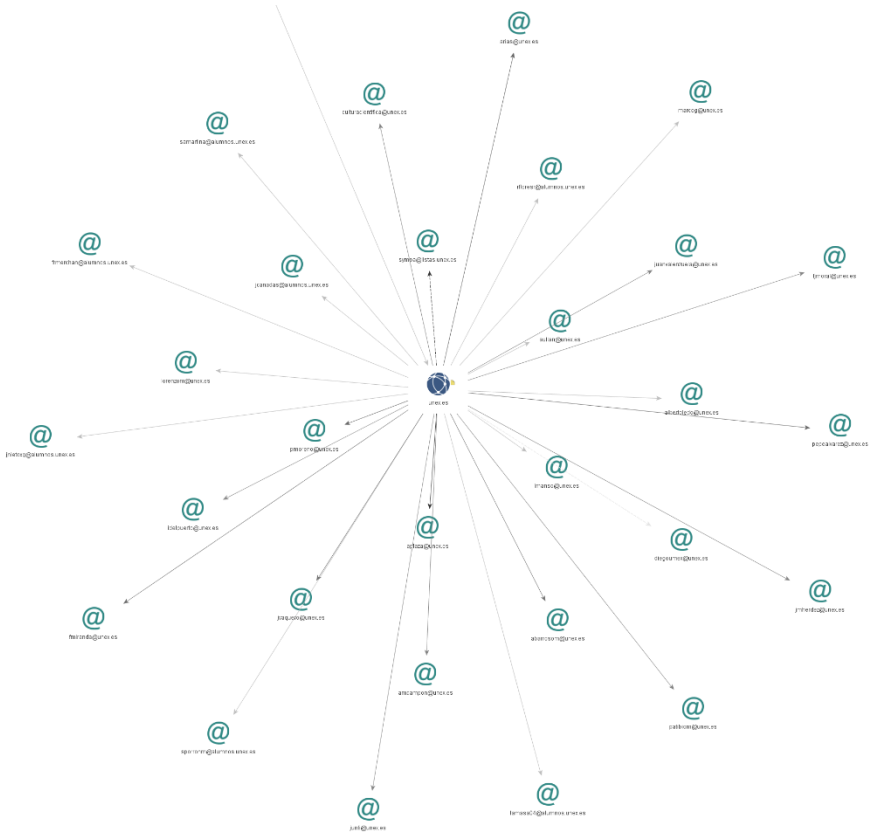


Ilustración 33, Direcciones de correo electrónico obtenidas con Maltego

Un detalle que hay que destacar, es la obtención de la IP de la universidad, incluyendo todo el rango de valores posibles e indicándonos la clase de esta, así como la IP del servidor DNS de la Escuela Politécnica que podría ser víctima de un ataque DDoS que bloquease el servidor.

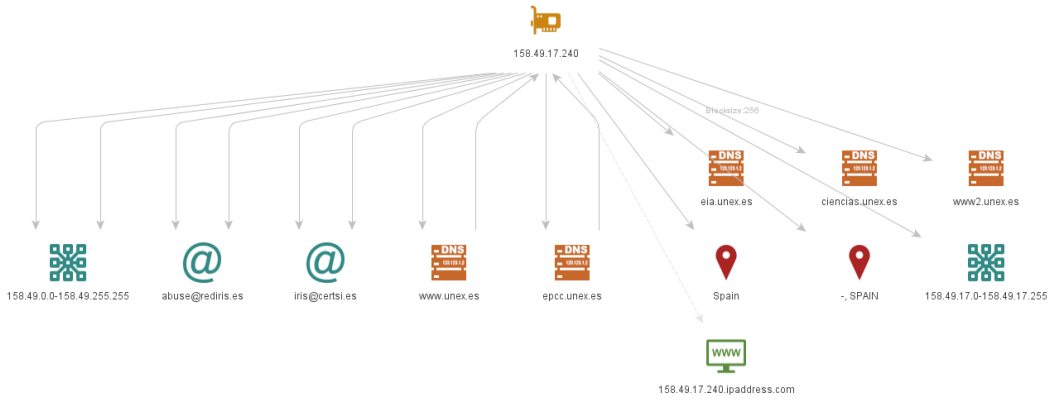


Ilustración 34. Datos obtenidos con Maltego

Esto ha sido una pequeña prueba, lo realmente importante es que aunque los datos parezcan no estar públicos, de esta forma se demuestra que están al alcance de cualquiera con lo se está expuesto a un ataque.

Esto mismo ocurre en las redes sociales, los usuarios cuya privacidad es más restrictiva son menos propensos a ser víctimas de un ataque, aunque cabe decir que el malware les puede afectar aún con la privacidad restrictiva ya que la principal forma de propagación del malware en las redes sociales es por los enlaces de amistad como se ha comentado anteriormente, con lo que la víctima directa será una persona cuyo perfil es público pero después el nivel de privacidad de sus enlaces es irrelevante.

A continuación se muestra un pequeño escenario, en el que se obtienen los datos de los tweet de un usuario cuya cuenta es pública y con Maltego se pueden correlar datos, es decir, si dicho usuario introduce en un tweet un alias de otro usuario, también se pueden obtener los datos de ese usuario, con esta técnica en el lado de un *hacker* podría buscar y encontrar el eslabón débil el cual comenzará la propagación de su malware.

10.3.2 Ejemplo 2

En el siguiente ejemplo, se muestra cómo obtener datos de un usuario a través de otro, algo muy importante que nos permite hacer Maltego, es la relación de usuarios, es decir, si un usuario nombra a otro usuario, haciendo re tweet o de cualquier otra forma, con Maltego podemos obtener todos los tweets de ese otro usuario y además todas sus cuentas, de otras redes sociales, etc.

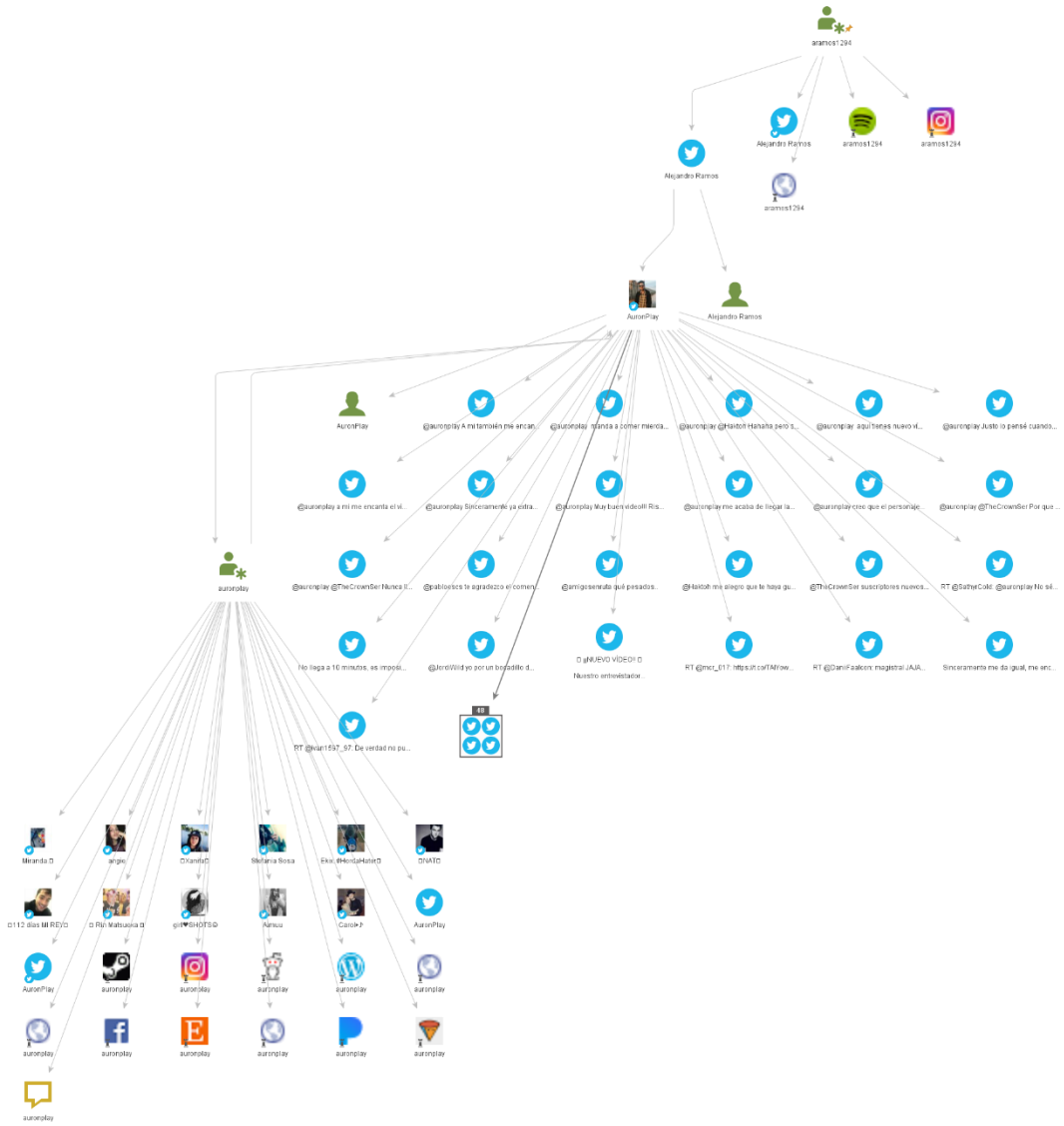


Ilustración 35. Gráfico obtenido con Maltego sobre Twitter

En el gráfico anterior se muestra cómo se han obtenido una parte de los tweets que ha publicado el primer usuario, y a partir de los usuarios que sigue, se pueden obtener los tweets de este segundo usuario.

Este tipo de gráficos es útil a la hora de obtener la actividad de un usuario, por ejemplo, es posible obtener todos los tweet por categorías, es decir, si los ha escrito el usuario o son fruto de un re tweet, con lo que permite obtener información de las comunicaciones llevadas por el usuario con otros a través de la plataforma.

Un fallo en la privacidad de Twitter, nos permite ver los tweets de una cuenta privada, si el usuario acaba de modificar la privacidad de su cuenta de pública a privada pocos minutos antes de introducir sus datos en Maltego.

10.3.3 Ejemplo 3

Debido a que la versión gratuita de Maltego ya no nos permite obtener cuentas Facebook, se explicará la metodología a seguir para la obtención de una cuenta en Facebook y cómo averiguar si dicha cuenta es falsa.

En primer lugar, se crea un objeto de tipo *Facebook object* (solo disponible en las versiones de pago) como se puede apreciar en la ilustración 36, y se procede a modificar sus atributos.

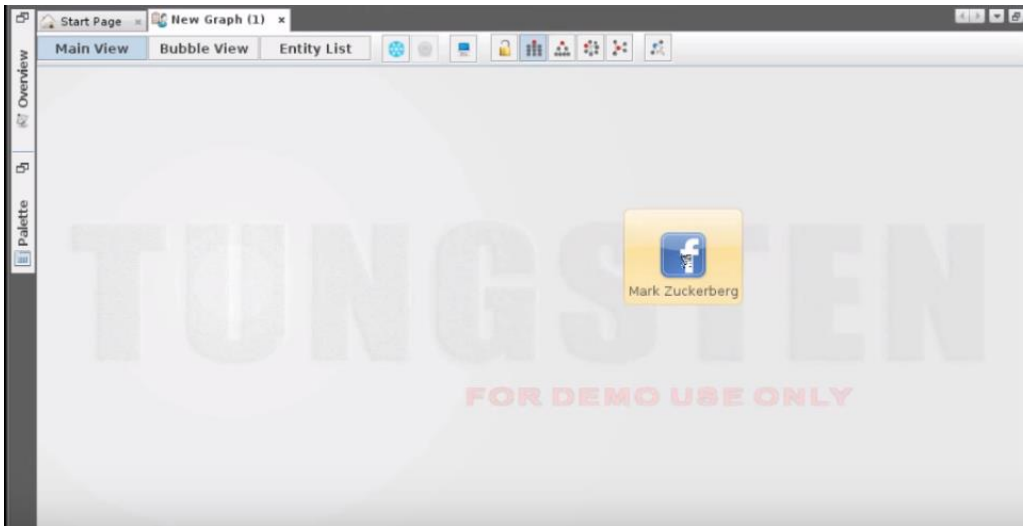


Ilustración 36. Facebook Object en Maltego

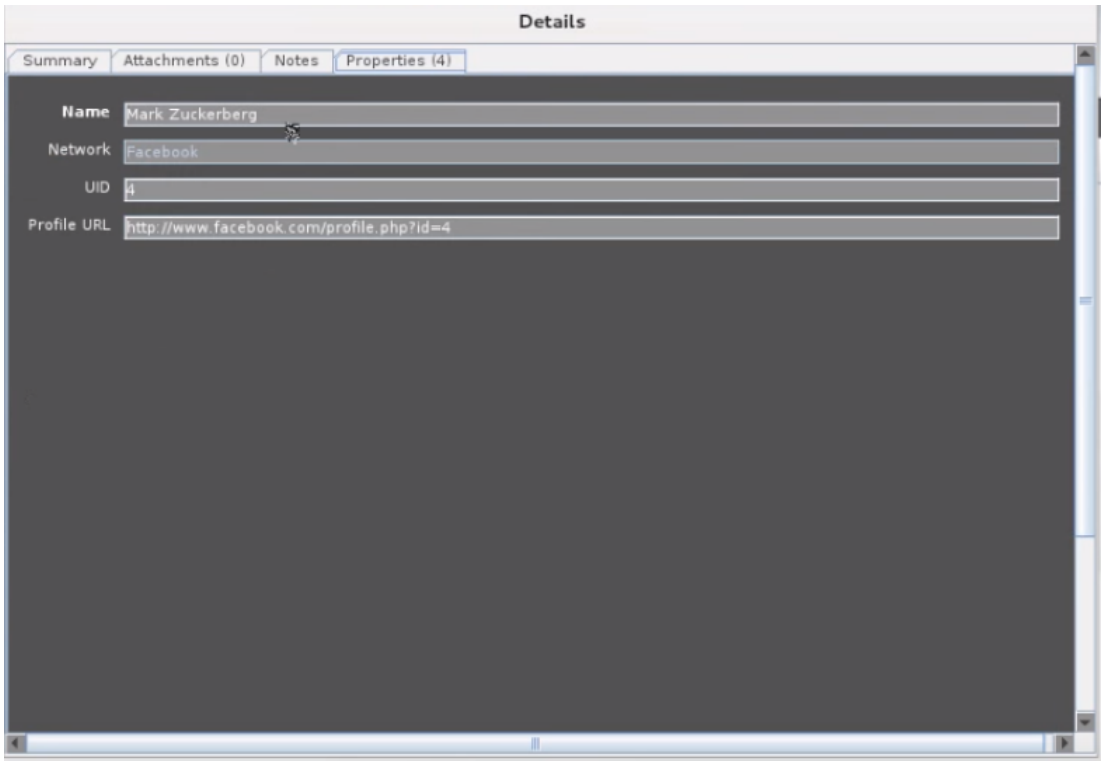


Ilustración 37. Propiedades de un Facebook object

Como se muestra en la ilustración 37, un objeto Facebook tiene las siguientes propiedades: nombre, red, UID, URL del perfil. Para ello modificamos el nombre e introducimos el del usuario del que deseemos obtener información y modificamos el UID, para obtener el UID de cualquier usuario abrimos el perfil de Facebook y abrimos una imagen, como se puede apreciar en la ilustración 38, en la cual está resaltado el *fbid* que corresponde con el identificador de usuario, en este caso el UID, y lo introducimos en Maltego. En el caso de la URL del perfil, modificamos el número correspondiente al identificador de usuario por defecto e introducimos el UID del perfil que vamos a identificar con Maltego.

https://www.facebook.com/photo.php?fbid=10208466272347924&set=a.1514667660224.72159.1040417309&type=3&theater

Ilustración 38. URL de una imagen de un perfil Facebook

Una vez, hemos realizado los pasos anteriores, aplicamos las transformadas del email, el cual nos permite obtener el email del usuario. Mediante la transformación SMTP nos permite verificar si el correo está activo, ya que normalmente las cuentas falsas de spam se crean cuentas de correo electrónico que sólo se utilizan para eso, con lo que Maltego nos debe decir que la dirección de correo de recibida no es accesible, si ocurre esto, nos encontramos ante una cuenta spam o falsa. Cabe destacar que actualmente este proceso solo se puede realizar con las versiones de pago.

Aunque en este ejemplo, se utiliza Maltego para saber si un perfil público en Facebook es falso o no, la principal función de esta herramienta es la de obtener datos, ya que también nos permite obtener gran cantidad de datos de una cuenta Facebook, al igual que de Twitter como se muestra en el ejemplo 2.

En la metodología que se muestra en el apartado siguiente, Maltego Community es utilizado para obtener los tweets de un Twitter o los post de una cuenta Facebook con Maltego XL.

11 DESCRIPCIÓN DE LA EXPERIENCIA

Para el desarrollo de este trabajo final de grado se ha propuesto analizar las redes sociales, ello incluye un análisis de los datos obtenidos de los *post* de Facebook, para ello se propone la siguiente metodología.

Ilustración 39. Metodología para la determinación de la reputación de un perfil

11.1 OBTENCIÓN DE LOS DATOS CON MALTEGO

Para la obtención de los datos con la herramienta Maltego, es necesario conocer el ID de Facebook o el de Twitter, con el que obtenemos otro tipo de información como, en el caso de Facebook, la imagen de perfil, email, en algunos casos es posible obtener el número de teléfono, datos personales del perfil, etc.; en el caso de twitter se pueden obtener el usuario, email, amigos, etc.

Se obtienen los mensajes públicos, en el caso de Twitter los tweets del usuario y en el caso de Facebook los post, y se exportan de Maltego a un Excel, como se muestra en la imagen siguiente, para la posterior inserción en la base de datos.

En la ilustración 40, se puede observar el gráfico creado por Maltego, una vez se han eliminado las entidades que no eran necesarias, dejando únicamente los tweets, el alias y los datos del usuario en caso de que los hubiese.

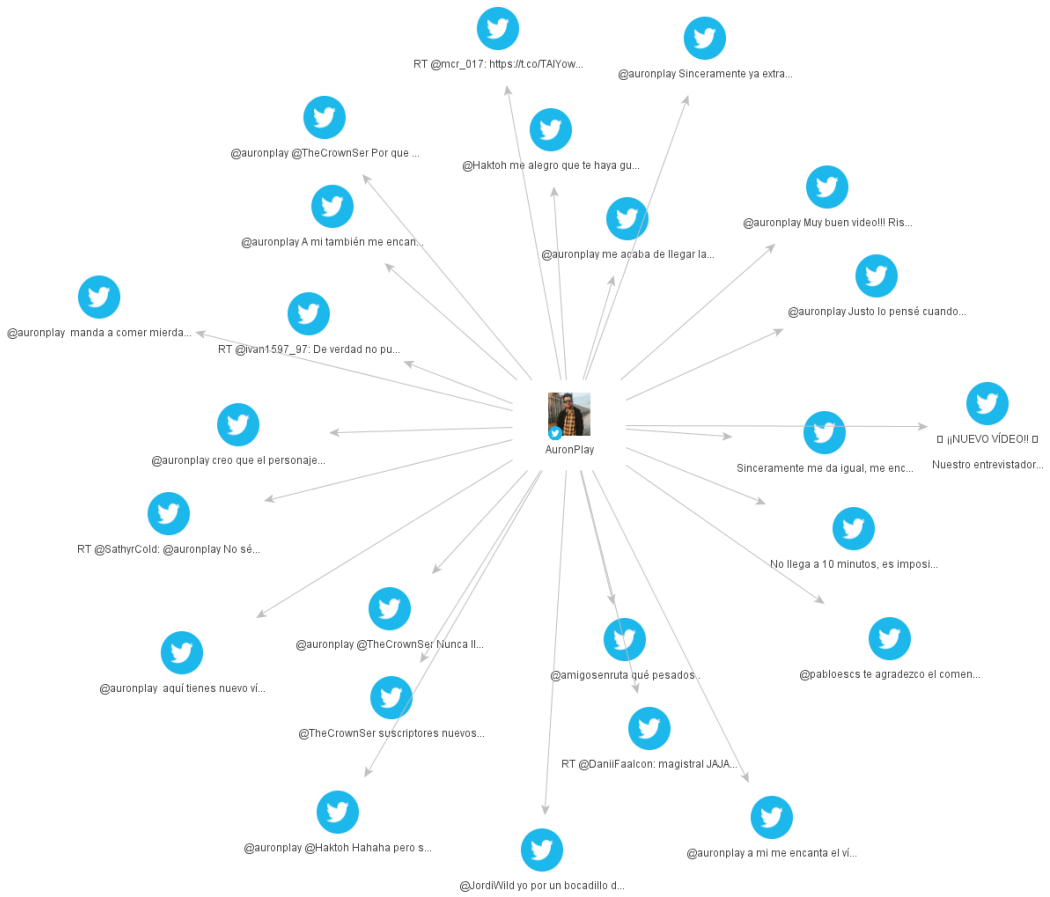


Ilustración 40. Tweets obtenidos de una cuenta de Twitter con Maltego

A continuación, se exporta el gráfico como una tabla en Excel, asegurando que no hay dos publicaciones iguales, ya que Maltego elimina las tuplas duplicadas, como se muestra en la ilustración siguiente.

	A	B	C	D	E	F
1	ID Twitter	Tweet				
2	AuronPlay	@Haktoh me alegro que te haya gustado, hay mucha...				
3	AuronPlay	@JordiWild yo por un bocadillo de panceta iba,...				
4	AuronPlay	@TheCrownSer suscriptores nuevos que se creen que...				
5	AuronPlay	@amigosenruta qué pesados..				
6	AuronPlay	@auronplay aquí tienes nuevo vídeo...				
7	AuronPlay	@auronplay manda a comer mierda a los te ...				
8	AuronPlay	@auronplay @Haktoh Hahaha pero si es algo de lo...				
9	AuronPlay	@auronplay @TheCrownSer Nunca llueve a gusto de...				
10	AuronPlay	@auronplay @TheCrownSer Por que se fijan en los...				
11	AuronPlay	@auronplay A mi también me encanta,lo que pasa es...				
12	AuronPlay	@auronplay Justo lo pensé cuando lo vi publicado...				
13	AuronPlay	@auronplay Muy buen video!!! Risas aseguradas con...				
14	AuronPlay	@auronplay Sinceramente ya extrañaba estos...				
15	AuronPlay	@auronplay a mi me encanta el vídeo esta super...				
16	AuronPlay	@auronplay creo que el personaje de Fistro Mejide...				
17	AuronPlay	@auronplay me acaba de llegar la notificación del...				
18	AuronPlay	@pabloescs te agradezco el comentario, variar de...				
19	AuronPlay	No llega a 10 minutos, es imposible, ni...				
20	AuronPlay	RT @DaniiFaalcon: magistral JAJAJAAJAJAJAJAJAJA...				
21	AuronPlay	RT @SathyrCold: @auronplay No sé si pedirte otro...				
22	AuronPlay	RT @ivan1597_97: De verdad no puedo con los...				
23	AuronPlay	RT @mcr_017: https://t.co/TAIYow7TdB gracias...				
24	AuronPlay	Sinceramente me da igual, me encanta hacer...				
25	AuronPlay	□ ¡¡NUEVO VÍDEO!! □Nuestro entrevistador...				

Ilustración 41.Excel generado a partir de Maltego

Para la inserción de los datos se ha utilizado una macro de Microsoft Excel (36), la cual nos permite generar código SQL a partir del Excel, como se muestra en la imagen siguiente, para posteriormente insertar dichos datos en la base de datos.

	A
1	INSERT INTO Tabla (ID_Twitter, Contenido) VALUES ('AuronPlay', '@Haktoh me alegro que te haya gustado, hay mucha...', ,'', '')
2	INSERT INTO Tabla (ID_Twitter, Contenido) VALUES ('AuronPlay', '@JordiWild yo por un bocadillo de panceta iba,...', ,'', '')
3	INSERT INTO Tabla (ID_Twitter, Contenido) VALUES ('AuronPlay', '@TheCrownSer suscriptores nuevos que se creen que...', ,'', '')
4	INSERT INTO Tabla (ID_Twitter, Contenido) VALUES ('AuronPlay', '@amigosenruta qué pesados..', ,'', '')
5	INSERT INTO Tabla (ID_Twitter, Contenido) VALUES ('AuronPlay', '@auronplay aquí tienes nuevo vídeo...', ,'', '')
6	INSERT INTO Tabla (ID_Twitter, Contenido) VALUES ('AuronPlay', '@auronplay manda a comer mierda a los te ...', ,'', '')
7	INSERT INTO Tabla (ID_Twitter, Contenido) VALUES ('AuronPlay', '@auronplay @Haktoh Hahaha pero si es algo de lo...', ,'', '')
8	INSERT INTO Tabla (ID_Twitter, Contenido) VALUES ('AuronPlay', '@auronplay @TheCrownSer Nunca llueve a gusto de...', ,'', '')
9	INSERT INTO Tabla (ID_Twitter, Contenido) VALUES ('AuronPlay', '@auronplay @TheCrownSer Por que se fijan en los...', ,'', '')
10	INSERT INTO Tweets (ID_Twitter, Contenido) VALUES ('AuronPlay', '@auronplay A mi también me encanta,lo que pasa es...', ,'', '')
11	INSERT INTO Tweets (ID_Twitter, Contenido) VALUES ('AuronPlay', '@auronplay Justo lo pensé cuando lo vi publicado...', ,'', '')
12	INSERT INTO Tweets (ID_Twitter, Contenido) VALUES ('AuronPlay', '@auronplay Muy buen video!!! Risas aseguradas con...', ,'', '')
13	INSERT INTO Tweets (ID_Twitter, Contenido) VALUES ('AuronPlay', '@auronplay Sinceramente ya extrañaba estos...', ,'', '')
14	INSERT INTO Tweets (ID_Twitter, Contenido) VALUES ('AuronPlay', '@auronplay a mi me encanta el vídeo esta super...', ,'', '')
15	INSERT INTO Tweets (ID_Twitter, Contenido) VALUES ('AuronPlay', '@auronplay creo que el personaje de Fistro Mejide...', ,'', '')
16	INSERT INTO Tweets (ID_Twitter, Contenido) VALUES ('AuronPlay', '@auronplay me acaba de llegar la notificación del...', ,'', '')
17	INSERT INTO Tweets (ID_Twitter, Contenido) VALUES ('AuronPlay', '@pabloescs te agradezco el comentario, variar de...', ,'', '')
18	INSERT INTO Tweets (ID_Twitter, Contenido) VALUES ('AuronPlay', 'No llega a 10 minutos, es imposible, ni...', ,'', '')
19	INSERT INTO Tweets (ID_Twitter, Contenido) VALUES ('AuronPlay', 'RT @DaniiFaalcon: magistral JAJAJAAJAJAJAJAJAJA...', ,'', '')
20	INSERT INTO Tweets (ID_Twitter, Contenido) VALUES ('AuronPlay', 'RT @SathyrCold: @auronplay No sé si pedirte otro...', ,'', '')
21	INSERT INTO Tweets (ID_Twitter, Contenido) VALUES ('AuronPlay', 'RT @ivan1597_97: De verdad no puedo con los...', ,'', '')
22	INSERT INTO Tweets (ID_Twitter, Contenido) VALUES ('AuronPlay', 'RT @mcr_017: https://t.co/TAIYow7TdB gracias...', ,'', '')
23	INSERT INTO Tweets (ID_Twitter, Contenido) VALUES ('AuronPlay', 'Sinceramente me da igual, me encanta hacer...', ,'', '')

Ilustración 42.Código SQL generado a partir de los datos de Excel

Para la realización de esta tarea, se realiza el mismo proceso que en el ejemplo 2 de la sección 10, en la cual se obtienen gran parte de los tweets de un usuario, así como sus amistades en la red social, etc.,

11.2 EXTRACCIÓN DE LOS DATOS

Una vez, tenemos los datos en Excel, los datos son almacenados en una base de datos creada exclusivamente para ello, la cual contendrá tres tablas:

Tabla 2. Tablas de las base de datos

Usuarios

- ID de Facebook
- ID de Twitter
- Nombre
- Apellidos
- Email
- Teléfono
- Puntuación obtenida
- Reputación

Post de Facebook

- ID del usuario que realizó el post
- ID de usuarios nombrados en el post
- Contenido del post
- URL
- Otros datos, como geolocalización.

Tweet de Twitter

- ID del usuario que realizó el post
- ID de usuarios nombrados en el post
- Contenido del tweet
- URL
- Otros datos, como geolocalización.

Dichas tablas están relacionadas por el identificador, tanto en el caso de Facebook como de Twitter, que se encuentran almacenadas en ambas tablas como claves externas a la tabla usuario, que a su vez, son claves primarias de la tabla usuario, como se muestra en la siguiente ilustración.

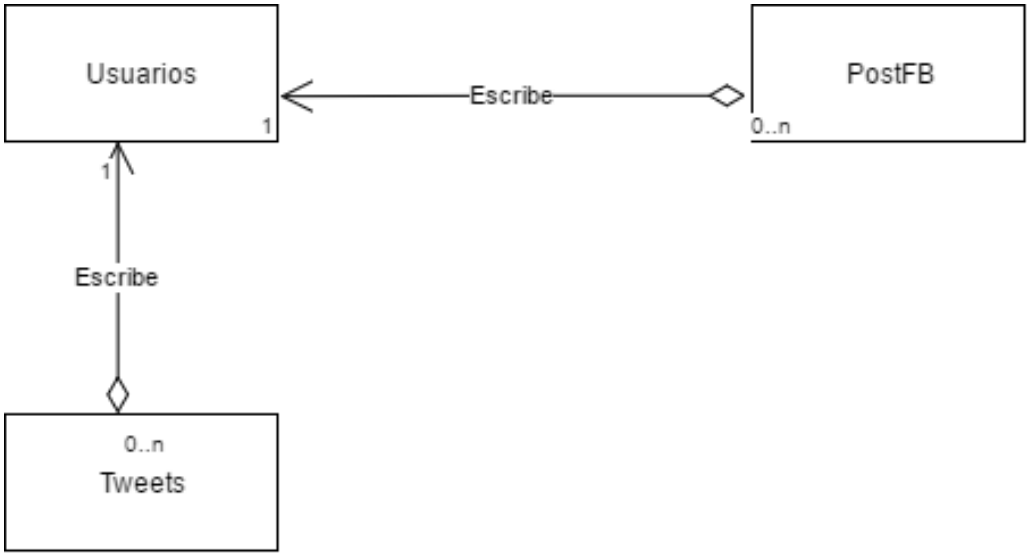


Ilustración 43. Diagrama UML sencillo de la base de datos

La base de datos se comunicará con el usuario a través de una API REST, la cual permite al usuario analizar los post realizados.

11.3 ANÁLISIS DE LOS DATOS

Para el análisis de los datos utilizaremos dos herramientas, la APIREST que estaría desarrollada para este fin y otras herramientas. La APIREST se encargará de procesar los datos que hemos introducido anteriormente, y comparar las URL con las listas negras como la de VirusTotal, Google SafeBrowsing o Web of Trust. Una vez realizado esto, las URL que no han sido clasificadas como maliciosas, se proceden a analizar utilizando la herramienta Weka, que las clasificará según los datos, para intentar demostrar si son maliciosas, y clasificar el contenido de la publicación dependiendo de las palabras que contenga.

Ilustración 44. Analizar URLs con VirusTotal Fuente: www.virustotal.com/es/

Otra forma de realizar esto, seria utilizando una herramienta que permita por sí sola la comprobación de la existencia de malware en URL, la versión de pago de Maltego permite buscar un *exploit* entre una serie de URL, dichas URLs pueden ser obtenidas de tweets o post con el propio Maltego, pero debido a las limitaciones existentes a la hora de realizar este trabajo no se ha podido comprobar con exactitud.

11.4 Determinación de la reputación del perfil

Si entre los datos analizados para un usuario obtenemos que más del 50% de las URL de las publicaciones, consideramos que el perfil tiene mala reputación. Aunque el usuario en sí, no publique los enlaces a páginas maliciosas el hecho de compartir los mensajes en los que se encuentran estos enlaces se considera peligroso, sin importar si el usuario lo hace consciente o inconscientemente, ya que el principal motivo del gran alcance de este tipo de ataques es que los usuarios lo comparte, lo que aumenta.

Además se calculará la puntuación de cada publicación, obteniendo los metadatos y comprobado su contenido, obteniendo una puntuación positiva en el caso de que la publicación no contenga imágenes pornográficas o violentas y

contenido textual sin palabras malsonantes, por el contrario si en la publicación se encuentran imágenes o palabras pornográficas o violentas, se le asignará una puntuación negativa.

La puntuación obtenida no tendrá valor si la publicación analizada contiene un enlace malicioso, con lo que su función es la de catalogar las páginas web fiables, para evitar que entren en dichas páginas los usuarios menores de edad o sensibles a determinadas imágenes, que puedan contener violencia, sexo explícito, etc.

Para terminar, se sumarán todas las puntuaciones del usuario y se realizará la media entre todas ellas, si el resultado obtenido es positivo, nos encontramos ante un perfil fiable, que tendría una buena reputación ya que en sus publicaciones no poseen contenido explícito ni malware en los enlaces, caso contrario la reputación del perfil sería negativa.

Ilustración 45. Como obtener perfiles con reputación negativa

12 CONCLUSIONES

Para concluir este trabajo, se quiere dar la importancia al conocimiento en cuanto al uso de las redes sociales en Internet, ya que a priori, parecen lugares seguros o al menos la seguridad no parece ser una prioridad para los usuarios. Sin embargo, los hechos nos demuestran cada día que nos encontramos ante una realidad completamente diferente, debido a que cada vez es más habitual encontrar usuarios de internet, y no necesariamente expertos, que las utilizan como herramienta a la hora de realizar un ataque o incluir malware en los ordenadores, encubierto tras las publicaciones a las que accedemos.

Al analizar las redes sociales con herramientas como Maltego, especializada para realizar pentesting (una función de defensa o seguridad, pero que a su vez pone también en manos de elementos criminales las mismas herramientas para propósitos no tan moralmente aceptables), se puede observar la gran cantidad de datos que pueden ser extraídos de un perfil, que a simple vista deberían gozar de un adecuado nivel de privacidad. Y lo que es peor, nos encontramos con que el usuario de dicho perfil desconoce que la mayoría de sus datos personales circulan y son públicos en internet, lo que evidencia una falta absoluta de control sobre los mismos.

El gran problema al que se enfrentan los usuarios, cuando navegan en internet, de forma general, pero mayoritariamente cuando se hallan en una red social, es el malware, esos códigos maliciosos que son capaces de subvertir los objetivos de los datos. Y cómo no, las víctimas potenciales ante un ataque suelen ser los usuarios con pocos conocimientos de informática o poco precavidos, mucho más fáciles de atrapar que otros usuarios contra los que se debe desarrollar otro tipo de ataques mucho más sofisticados.

Este trabajo ha querido recopilar y analizar las “trampas” más habituales de las que hacen uso algunos usuarios con intenciones dudosas, para ayudar a los miembros de la comunidad de internet a navegar en internet de una forma más segura y sin la exposición que el desconocimiento nos lleva a asumir.

Además de los ataques basados en malware, en la actualidad nos preocupe enormemente que la mayoría de los usuarios de redes sociales y del correo electrónico por extensión, seamos víctimas del conocido como spam que se encuentra presente por todo internet, verdadero devorador de recursos informático y de comunicaciones, que se basa sobre todo en una publicidad abusiva, en gran parte debido a un uso desleal de los datos de los usuarios para la orientación de dicha publicidad.

Con este fin, este proyecto ha intentado analizar algunas redes sociales con herramientas que están al alcance de cualquier usuario para evidenciar la cantidad de datos de cualquier usuario que navegan por internet y que con las correlaciones y operaciones adecuadas, pueden aportar el número suficiente de datos de un usuario que deja fácil una actividad maliciosa. Por ello, con esas mismas herramientas de fácil acceso, se ha intentado aportar una metodología de revisión de perfiles de los usuarios de Facebook, Twitter, etc. con la idea de, en primer lugar, analizar su privacidad, y en segundo lugar, establecer una escala de reputación que permita detectar aquellos perfiles que o bien son falsos o tienen acceso a webs o links con malware. En varios ejemplos en laboratorio, se ha expuesto la forma de recolectar datos de algunas cuentas y posteriormente se ha realizado una propuesta teórica de detección de aquellos perfiles con una reputación deficiente, que principalmente se encargan en la creación y difusión de todo tipo de malware, spam, phishing, Cross-site, etc.

Para completar este trabajo, faltaría una implementación práctica de la metodología propuesta y automatizada que llevase a cabo los puntos propuestos, detectando los perfiles sospechosos de forma automatizada, que permitiera a los usuarios advertir de las vulnerabilidades que están asociadas a determinados ¨amigos¨ y asimismo determinase la reputación de un usuario en una red social.

Otra ampliación que se podría llevar a cabo sería la contrastación de los datos de un usuario en diferentes redes sociales, de forma que mediante la correlación de determinados datos, se pudiera detectar cualquier usuario que atesora perfiles falsos. Aspectos como el idioma, el deporte o los ¨me gusta¨ y un sinnúmero más de datos de tipo similar pueden ayudar a elaborar un perfil real del individuo que puede

resultar beneficioso para las Fuerzas de Seguridad del Estado para perseguir a los malhechores.

Sin embargo, en esta carrera sin destino final, la recolección y la correlación de datos son dos aspectos de la misma disputa dialéctica entre el bien y el mal, entre los usuarios leales y los maliciosos, entre la policía y los malhechores. En efecto, las mismas metodologías y herramientas que sirven para identificar estos perfile, sirven igualmente para recabar información necesaria para un ataque.

En definitiva, se demuestra una vez más que la tecnología, lejos de ser una solución a determinados problemas, los desplaza a un mundo virtual donde, si cabe, las restricciones de espacio y tiempo desaparecen y sus efectos se multiplican. Será el reto próximo que la identidad digital asociada a todos los datos que naveguen por internet tengan un vínculo común sobre la que podamos ejercer un control seguro y cederlos a nuestro aleccionado criterio.

13 REFERENCIAS

1. **UAL.** Universidad de Almería. [En línea] http://cms.ual.es/UAL/universidad/serviciosgenerales/stic/servicios/recomendaciones/redessociales/index.htm.

2. **IAB. *IAB.* [En línea] 2016. http://www.antevenio.com/blog/2016/05/analisis-del-informe-de-2016-del-iab-sobre-el-uso-de-redes-sociales/.**

3. *AV.* [En línea] [Citado el:] https://www.av-test.org/en/statistics/malware/.

4. Cisco. Cisco. *Informa anual de ciberseguridad 2016.* [En línea] 2016. http://www.cisco.com/c/dam/m/es_es/internet-of-everything-ioe/iac/assets/pdfs/security/cisco_2016_asr_011116_es-es.pdf.

5. europapress. *Yihadistas en Siria usan Facebook para cibersexo o pedir dinero que luego va a su bolsillo.* [En línea] 6 de Septiembre de 2016. [Citado el: 13 de Junio de 2017.] http://www.europapress.es/nacional/noticia-yihadistas-siria-usan-facebook-cibersexo-pedir-dinero-luego-va-bolsillo-20150926122435.html.

6. WeAreSocial. [En línea] https://wearesocial.com/uk/special-reports/digital-in-2016.

7. IAB. *Estudio de las redes sociales en 2017.* [En línea] Abril de 2017. http://iabspain.es/wp-content/uploads/iab_estudioredessociales_2017_vreducida.pdf.

8. Abc. *Abc.* [En línea] 28 de Diciembre de 2015. http://www.abc.es/deportes/futbol/abci-barca-despide-ultimo-fichaje-publicar-mensajes-ofensivos-twitter-contra-cataluna-201512282225_noticia.html.

9. Security Issues in Social Networks. [aut. libro] Jun Hu,Tuo Huang, Jingnan Wang Hongyu Gao. *Security Issues in Social Networks.* s.l. : IEE, 2011.

10. ComputerHoy. *Vulnerabilidad de Facebook permite robar múltiples cuentas.* [En línea] 26 de Agosto de 2016.

http://computerhoy.com/noticias/internet/vulnerabilidad-facebook-permite-robar-multiples-cuentas-50174.

11. ExpresiónBinaria. *Anatomía de un ataque basado en redes sociales.* [En línea] 20 de Marzo de 2017. http://www.expresionbinaria.com/anatomia-de-un-ataque-basado-en-redes-sociales/.

12. Moreno, Manuel. Trece Bits. *Facebook ya tiene 1.860 millones de usuarios.* [En línea] 2 de Febrero de 2017. http://www.trecebits.com/2017/02/02/facebook-ya-tiene-1-860-millones-de-usuarios/.

13. Mejía, Juan C. JuanCmejia. [En línea] 2 de Mayo de 2017. http://www.juancmejia.com/marketing-digital/estadisticas-de-redes-sociales-usuarios-de-facebook-instagram-linkedin-twitter-whatsapp-y-otros-infografia/#1_Usuarios_de_Facebook.

14. IAB. *Estudio redes sociales 2016.* [En línea] Abril de 2016. http://www.iabspain.net/wp-content/uploads/downloads/2016/04/IAB_EstudioRedesSociales_2016_VCorta.pdf.

15. Luz, Sergio de. Privacidad y Seguridad en las Redes Sociales. *Privacidad y Seguridad en las Redes Sociales.* 2010.

16. Wikipedia. [En línea] 2017. https://es.wikipedia.org/wiki/Acreditaci%C3%B3n_de_identidad.

17. OEDI. *OEDI.* [En línea] 2016. http://oedi.es/estadisticas/.

18. Soler. *Soler.* [En línea] [Citado el: 2017 de Mayo de 30.] http://www.soler-gdi.es/?page=8.

19. Sandoval, Jorge Ivanr Ramirez. Tipos de Ataques Informáticos. [En línea] https://es.scribd.com/doc/19397003/Tipos-de-Ataques-informaticos.

20. ComputerHoy. *Descubren un bug en Facebook que atenta contra la privacidad de facebook.* [En línea] 29 de Mayo de 2015.

http://computerhoy.com/noticias/internet/estudiante-harvard-te-permite-rastrear-amigos-facebook-29151.

21. LSSI. *LSSI.* [En línea] 2011. http://www.lssi.gob.es/la-ley/aspectos-basicos/Paginas/publicidad-internet.aspx.

22. EUROPA PRESS. 20Minutos. *20Minutos.* [En línea] 2017. http://www.20minutos.es/noticia/2992952/0/detenidos-dos-menores-por-crear-perfil-falso-redes-sociales-con-imagenes-intimas-otra-menor/.

23. developersFacebook. *Facebook developers, permisos login.* [En línea] 2017. https://developers.facebook.com/docs/facebook-login/permissions.

24. digicert. *capa de conexión segura.* [En línea] 2015. https://www.digicert.com/es/ssl.htm.

25. R. Dhamija, J.D. Tygar, M. Hearst,. *"Why Phishing Works", Conference on Human Factors in Computing Systems.* 2006.

26. SafeLayer. *Autenticación segura por capas. .* 2013.

27. Lab, Karpesky. Interempresas. *Kaspersky Lab descubre un nuevo ataque phishing en Facebook con 10.000 víctimas en dos días.* [En línea] 1 de Julio de 2016. https://www.interempresas.net/TIC/Articulos/169547-Kaspersky-Lab-descubre-nuevo-ataque-phishing-en-Facebook-con-10000-victimas-en-dos-dias.html.

28. Wikipedia. *Wikipedia.* [En línea] https://es.wikipedia.org/wiki/Malware.

29. EuropaPress. *'ImageGate', el ransomware que utiliza imágenes como anzuelo para infectar los equipos a través de Facebook.* [En línea] 28 de noviembre de 2016. [Citado el: 26 de mayo de 2017.] http://www.europapress.es/portaltic/socialmedia/noticia-imagegate-ransomware-utiliza-imagenes-anzuelo-infectar-equipos-traves-facebook-20161128183929.html.

30. Wikipedia. *Ramsomware.* [En línea] Mayo de 2017. [Citado el: 8 de Junio de 2017.] https://es.wikipedia.org/wiki/Ransomware#C.C3.B3mo_act.C3.BAa.

31. Oficina de seguridad del internauta. *OSI.* [En línea] 2017. https://www.osi.es/es/guia-de-privacidad-y-seguridad-en-internet.

32. OSI. *OSI.* [En línea] 2014 de Abril de 01. https://www.osi.es/es/actualidad/blog/2014/04/21/seguridad-y-privacidad-en-redes-sociales-ii-twitter-todo-lo-que-debes-sab.

33. Prateek Dewan, Ponnuragam Kumaraguru. *Detecting Malicious Content on Facebook.* Delhi : s.n., 2015.

34. Prateek Dewan, Shrey Bagroy, Ponnurangam Kumaraguru. *Hiding in Plain Sight: Characterizing and Detecting.* Delhi : Cybersecurity Education and Research Centre (CERC), IIIT-Delhi, 2016.

35. Paterva. *Maltego.* [En línea] 2017. https://www.paterva.com/web7/buy/maltego-clients/maltego-ce.php.

36. Blog. *Genear sentencias sql insert into en excel.* [En línea] 2013. http://blogs.itpro.es/exceleinfo/2013/06/24/generar-sentencias-sql-insert-into-en-excel/.

37. [En línea] http://franbarquilla.com/estado-internet-redes-sociales-2015-espana-estudio/.

38. [En línea] http://cms.ual.es/UAL/universidad/serviciosgenerales/stic/servicios/recomendaciones/redessociales/index.htm.

39. portaley. *portal ley.* [En línea] http://portaley.com/usuario/revista03092002.shtml.