Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Amenazas al personal de las FAS por medio de la ingeniería social, mediante ciberataques dirigidos, utilizando información adquirida de fuentes abiertas y redes sociales

Grado en Ingeniería Mecánica

ALUMNO: Álvaro Andrés de la Cuadra

DIRECTOR: Rafael Asorey Cacheda

CURSO ACADÉMICO: 2016-2017

Universidade Vigo

TODOS LOS DATOS E INFORMACIONES EMPLEADOS EN ESTE TRABAJO HAN SIDO OBTENIDOS LEGALMENTE EN LA RED, SIN EMPLEAR PROGRAMAS QUE IMPLIQUEN GASTO ALGUNO O FORMACIÓN ESPECÍFICA PARA SU MANEJO, LO QUE SIGNIFICA QUE DADO EL "CARÁCTER PÚBLICO" DE LOS MISMOS, CUALQUIER PERSONA CON UN NIVEL "USUARIO" PODRÍA ACCEDER A ELLOS.

Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Amenazas al personal de las FAS por medio de la ingeniería social, mediante ciberataques dirigidos, utilizando información adquirida de fuentes abiertas y redes sociales

Grado en Ingeniería Mecánica

Intensificación en Tecnología Naval

Cuerpo General

Universidade Vigo

RESUMEN

La falta de concienciación y sensibilidad en la información vertida a la red por los integrantes de las FAS ha situado al personal militar como eslabón más débil en la cadena de tecnologización de los ejércitos modernos. En este TFG se demuestran estas vulnerabilidades a través de la información obtenida de fuentes abiertas, sensible y susceptible de ser empleada para la ejecución de ciberataques dirigidos sobre el personal de las FAS. Además, se muestra la importancia de la ingeniería social como elemento base en la realización de ciberataques. La exposición finaliza con conclusiones que sirvan de ayuda al personal de las FAS en la reducción del vertido de información a la red.

PALABRAS CLAVE

Ingeniería social, OSINT, ciberataque, Fuerzas Armadas (FAS), Fuentes abiertas, *malware*

AGRADECIMIENTOS

En especial agradecimiento a J.A.D. y E.P.M. personal del CIFAS (Centro de Inteligencia de las Fuerzas Armadas) por su desinteresado apoyo y ayuda.
En agradecimiento a mi tutor, por animarme y orientarme durante el presente trabajo.
En agradecimiento al Capitán de Corbeta A.F.Q. por su apoyo y ayuda desinteresada.
En agradecimiento a mi familia y novia por apoyarme en este proyecto y en los acontecidos durante estos últimos cinco años.
Por último, agradecer a mi compañero y amigo J.G.C. el haber sido sufridor de un ataque y darme permiso para plasmarlo en el presente trabajo.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Presentación

Con el paso del tiempo y el desarrollo de las tecnologías, los conflictos del mundo moderno han tomado un cariz distinto: desde las grandes guerras de comienzo de siglo XX hasta las guerras actuales, el cambio ha sido significativo. El factor humano[1] sigue teniendo importancia, pero revestido de una importante componente tecnológica. Frente a esto, cobra importancia el axioma de "bajas cero"[2] a la vez que se va imponiendo con cada vez más fuerza la cuestión: "¿Será posible continuar atacando a un enemigo reduciendo mis bajas al máximo?".

Es de esta forma cuando en el siglo XXI nace la ciberguerra[3], y con ella los ciberataques[4]. Habrá una evolución en los objetivos. Se pasa de batir personas a batir infraestructuras críticas, entendiéndose por infraestructuras críticas aquellas a las que está supeditada la economía de un país. Todas ellas, hoy en día, equipadas con las últimas tecnologías, y de una u otra forma interconectadas.

Es con esa interconexión cuando llegan las vulnerabilidades, de carácter técnico y humano. En este trabajo se demuestra como este factor humano es una puerta de entrada al sistema global, como se constituye en un vector de ataque a las mismas y como la falta de mentalización del mismo es una garantía del fracaso.

1.2 Motivación

Hemos podido observar como las principales infraestructuras, objetivos potenciales, han desarrollado sus mecanismos de defensa, instalando medidas de seguridad tecnológica prácticamente infranqueables. Pero, ¿se ha tenido en cuenta el factor humano? Este trabajo no está dirigido a evaluar los parámetros de seguridad de las infraestructuras críticas, sino que se centra en demostrar que, independientemente de todos los parámetros de seguridad establecidos, es el hombre, a través de su falta de conocimiento, formación, así como motivación, el que puede constituir lo que hoy se denomina "puerta trasera" para alguien que ataque nuestra red de instalaciones, con los problemas

[1] Término que hace referencia al humano como herramienta en sí misma.
[2] Término que hacer referencia a no sufrir ninguna baja durante el desarrollo de una contienda.
[3] Neologismo que hace referencia a la guerra llevada a cabo a través de la red.
[4] Neologismo que hace referencia a los ataques sufridos a través de una plataforma cibernética.

añadidos de seguridad (personas e instalaciones) que acarrea, tanto para las FAS[5] como para los entornos familiares.

En la actualidad hay un gran volumen de información circulando. A mucha de ella no se le presta una atención o cuidado adecuado. Es por ello que la gran mayoría de los ataques de ingeniería social están basados en técnicas OSINT[6] (*Open Source Intellingence*). Aunque creamos que estamos protegidos, muchos de nuestros datos e información son de dominio y acceso público, como por ejemplo: cuentas de correo, cuentas de Skype, DNI, lugares de residencia o incluso nuestra localización actual. Este trabajo demuestra que se puede acceder a dichos datos mediante el empleo de motores de búsqueda y herramientas adecuadas o mediante la exploración de los metadatos[7] implícitos a las informaciones.

Aunque pensemos que podemos vivir de forma anónima, siempre que estemos conectados a la red, de manera directa o indirecta, se pierde la condición de "anónimo". Siempre que empleemos un teléfono móvil Android, IOS o similar se pierde el "anonimato". Siempre que usemos una red social, aunque solo se tenga a usuarios conocidos, perdemos la condición de "anónimo". Siempre que usemos un correo perdemos de nuevo nuestro "anonimato".

¿Es realmente el anonimato un factor importante en nuestra vida? En las Fuerzas Armadas, a medida que se adquieren responsabilidades, se convierte en lo que la OTAN[8] denomina un objetivo potencial. El paradigma de nuestra sociedad está en que si quieres pertenecer a la misma y quieres verte inmerso en ella has de formar parte de "la red". Esto lleva asociado un desprendimiento de la seguridad personal, y, lo que es peor, de la institución (en este caso las FAS) y, en muchos casos, la familiar y la de allegados.

Por todo esto, una de las conclusiones de este trabajo es la de optar por el "anonimato social" a medida que se asciende en el escalafón, siempre con el fin de buscar el bien de la organización y seguridad de los nuestros.

Con el objetivo de demostrar la valía o necesidad de ese anonimato, a lo largo de este trabajo se realizan investigaciones (tomando como base información accesible para cualquier ciudadano), cuyos resultados pueden emplearse contra el sujeto en particular o contra el colectivo de las FAS; entendiendo como tal: instalaciones, personal o la imagen de las FAS y de sus integrantes, sin olvidarnos de familiares o allegados. Podríamos tomar como base de partida la frase de la escritora C.J. Cherryh:

"El comercio no trata sobre mercancías, trata sobre información. Las mercancías se sientan en el almacén hasta que la información las mueve."

Somos información, la cantidad o calidad de la misma nuestra valía, pero la conclusión es que somos información. Se ha de tratar de cuidar hasta qué punto, si somos información, somos asequibles a aquellos que puedan actuar en contra de nosotros como individuos y en contra de las FAS.

Con todo ello se demuestra que el factor humano es el eslabón más débil de la cadena, el punto a partir del cual comienzan los ataques al sistema mediante la obtención de información asociada al mismo, siendo de nuevo la persona el centro del sistema. Por ello, es la necesidad de que los componentes del sistema se sientan parte del mismo (mediante su formación) lo que puede ser el origen del fracaso.

Independientemente de la diferencia de siglos, ¿son tan diferentes unas FAS del siglo XXI respecto a los ejércitos de Esparta? La respuesta es solo la diferencia de tecnología, que pasa de técnicas en las que se combinan lanza/escudo a las del siglo XXI, en las cuales se combinan

[5] Fuerzas Armadas.
[6] Procedimiento de obtención de inteligencia a través de fuentes abiertas.
[7] Conjunto de datos contenido dentro de un archivo.
[8] Organización del Tratado del Atlántico Norte.

ciberataques con ataques selectivos. El factor humano sigue siendo el mismo: formación, motivación y el espíritu de unidad.

1.3 Objetivos

Durante el desarrollo de este trabajo, se describe la cantidad de información que, asociada a los miembros de las FAS, se cataloga como sensible y que, como tal, puede emplearse para la ejecución de ciberataques. Estos mismos podrían lanzarse sobre su persona o sobre el colectivo de las FAS. Para ello, se ha empleado exclusivamente información de la red (OSINT):

- Páginas web como Shodan, Namechk, Tineye, Pipl, Tagboard, etc.
- Redes sociales como Facebook, Twitter, Instagram o LinkedIn, entre otras.
- Datos multimedia con sus respectivos metadatos.
- Foros, blogs, etc.
- Software[9] como FOCA, Maltego, Exiftool, etc.

El trabajo muestra distintas formas de realizar ciberataques, apoyados todos ellos en técnicas de ingeniería social accesibles en la red y en la información existente en la misma red. Se realiza un análisis de redes sociales en las que participa el personal de las FAS, que puede ser explotar cualquier individuo con acceso a la red. Del mismo modo se muestran las maneras más simples (no por ello eficientes) de articular un ataque. Por último, se indican procedimientos para evitarlo.

Por último, se resalta la importancia que tiene hoy en día la concienciación y sensibilización de los miembros de las FAS. Lo importante es no verter en la red "información innecesaria" y destacar las consecuencias nefastas que pueden darse sobre la seguridad.

1.4 Estructuración de la memoria

Este trabajo fin de grado consta de 6 capítulos y 2 anexos.

- En el capítulo 2 se analiza, tras una breve introducción general, el concepto de ingeniería social. Sobre este concepto se destacan los principales vectores de ataque, así como las principales herramientas con las que se contaría en la red para la realización de un ataque de ingeniería social. En este capítulo se tratan distintos ejemplos que se han dado en la actualidad y se profundiza en el concepto de inteligencia de fuentes abiertas (OSINT) y en los métodos y procedimientos que lleva asociado. Continua el capítulo con un análisis (desde punto de vista privacidad y la seguridad) de las redes sociales y en la repercusión que su empleo tiene sobre personal de las FAS, citando algunos ejemplos. Se concluye el capítulo 2 mostrando la vulnerabilidad potencial del personal de las FAS a sufrir un ciberataque.
- En el capítulo 3 se presenta el proceso mediante el cual se obtiene la información empleada en el trabajo y las distintas formas de acceder a ella. Además, durante el capítulo se lleva a cabo la elección de un sujeto de partida, se justifica su elección y se procede a la obtención de información de los sujetos adyacentes. Una vez obtenida dicha información, se eligen los que pudiéramos considerar como "principales", estudiándose sus vulnerabilidades. En este capítulo se presentan las redes sociales como repositorios de información, así como el empleo de determinadas herramientas (todas ellas en la red) para aumentar la cantidad y calidad de la información obtenida y las corroboraciones (contrastar información para darla

[9] Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en un ordenador.

como válida). Finaliza el capítulo mostrando un ataque sobre un sujeto objetivo, empleando para el mismo herramientas y conocimientos expuestos en el trabajo.

- En el capítulo 4 se interpretan los resultados obtenidos en el capítulo anterior. Además, se justifica el proceso seguido. En el capítulo 4 se lleva a cabo un análisis, basado en los estándares OTAN de las valoraciones de amenaza TESSCO[10] (terrorismo, sabotaje, subversión y crimen organizado) de los distintos sujetos obtenidos, de forma que se pueda ver la repercusión de la información obtenida en la red. Para finalizar el capítulo, se lleva a cabo una justificación del *malware*[11] empleado y el motivo de la elección del mismo.
- En el capítulo 5 se exponen las conclusiones obtenidas en el trabajo, se presentan los puntos débiles a mejorar y se realiza una breve valoración sobre la presencia del personal de las FAS en las distintas redes sociales. Se completa el capítulo con la exposición de posibles líneas futuras de trabajo y que pueden contribuir a la sensibilización del personal de las FAS.
- Para finalizar el TFG, se añaden dos anexos; Anexo I: Glosario de términos, que tratará sobre los principales términos utilizados y explicados durante el desarrollo de la memoria, y Anexo II: Ejemplos reales, con información ampliatoria del TFG con más ejemplos reales.

[10] Valoraciones que hacen referencia a las posibles amenazas surgidas del terrorismo, espionaje, subversión, sabotaje y crimen organizado.

[11] Abreviatura de "software malicioso", se define como un software destinado a acceder a un dispositivo de forma inadvertida.

2 ESTADO DEL ARTE

2.1 Introducción del apartado

En este capítulo se expone de dónde nace el concepto de ingeniería social, cuál es su historia y su relación con los ciberataques dirigidos, sobre lo que se apoya un ataque de ingeniería social (OSINT), cómo se relaciona la obtención de información con los ciberataques, las distintas medidas defensivas con las que cuentan las fuentes para protegerse en el ámbito de privacidad y obtención de información, así como afectan hoy en día dichos conceptos a España y, en particular, a las FAS.

Se expone cómo ha afectado el desarrollo de la ingeniería social para la creación de unidades u organizaciones dedicadas a la ciberdefensa, así como que clases de normativas internas existentes dentro de las FAS que regulan el vertido de información sensible. Tomando como base todo lo anterior, señalamos a qué clases de ataques son más susceptibles los miembros de las FAS, tomando en la mayoría de los casos como vector de ataque las redes sociales.

2.2 Ingeniería social

2.2.1 Concepto de ingeniería social

Se define "ingeniería social" como un conjunto de habilidades entre las que se incluye la manipulación de otros usuarios con el fin de obtener información no necesariamente confidencial, pero sí en la mayoría de los casos de carácter reservado ya que su conocimiento puede ser dañino para un usuario u organización. Se basa en los siguientes principios [1]:

- Reciprocidad.
- Urgencia.
- Consistencia.
- Confianza.
- Autoridad.
- Validación social.

Según uno de los ingenieros sociales más famosos, cuyo historial de ciberdelitos[12] basados en la ingeniería social le hizo ser perseguido por la justicia estadounidense, el *hacker* Kevin Mitnick expone que los pilares básicos para cualquier ataque de ingeniería social son [2]:

- Las ganas del ser humano por sentirse útil y ayudar.
- La confianza hacia el otro.
- Que a todo el mundo le encanta sentirse alabado.
- Que no nos gusta decir que no.

2.2.2 Ingeniería social como ciberarma[13]

Mucho antes del auge de Internet, existían los ataques de ingeniería social. Aunque su componente no fuera cibernético, muchos "ingenieros sociales" habían materializado sus ataques, en el mejor de los casos llamados "timos". Destacamos timos como la venta de la Torre Eiffel y el timo del entierro que consistía en engañar a una persona haciéndole creer que se necesitaba dinero para enterrar a un familiar lejano, pero a cambio de pagar su entierro, heredaría su fortuna. Si nos remontamos en la historia, hay otros ejemplos de engaños "estratégicos" como "el caballo de Troya". Al final, todos los engaños o timos consisten en presentarse como cordero, cuando al final se es lobo.

En la historia moderna ocurre lo mismo. Se ha pasado de emplear llamadas telefónicas como simples vectores portadores de un ataque al empleo de verdaderas herramientas cibernéticas, que emplean el vector Internet como portador del ataque.

A continuación, se resumen las principales técnicas empleadas en la ingeniería social [2]:

- Las basadas en hacking tecnológico o en ordenadores, que será sobre la que se centre este trabajo.
- Las basadas en la interacción humana.

Hay que remontarse al inicio de Internet para comprender la ingeniería social como ciberarma. En los inicios las redes tenían una estructura simple y con apenas seguridad en las comunicaciones; de forma que hacer "*sniffing*"[14] en la red se hacía con relativa frecuencia y con relativa facilidad. A través de esta técnica de espiar los paquetes transmitidos por la red se podía obtener nombres de personas, así como otros datos empleados en posteriores ataques de ingeniería social.

Si bien, desde el comienzo, los actores relacionados con la seguridad informática, conscientes del peligro, empiezan a desarrollar procedimientos de seguridad, no es hasta el año 2010 cuando surge en España el sentimiento de inseguridad. Así se comienza a desarrollar de manera institucional todo tipo de herramientas llamadas a implantar los primeros cánones de seguridad. En la empresa privada todo es más rápido y casi cinco años antes, apoyándose en compañías especializadas y de manera unilateral después, comienza a desarrollar sus procedimientos de seguridad. Sin embargo, la persona se sigue contemplando como un factor no sujeto a la técnica, ni a las innovaciones en seguridad, solamente sujeto a su propio "yo" y a la disciplina que sobre la materia se quiera imponer. Todo queda resumido en la siguiente cita de *hacker* Kevin Mitnick [3]:

"Una compañía puede gastar cientos de miles de euros en firewalls, sistemas de cifrado y demás tecnologías de seguridad, pero si un atacante engaña a un empleado, todo ese dinero no habrá servido para nada."

El bucle atacante/atacado es difícilmente detectable según el "Estudio de Ciberseguridad y Confianza en los hogares españoles", efectuado por el Instituto Nacional de Ciberseguridad (INCIBE)

[12] Neologismo que hace referencia a los delitos cometidos a través de la red.
[13] Neologismo que hace referencia a las armas utilizadas en el ámbito ciber.
[14] Efecto de capturar los paquetes que viajan dentro de una red.

y el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI). Así solo un 40% de internautas percibe ataques y robos de información [4].

De esta forma, estos ataques o robos primarios están dirigidos a obtener datos básicos, tales como nombre, correo o teléfono, básicamente mediante la detección de los mismos en la red.

Esos ataques ya no quedan reducidos a la obtención de datos básicos, sino de aquellos que permitan al atacante emprender una serie de acciones que podrían calificarse como delictivas.

Cabe destacar entonces que, ya que en la actualidad la mayoría de la población mundial tiene acceso a la red, es susceptible de sufrir un ciberataque y, debido al gran número de redes sociales y la interacción del ser humano con estas, el volumen de información a encontrar de una persona que tenga una vida en las redes sociales es mayor que una persona que carece de interacción con las mismas [2].

2.2.3 Principales vectores de ataque

A continuación, se introducen los principales vectores de ataque:

- *Eavesdropping:* Consiste en interponerse entre la comunicación de dos usuarios. La finalidad es recopilar información. Cuando se realiza sobre medios de la red se denominará "*network sniffing"* y, si se hace sobre una comunicación de voz digital, se trata de *"wiretapping"* [2].
- *Trashing:* Consiste en analizar los "desechos" de una entidad u organización físicamente, como accediendo al ordenador que pueda contener la información de "desecho" [2].
- *Shoulder surfing:* Aunque se traduzca el concepto como "mirar por encima del hombro", en este contexto consiste en el empleo de medios audiovisuales para captar información de interés. Un ejemplo es la intrusión en el circuito cerrado de cámaras de seguridad de una empresa determinada [2].
- *Office snooping:* Se trata de aprovechar un descuido de la víctima para acceder a su terminal y acceder a sus privilegios. Este ataque se puede complementar con el robo de cuenta y usuario de la víctima [2].
- *Phishing:* Consiste en acceder a información ajena, sin autorización de la víctima. Según Hispasec[15], el 66% de este tipo de ataques [5] se cuelga en webs comprometidas (no confiables) y utilizan los siguientes métodos [6]:

  -*Deceptive Phishing*: Se envía un correo electrónico "engañoso", haciéndose pasar por una compañía o empresa de confianza o conocida por la víctima de forma que el atacado confíe en el atacante, y siga sus indicaciones. El fin último del mismo es desviarle a un espacio fraudulento de forma que consiga entrar en su terminal. Es el ataque más efectuado. Lo normal es introducirlo a través del conocido como *"Malware-Based Phishing"*.

  -*Malware-Based Phishing*: Consiste en engañar al atacado para que ejecute, abra o inspeccione un archivo, o que ejecute la descarga del mismo, de forma que se ejecute automáticamente un *malware* en el ordenador víctima. Podemos encontrar numerosos ejemplos en la prensa diaria como el robo de cuentas a famosos, realizado por un ciberdelincuente en España [7].

  -*Keyloggers y Screenloggers*: Los *keyloggers* son programas que registran las pulsaciones del teclado o pantalla efectuadas por el atacado, de forma que le muestre los

[15] Organización informática dedicada a la seguridad informática.

resultados al atacante a través de internet. Los *screenloggers* sacan imágenes de la pantalla del atacado. Se han dado casos de introducción de *keyloggers* en cajeros automáticos [8].

-*Session Hijacking*: Consiste en obtener los datos de sesión de una página registrada por el software. Suelen relacionarse con las ventanas emergentes de los navegadores.

-*Web Trojans*: Es un software malicioso camuflado en una URL y camuflada como web legítima, de forma que el atacado ejecute el *malware*. Un ejemplo es el gusano "Myparty" [9].

-*System Reconfiguration Attacks*: Está basado en la modificación de parámetros como los servidores DNS. De esta forma se podría efectuar un *DNS Spoofing*[16] (*Pharming*).

-*Data Theft*: Son códigos maliciosos cuya función es recabar información del atacado.

-*DNS-Based Phishing (Pharming)*: Consiste en una modificación de la búsqueda de un nombre de dominio. Es decir, modificar fraudulentamente la resolución del nombre de dominio enviando al usuario a una dirección IP distinta [10].

-*Hosts File Poisoning*: Consiste en alterar el fichero *"Host"*[17], dentro del servidor DNS[18].

-*Content-Injection Phishing*: Es la introducción de "contenido ilegitimo" dentro de una web legítima.

-*Man-in-the-Middle*: Es una técnica que consiste en que el atacante se posiciona entre ordenador y servicios. A día de hoy, este método es uno de los más utilizados [11].

-*Search Engine Phishing*: Consistente en buscadores falsos que llevan al atacado a sitios ilegítimos.

-*Backdoor*: Es la creación de una puerta trasera, que permite entrar en la máquina víctima como si tuviésemos todos los permisos del atacado. No solo se entiende por máquina un ordenador, ya que se podría dar casos de que fuese una cámara, como le ocurrió a Sony en 2016 [12] o un terminal telefónico.

2.2.4 Herramientas para un ataque de ingeniería social

A lo largo de este apartado vamos a exponer las principales herramientas diseñadas exclusivamente para ingeniería social. Aunque en la actualidad hay numerosas herramientas enfocadas a la ingeniería social, muchas de ellas dejan de ser útiles para el usuario cuando es necesario realizar un aporte económico para su adquisición, o cuando el software base para realiza los ataques es Windows, ya que su carácter comercial ha lo convierte en un sistema operativo con escasas capacidades. Es por ello, por lo que prácticamente la totalidad de las herramientas emplean Linux como sistema operativo.

[16] Método para alterar las direcciones de los servidores DNS que utiliza la potencial víctima y de esta forma poder tener control sobre las consultas que se realizan.

[17] Archivo utilizado por Windows para asociar nombres de dominio con direcciones IP.

[18] *Domain Name System* - Sistema de nombres de dominio. Es un servidor que traduce nombres de dominio a IP y viceversa. En las redes TCP/IP, cada PC dispone de una dirección IP para poder comunicarse con el resto de PC.

- SET (*Social Engineer Toolkit*): Es un conjunto de herramientas para realizar tareas tales como *spam*[19], *spear phising*[20], crear puntos de acceso Wi-Fi [21] falsos, etc.

  El poder de la herramienta radica en la facilidad de su uso, pudiendo realizar complejos ataques con sencillos pasos. Tiene como característica que, para la realización de ciertos ataques, es necesario el uso de *Metasploit*[22], programa preinstalado en sistemas operativos como Kali Linux[23] [13].

  La portada de la herramienta se puede ver en la Figura 2-1.

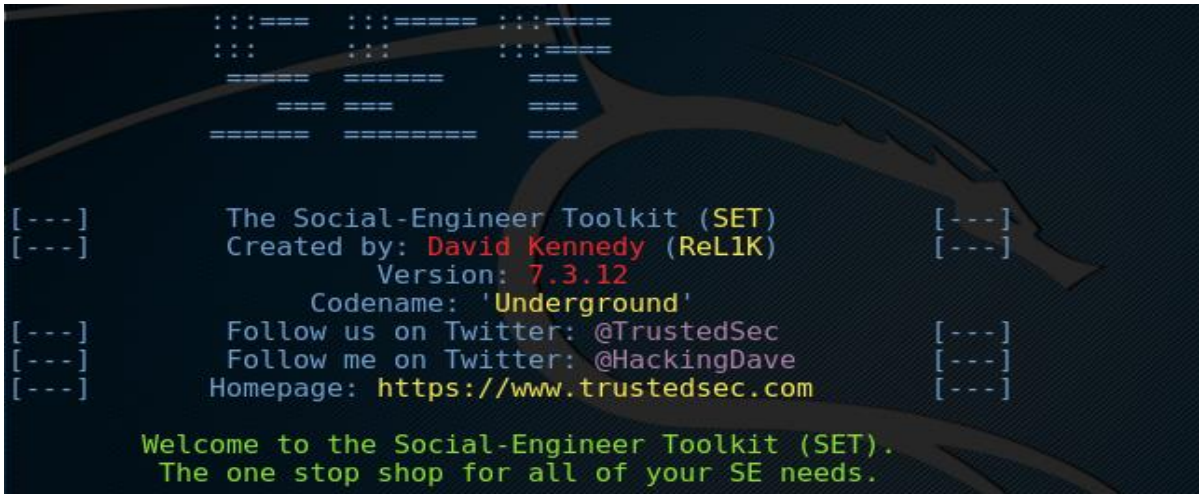


Figura 2-1 Herramienta SET (Social Engineering Toolkit).

La Figura 2-2 muestra los distintos ataques que ofrece la herramienta.

Figura 2-2 Menú principal.

Para la realización de cualquier ataque, van a existir dos configuraciones básicas:

[19] Correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales.

[20] Consiste en crear un correo electrónico que aparenta ser de una persona o empresa conocida, con el fin de introducir un malware en la plataforma objetivo.

[21] Área física en la cual se puede conectar un equipo con capacidades Wi-Fi.

[22] Es un proyecto de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad.

[23] Sistema operativo utilizado para realizar pruebas de seguridad, así como auditorias de seguridad.

-Utilizando los múltiples *payloads*[24] y *exploits*[25] que proporciona la herramienta, pero siendo conocedor de la existencia de vulnerabilidades ya conocidas en estos.

-Crear ataques personalizados mediante *exploits* propios y a través de la utilización de *encoders*[26] en estos.

Tras el uso de la herramienta, podemos concluir que la misma:

-Nos permite enviar correos electrónicos en forma de *spam*, o incluso enviar un archivo adjunto, camuflando en este una conexión que se crea al abrir la victima el archivo. De esta forma, el comienzo del ataque consiste en enviar un documento de valor a la víctima y que esta, tras reconocerlo, proceda a su apertura.

-Nos permite utilizar como vector de ataque una web para vulnerar la máquina de la víctima. Permite clonar una página o redirigir a una falsa con el objetivo de obtener las credenciales de la víctima.

-Permite infectar un dispositivo de almacenamiento, consecuencia de almacenar en el dispositivo un *autorun*[27], que puede ir camuflado o no en un archivo, o simplemente ejecutarse al insertar el dispositivo. De esta manera se abre entre víctima y atacante una conexión gracias a los *payloads*. Por su eficacia y simpleza es uno de los métodos más utilizados a día de hoy, basando su eficacia en la falta de concienciación de las personas que, tras toparse con un elemento desconocido, lo almacenan en su ordenador.

-Permite crear, de manera guiada y sin necesidad de grandes conocimientos, ejecutar tus propios *payloads*.

-Permite enviar correos electrónicos de forma masiva, como en casos anteriores, pero para más de un destinatario.

-Permite utilizar dispositivos *Teensy*[28] para infectar una máquina remota. Sería parecido a infectar un dispositivo de almacenamiento externo, con la diferencia de que ahora no adjunta ningún tipo de archivo. Se trata de un dispositivo que, tras su manipulación ejecuta un código malicioso en función de otros parámetros.

-Permite crear y configurar un punto de acceso Wi-Fi falso, sirviendo de base para realizar ataques de ingeniería social sobre el resto de usuarios. Con ello capturaríamos conexiones o ejecutaríamos diversas técnicas de *spoofing*.

-Permite crear actividad maliciosa a través de códigos QR[29], haciendo que dicho código, al ser escaneado reconduzca a la descarga de una aplicación, página o similar. El objetivo es obtener de la víctima información personal y privada. Se trata de un ingenioso ataque de ingeniería social, que va cobrando cada vez más víctimas debido al uso de dichos códigos.

-Permite atacar a la *Powershell*[30], permitiendo que se pueda insertar códigos maliciosos en esta, y consiguiendo un volcado masivo de datos [2].

- *Pineapple:* Denominado "la piña", se trata de un dispositivo físico que se utiliza como herramienta de análisis de redes inalámbricas. Está en proceso de expansión, en cuanto a su

[24] Parte del malware que realiza la acción maliciosa.
[25] Programa o código que se aprovecha de un agujero de seguridad (vulnerabilidad) en una aplicación o sistema.
[26] Programa utilizado para convertir una información de un formato a otro.
[27] Capacidad de un sistema/programa/archivo de ejecutarse sin la necesidad de interactuar con él.
[28] Pequeño microcontrolador HID programable con interfaz USB que permite emular un teclado y mouse para enviar comandos a cualquier sistema operativo.
[29] Módulo que permite almacenar información en una matriz de puntos.
[30] Terminal de un sistema operativo.

utilidad se refiere, y su comunidad de usuarios no es tan grande como los que puedan tener otras herramientas.

Este dispositivo es capaz de realizar distintos ataques Wi-Fi como *DNS spoofing*, *phising*, *MITM*[31], *Fake AP*[32] (*Rogue Ap*).

El objetivo es crear un punto de acceso falso para realizar todas las actividades citadas en el párrafo anterior. Observamos que presenta utilidades similares a las citadas en SET, si bien su grado de sofisticación y sigilo son mucho mayores. Por su tamaño y apariencia física, puede hacerse pasar por un disco duro externo [14] [2].

- *Honeypots:* Es una de las principales técnicas de ingeniería social inversa. Su objetivo principal es hacerse pasar por un sistema vulnerable, atrayendo a *hackers*, con la intención de que estos realicen un ataque sobre las víctimas. De esta forma, la falsa víctima podría saber las distintas técnicas utilizadas por los atacantes para vulnerar su propio sistema.

  En la actualidad, se conoce en la comunidad *hacker* que distintos organismos de las Fuerzas y Cuerpos de Seguridad del Estado utilizan *Honeypots* con la intención de localizar y detener delincuentes, pederastas, terroristas, traficantes, etc.

  Por último, destacamos como herramienta para la creación de *Honeypots*, la distribuida por Linux exclusivamente para tal finalidad. Se conoce como Kippo. Permite crear un servicio SSH que, actuando a modo de anzuelo, registra cada uno de los comandos que el atacado introduce, guardando los mismos en una base de datos [2].

2.3 OSINT

2.3.1 Concepto de OSINT

Del inglés *"Open Source Intelligence"* hace referencia a la "inteligencia de fuentes abiertas". Es un procedimiento de obtención de información. Dicha información se caracteriza por ser accesible a cualquier tipo de individuo [15].

En la Figura 2-3 se puede ver el ciclo de la inteligencia, del que forma parte OSINT, contenida dentro de la fase de obtención.

Figura 2-3 Ciclo de la inteligencia [16].

[31] (*Man In The Middle*) ataque consistente en situarse entre usuario y sistema.
[32] Punto de acceso Wi-Fi falso.

Es importante señalar que, junto a otros procedimientos de obtención de información como HUMINT (*HUman INTelligence*)[33], IMINT (*IMage INTelligence*)[34], SIGINT (*SIGnal INTelligence*)[35] o MASINT (*Measurement and Signature INTelligence*)[36] forman parte de la segunda fase del ciclo de inteligencia (obtención de información) y que, en combinación con el resto (difusión , análisis y elaboración), constituye el ciclo de todo procedimiento destinado a elaborar un producto de inteligencia, primero de los niveles a alcanzar en todo proceso de toma de decisiones [16].

También es importante resaltar que todo proceso de obtención de información se doble. Es decir, se combine al menos dos de ellos. Lo normal, hoy en día, es que uno sea OSINT. De no hacerse de esta manera, el analista de inteligencia no contaría con información contrastada, lo que haría que su producto perdiese objetividad (entre otras cosas) y, en lugar de proporcionar al mando un producto de inteligencia destinado a apoyar su decisión, le estaría proporcionando una "opinión", lo que podría acarrear graves consecuencias, como el ejemplo de las armas de destrucción masiva en la guerra de Irak [17].

En la Figura 2-4 se puede ver que el concepto "inteligencia", se apoya en los procedimientos de obtención citados.

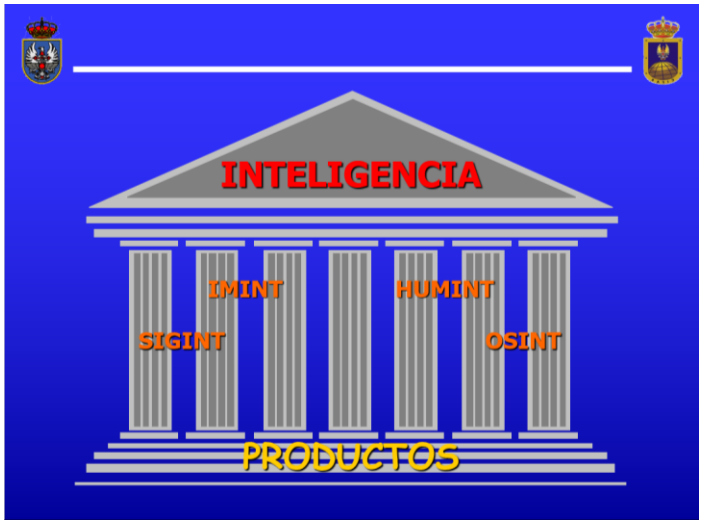


Figura 2-4 Pilares de la inteligencia [18].

De manera general, se puede decir que OSINT sirve como punto de partida para la primera fase de búsqueda de información sobre el objetivo.

2.3.2 Nacimiento de OSINT como método de obtención de información

Se empiezan a tener las primeras referencias de OSINT como concepto en 1988, de mano de la inteligencia militar estadounidense (DIA, *Defense Intelligence Agency*). Es entonces cuando, al General de los Marines Alfred M. Gray Jr se le encomienda la elaboración de inteligencia básica sobre nuevas áreas de operaciones potenciales. Es en esa compilación masiva de información cuando se recurre al OSINT, a la información vertida a la red.

En noviembre de 2005, el entonces director de la DIA, anuncia la creación del OSC (*Open Source Center*). Este centro absorbería al ya existente desde 1941 FBIS (*Foreing Broadcast Information Service*) [17], siendo su misión general la compilación de información existente en Internet, prensa,

[33] Procedimiento de obtención de inteligencia a través de humanos.
[34] Procedimiento de obtención de inteligencia a través de imágenes.
[35] Procedimiento de obtención de inteligencia a través de señales(electromagnéticas).
[36] Procedimiento de obtención de inteligencia a través de mediciones y firmas electrónicas.

radio, TV, bases de datos abiertas, publicaciones especializadas (por ejemplo, geoespaciales), publicaciones tecnológicas, etc. En definitiva, recolectar toda la información a la que podría acceder un ciudadano normal en el mercado.

Así, según los expertos, hoy en día el 90% de la información está en las fuentes abiertas, encontrándose sin compilar, tratar y relacionar. Este es el gran reto del siglo XXI. La diferencia ahora, en el mundo de la inteligencia, no va a estar en acceder a la información, sino contar con ella en unos plazos de tiempo acotados, que permita tomar decisiones a tiempo.

En España, las FCSE (Fuerzas y Cuerpos de Seguridad del Estado) y el CNI (Centro Nacional de Inteligencia), cuentan con departamentos y divisiones dedicadas exclusivamente al OSINT. Dentro de las FAS españolas, hay dos estructuras (ambas dependientes del JEMAD, Jefe del Estado Mayor de la Defensa) con departamentos dedicados a este procedimiento: CIFAS (Centro de Inteligencia de las Fuerzas Armadas) y el MCCD (Mando Conjunto de Ciber Defensa).

Los objetivos que ambos persiguen dentro de OSINT son completamente diferentes. Aunque comparten técnicas y procedimientos, el primero dedica su esfuerzo OSINT a la obtención de información destinada a satisfacer las necesidades del JEMAD y el segundo a la obtención de información dirigida a evitar cualquier tipo de ataque o intrusión en los sistemas de mando y control de las FAS.

2.3.3 Métodos y herramientas de obtención

Dentro del gran abanico que es el OSINT, encontramos diversos tipos de fuentes. Así, podemos hablar de medios de comunicación, información pública, bibliotecas en línea, foros, redes sociales, blogs, etc. Todos y cada uno de ellos aportan información para ser posteriormente analizada.

La Figura 2-5 muestra las distintas fases de las que está compuesta OSINT.

Figura 2-5 Fases OSINT [19].

Es dentro de este gran volumen de información en el que existirán diferentes herramientas que nos permitan su análisis y explotación. Es de nuevo importante resaltar que todas las herramientas a continuación expuestas están en la red y son de acceso libre y gratuito, siendo las más importantes:

- Maltego: Se considera como la principal herramienta de minería de datos disponible en el mercado. Cuenta con diversas versiones y con softwares independientes. Dichas versiones

van desde la más básica gratuita hasta la comercial XXL. La principal diferencia está en la cantidad de información que nos muestra. Es decir, no se muestra toda la información disponible, a no ser que queramos comprar una de sus versiones de pago [2].

Otra de las principales diferencias de esta herramienta con el resto de herramientas es la forma gráfica en la que muestra la información, haciendo incluso diferencia de colores con leyenda para su uso.

La información principal que podemos obtener de la versión gratuita tiene un máximo de doce saltos de información sobre el objetivo a buscar: direcciones de correo electrónico, redes sociales, dominios, empresas relacionadas, números de teléfono, artículos de internet relacionados con la búsqueda, relaciones entre las IP buscadas [20]. Un ejemplo se muestra en la siguiente Figura 2-6 [21]:

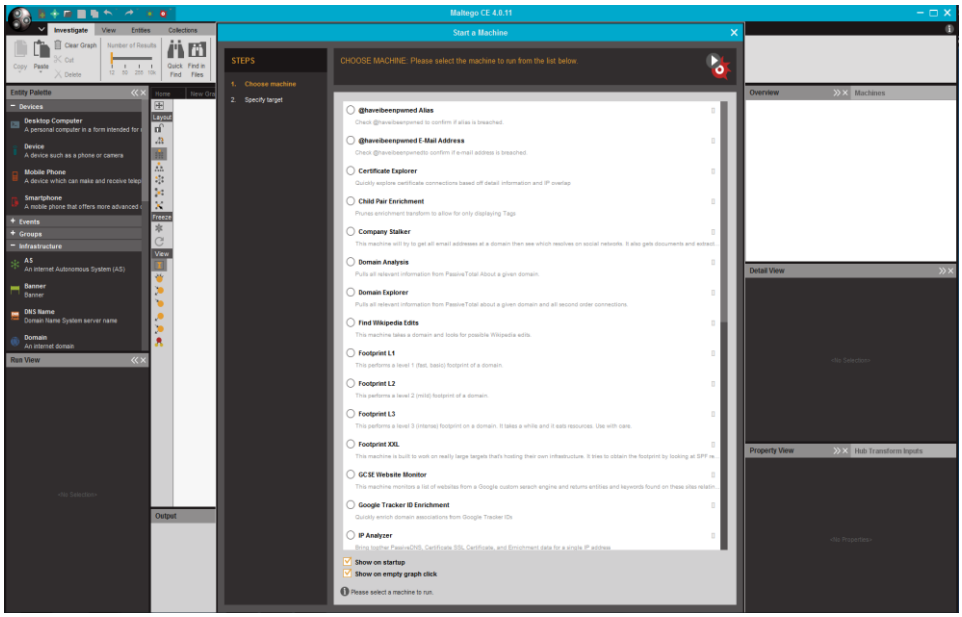


Figura 2-6 Menú principal de Maltego.

Maltego permite comenzar la búsqueda con un simple dominio, con un correo, con un usuario, con nombre y apellido, a través de las redes sociales, o a través de una geolocalización tras de un mensaje expuesto en Twitter.

- FOCA (*Fingerprinting Organizations with Collected Archives*): Es una herramienta perteneciente a ElevenPaths que tiene como finalidad la obtención de metadatos de archivos y documentos. De dichos metadatos se obtiene: nombres de usuarios, geolocalización, sistemas operativos y correos electrónicos.

  Sirve de valiosa ayuda para realizar un ataque de ingeniería social, ya que en el caso de que se partiese de la información contenida en una fotografía, el atacante sería capaz de conocer la marca, modelo, SO y geolocalización de la fotografía. Destacar que las principales redes sociales, realizan un borrado de metadatos, pero esto no las exime a las propias redes sociales de la utilización de los mismos. Es bien sabido que las principales redes sociales son capaces de geolocalizarnos y tras ello compartirlo con nuestros contactos, aunque nuestra geolocalización esté apagada. En el caso de que sea un documento (Microsoft Office, Open Office, PDF, etc.) lo que se analice, seremos capaz de sacar nombres de usuarios, creadores del documento, metadatos de las imágenes contenidas, contraseñas, fechas de creación, modificación, compañía que lo creó, etc [22].

En la Figura 2-7 se puede ver la pantalla de inicio de la herramienta.

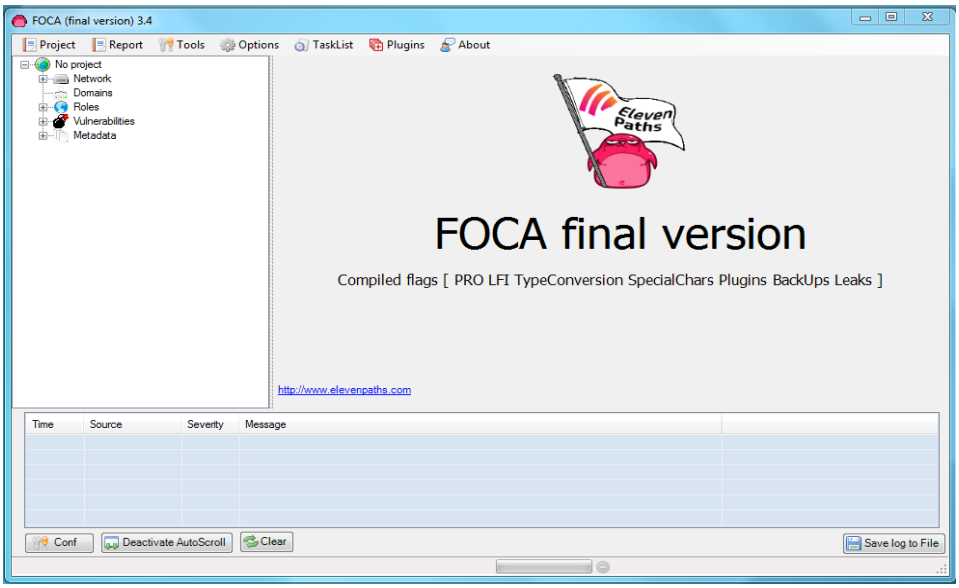


Figura 2-7 Interfaz FOCA.

FOCA no solo trabaja con archivos que se tienen dentro del sistema, cuenta con un apartado con capacidad de mostrar los hábitos de navegación de los integrantes de una empresa (dentro de su propio servidor DNS) [23], mediante los nombres almacenados en caché[37] como se puede ver en la Figura 2-8.

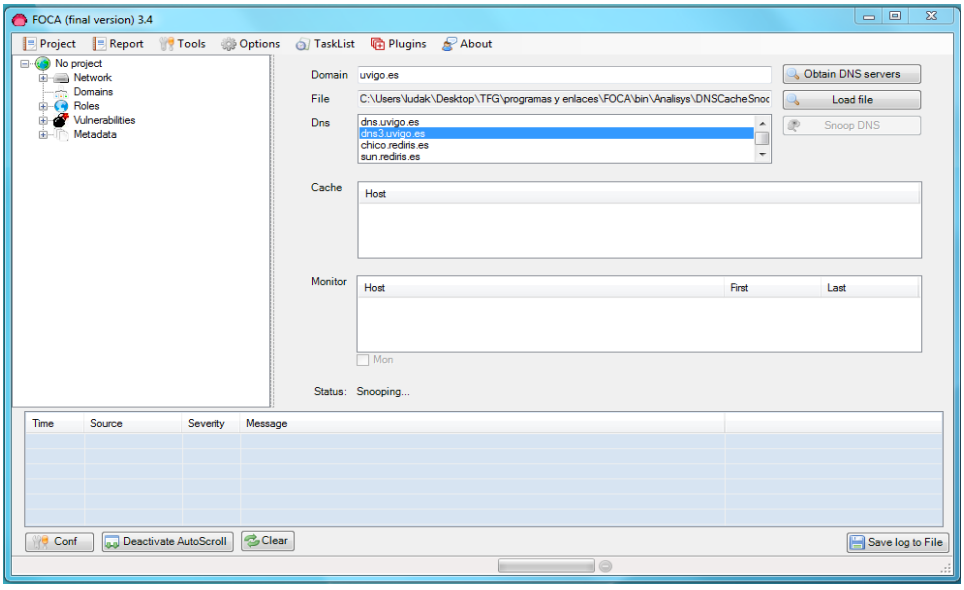


Figura 2-8 Funcionalidades de FOCA.

FOCA cuenta también con la posibilidad de buscar información directamente a través de tres buscadores: Google, Bing y Exalead, facilitando en trabajo de los denominados Google Dorks, explicado en el siguiente aparatado.

En España, cabe destacar que el uso de información relevante en los metadatos, viene legislada según la Ley 18/2011 de 5 julio [24].

[37] Área de almacenamiento dedicada a la recuperación a gran velocidad de los datos usados o solicitados con más frecuencia

- Google Dorks: Consiste en hacer una búsqueda avanzada en Google, tomando como base la información que Google ha indexado, de forma que la búsqueda se afine, hasta lograr la información deseada.

  Entre la información que se puede obtener, mediante el filtrado, hallaremos documentos confidenciales, nombres de usuarios, contraseñas, números de teléfono, perfiles, contenido privado, acceso a cámaras de seguridad, tablas de código o tablas de Excel [25].

  Para una mejor navegación, la Figura 2-9 destaca los parámetros a utilizar.

Búsqueda de:	Parámetros	Ejemplo
Palabra(s) dentro de un texto	*Allintext:*	*Allintext: Operaciones en el mar*
Encuentra dentro de la búsqueda la palabra deseada	*intext:*	*operacion intext: cifas*
Busca en el título del navegador	*Allintitle:*	*Allintitle: Operaciones en el mar*
Busca palabras que se utilizan para enlazar a otra pagina	*Inanchor:*	*Inanchor: cifas*
Búsqueda en el nombre de la url	*Inurl:*	*Inurl: cifas*
Busca en o fuera de los sitios	*(-)Site:*	*Site:.es o allintext: cifas -site:.es*
Buscar por documentos	*Filetype: (pdf,doc,....)*	*Operaciones en mar filetype:doc*
Paginas similares	*Related:*	*Related: www.emad.mde.es*
Muestra información de la pagina	*Info:*	*info: www.emad.mde.es*

Figura 2-9 Uso de Google Dorks [18].

Resaltar que existen páginas web que recopilan toda la información de carácter "relevante" para los atacantes potenciales.

En la siguiente Figura 2-10 se puede ver el ejemplo de una de las búsquedas realizadas.

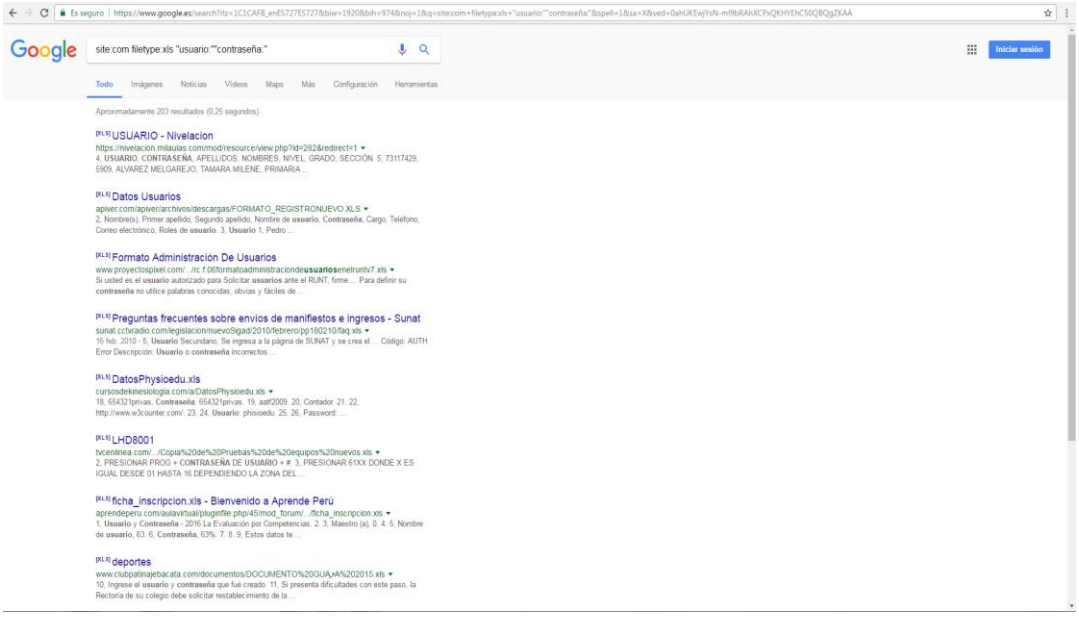


Figura 2-10 Ejemplo Google Dorks.

- Creepy: Es una herramienta que permite la geolocalización a través de las redes sociales como Google+, Instagram, Twitter y Flickr.

  Una vez hecha la búsqueda, se puede ver la interactuación del objetivo con las redes sociales (comentarios, tuits, etc.) así como sus fotos y nombre de usuario [26].

  A continuación, en la Figura 2-11 se puede ver un ejemplo de localización.

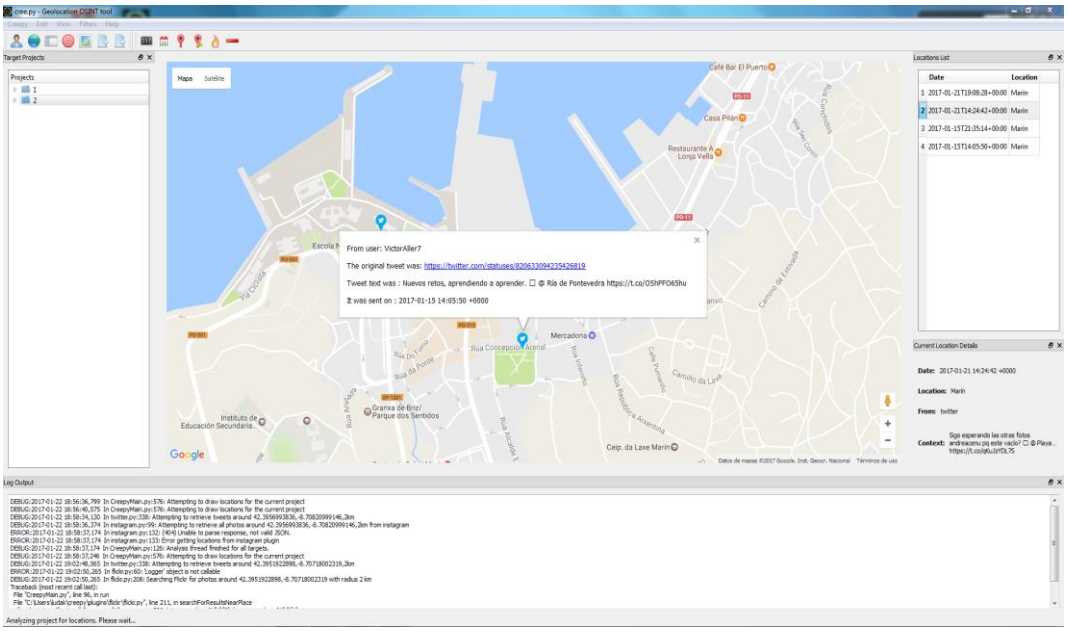


Figura 2-11 Ejemplo localización con Creepy.

- TheHarvester: Es una herramienta de Linux que trata de obtener información sobre correos electrónicos, subdominios, equipos, nombres de empleados, puertos abiertos, banners, etc. Utilizando fuentes públicas como motores de búsqueda, la red social LinkedIn y la base de datos de SHODAN (buscador de dispositivos conectados a Internet) [27].

  En la Figura 2-12 se puede ver la interfaz inicial de la herramienta.

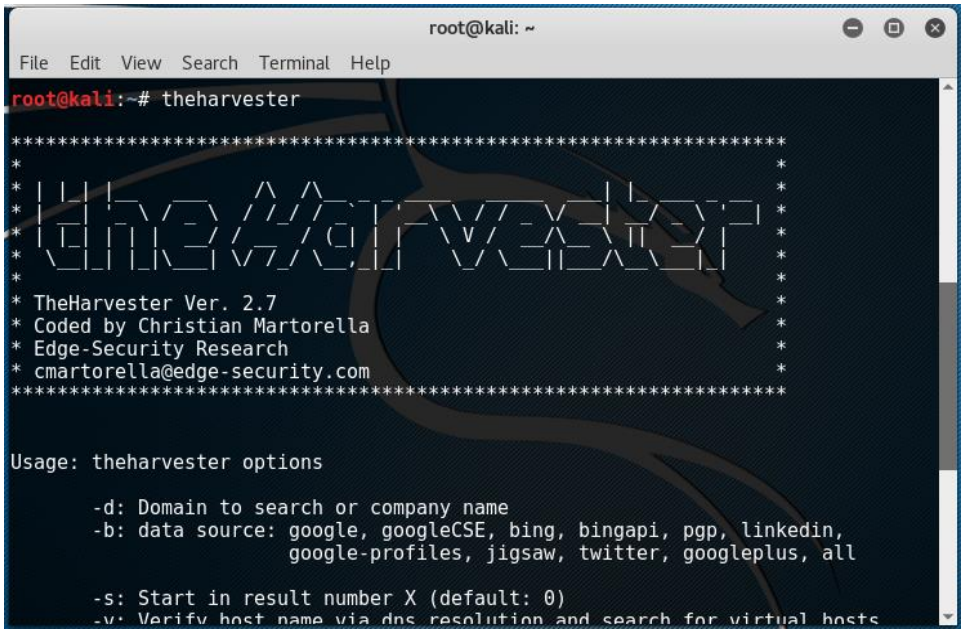


Figura 2-12 Interfaz de TheHarvester.

- Dmitry: Es una herramienta que obtiene toda la información de un dominio. Esta información es de gran relevancia si solo se conoce la dirección web pudiendo obtener el contacto del dominio, la fecha de alta del dominio, fecha de expiración del mismo, el correo electrónico, teléfono e incluso ubicación física si este correspondiera a alguna empresa. Sus búsquedas, en gran parte, se materializan en Ripe.net[38] [28] pero entre la gran cantidad de datos aportados, solamente extrae el nombre, el teléfono, así como la dirección física.
- Otras herramientas: Las anteriormente nombradas son las principales herramientas de OSINT, utilizables para realizar una búsqueda sobre personal, correos, organizaciones y demás. Sin embargo, existe otra gama de herramientas, como Shodan, que permite buscar dispositivos conectados a la red, con una configuración de seguridad errónea [29]. Además, también podemos encontrar páginas en Internet [30] especializadas en herramientas de OSINT en línea, así como otras cuyos menús desplegables permiten acotar la búsqueda [31] también en línea. Sin embargo, y de manera general su precisión es menor que los softwares anteriormente citados.

2.3.4 Información obtenida por OSINT

Después de revisar las principales herramientas dentro del ámbito de OSINT, así como la cantidad de información que estas nos pueden proporcionar, se realiza un estudio sobre la posibilidad de ser "objetivo" exclusivamente tomando como base la información obtenida en fuentes abiertas.

Hoy en día, cualquier persona que tenga un perfil o interactúe a través de redes sociales o de la red, es prácticamente imposible que lo haga de forma anónima, o que sus datos no puedan obtenerse de una forma sencilla. Direcciones de correo, junto con números de teléfono e información anexada a los metadatos inclinan la balanza para pasar a ser un objetivo potencial para un atacante. Es cierto que otras informaciones, tales como nombres de usuario o software empleados son importantes, pero ahora pierden parte de su valor frente a los ataques que se proponen.

Pasamos a enumerar el tipo de información que podemos considerar útil para los ataques posteriores [2]:

- Usuarios y contraseñas.
- Direcciones de correo electrónico.
- Números de teléfono.
- Información de la IP.
- Geolocalización.
- Detalles personales.
- Otros (a toda esta información se le podría añadir la proporcionada tras los fallos de seguridad, software empleado o sistemas operativos, para poder tener un amplio abanico de posibilidades).

Mención aparte le corresponde a la información procedente de imágenes satélite. Hoy en día podemos encontrar una gran variedad de empresas dedicadas a suministrar este material para usos diversos. Los mismos fines van desde usos catastrales, expansión de cultivos, localización de minerales, etc.

Sin embargo, si nos focalizamos en imágenes de carácter militar, las mismas quedarían fuera de lo que estamos tratando como OSINT, ya que estas no se encuentran (a no ser que se haya procedido a su descatalogación) en fuentes abiertas.

[38] Página dedicada a dar información sobre IP/usuarios, así como controladores de redes.

Otra cosa es que a partir de una fotografía "comercial" un analista militar llegase a unas determinadas conclusiones. Son estas las que no aparecen en fuentes abiertas, ya que son de carácter "clasificado", pero no el soporte gráfico [16].

2.4 Redes sociales

2.4.1 Introducción a las redes sociales

Según la Real Academia Española (RAE), se define "red social" como: "plataforma digital de comunicación global que pone en contacto a gran número de usuarios [32]". Cabe destacar que es el siglo XXI, el que ha sido bautizado como el gran siglo de las comunicaciones ya sea por los adelantos en las plataformas de telecomunicaciones como las plataformas cibernéticas para el desarrollo de las mismas.

Aunque hayan supuesto un novedoso avance para las comunicaciones, a día de hoy las redes sociales no solo nos favorecen la relación entre usuarios, sino que su capacidad se extiende más allá, llegando a ofrecer video, audio o fotografía en ese intercambio "social"; elementos que favorecen que redes sociales sean un campo de búsqueda para delincuentes. Es por ese motivo por lo que diferentes departamentos de la administración empiezan a dictar normas para evitar que sus trabajadores puedan ser objeto de cualquier ataque [33].

Las redes sociales favorecen en la actualidad las movilizaciones llevadas a cabo por los usuarios para apoyar o denunciar un hecho. Son también utilizadas por personajes públicos relevantes para difundir mensajes. No es extraño ver en la actualidad a los políticos u otros personajes cruzar declaraciones utilizando dichos medios.

Es también destacable el auge de la utilización de las redes sociales por organizaciones terroristas convencionales como veremos más adelante.

El comienzo de las redes sociales está ligado al comienzo de Internet. Hoy en día se cuentan por cientos este tipo de plataformas, abriéndose un abanico más amplio que la simple mensajería. Se consideran redes sociales plataformas como YouTube, WhatsApp, SoundCloud entre otras.

Atendiendo a su objetivo podremos distinguir entre las siguientes redes:

- Contactos: Badoo, Match, Tinder.
- Mensajería: WhatsApp, Telegram, Twitter.
- General: Facebook, Instagram, Tumblr.
- Música/foto/video: Flickr, Spotify, Soundhound, SoundCloud, YouTube.

Durante el desarrollo del trabajo, nos centramos en las denominadas redes sociales puras, siendo estas Facebook, Twitter, Instagram y LinkedIn. Añadimos WhatsApp como elemento básico de comunicación y no como fuente, que se considera como red social en proceso, aunque su uso como tal se encuentre en debate en la actualidad.

2.4.2 Plataformas utilizadas

- Facebook: Considerada como la red social por excelencia, tiene como fecha de creación el año 2003, aunque la versión inicial de esta dista mucho de la realidad actual. En sus orígenes era una red destinada al alumnado de la universidad de Harvard pero que ha llegado a expandirse hasta contar en la actualidad con más de 1500 millones de usuarios y traducida a más de 70 idiomas. En la actualidad se encuentra bajo censura política en

aquellos regímenes en los que se carece de libertad de expresión, o incluso está perseguida, como pueden ser China, Irán o Corea del Norte, entre otros [34].

Las ofertas de esta red social han crecido con el paso de los años, incorporándose nuevas opciones de uso para los usuarios y no ciñéndose a un uso exclusivo de un simple *chat* o intercambio de fotografías como sí han hecho otras redes sociales. Su crecimiento y la incorporación de nuevos usos, sirve de referencia a otras redes sociales con menor número de usuarios.

A continuación, en la Figura 2-13 se puede ver el logotipo de Facebook:

Figura 2-13 Logotipo de Facebook [35].

La franja de edad que predomina en el uso de esta red social está entre los 18-29 años, seguido de la franja de los 30-49 años [36]. Dentro de Fuerzas Armadas su uso es amplio, siendo más normal entre integrantes más jóvenes.

Con el paso del tiempo y a medida que Facebook ha ido creciendo, ha ido adquiriendo otras redes sociales como Instagram, WhatsApp, así como diversas tecnologías, como realidad virtual o reconocimiento facial. Sin embargo, con el paso del tiempo, Facebook ha tenido graves problemas de seguridad y la privacidad de los usuarios de la red habría quedado al descubierto en más de una ocasión [37].

Como consecuencia de lo anterior, la propia red ha sido la encargada de ir proporcionando mayores garantías de seguridad y privacidad a sus usuarios, aunque la red almacena automáticamente datos como fotos, correos electrónicos, números de teléfono, etc. Tiene prohibido cualquier negocio con la información de sus usuarios, pero sí se permite el uso de esta, como se recoge en uno de los siguientes términos legales que los usuarios han aceptado por defecto:

"Usted le otorga a Facebook el derecho irrevocable, perpetuo, no exclusivo, transferible y mundial (con la autorización de acordar una licencia secundaria) de utilizar, copiar, publicar, difundir, almacenar, ejecutar, transmitir, escanear, modificar, editar, traducir, adaptar, redistribuir cualquier contenido depositado en el portal" [38].

Sucesivamente Facebook ha ido incorporando medidas de privacidad y seguridad para sus usuarios, permitiéndole a estos cambiar configuraciones de seguridad como apariencia del muro, códigos de verificación, información al correo de si alguien utiliza un usuario indicando incluso la IP y la localización desde la que se realizó la búsqueda.

Otras de las medidas que la red social ha llevado acabo es el borrado masivo de información anexada en los metadatos [39]. Esto significa que una vez que se sube una foto o vídeo, queda registrado dentro de los servidores de Facebook, y borra cualquier información contenida en los metadatos de la foto, como usuario, modelo de cámara o móvil, geolocalización, etc.

A día de hoy, Facebook sigue teniendo motivos suficientes para preocupar a los usuarios en lo que a su privacidad se refiere. No es por el borrado de datos o la utilización que puedan hacer de los mismos, ni porque los usuarios den acceso a Facebook a sus archivos personales, con las posibles filtraciones de los mismos. Hoy en día preocupa más el cariz de inteligencia artificial que se le ha otorgado a la red social, permitiendo que ella misma

(a través de modelos matemáticos [40] y mediante la vinculación de cuentas) nos sugiera amistades. esto hace pensar al usuario hasta qué punto puede conocernos Facebook y hasta qué nivel dentro de la red es capaz la aplicación de llegar.

Como curiosidad para el desarrollo del presente trabajo, se llevó a cabo la apertura de un perfil falso de Facebook, para lo cual se usaron imágenes de fuentes abiertas con el fin de hacer un perfil creíble. Sin embargo, tras un periodo de uso de la cuenta el propio sistema de Facebook pidió la identificación positiva de la misma. Es decir, solicitó enviar un documento que acreditase que dicha cuenta estaba relacionada con un usuario real. Dicho acontecimiento es un punto a favor en lo que a privacidad y seguridad se refiere.

En este punto surge la siguiente pregunta: ¿realmente es necesario que la aplicación piense por sí sola e intente facilitar las comunicaciones a costa de nuestra privacidad? ¿Es necesario que, desde la adquisición de WhatsApp, la red social sea capaz de entrar en nuestra agenda, compararla con la de Facebook y comenzar a proponernos acciones? ¿Es Facebook una rueda de reconocimiento pública? Estas preguntas que, hoy en día subyacen en la cabeza de cualquier usuario, serán contestadas a lo largo del presente trabajo.

- Twitter: Es una aplicación y red social de *microblogging*[39]. Denominado por las industrias tecnológicas como el SMS de Internet, tiene su fecha de lanzamiento en marzo de 2006 y cuenta hoy en día con más de 500 millones de usuarios. Tiene como característica principal que sus mensajes no pueden superar los 140 caracteres, permitiendo compartir las fotos de otras aplicaciones, como Instagram o vídeos de YouTube. Cuenta además con la opción de geolocalizar cada uno de los mensajes (tuits) por parte del usuario [41].

  A continuación, en la Figura 2-14 se puede ver el logotipo de Twitter.

Figura 2-14 Logotipo de Twitter [42].

En cuanto a su privacidad, se ha especulado mucho sobre la posibilidad de que Twitter estuviera vertiendo sus mensajes entre usuarios a la NSA[40] [43]. También se desconoce qué hace la red social en cuanto al almacenaje de fotos y datos como pasaría con la anterior red social (Facebook).

Pese a no tener tantas configuraciones, como Facebook, también cuenta con la tecnología de borrado de metadatos [39]. Si bien la geolocalización y ciertos datos vertidos a la red son el punto débil de la aplicación, ya que con el empleo de ciertas herramientas (como Creepy) somos capaces de obtener la localización de los tuits, la ubicación física del usuario, así como el terminal en uso y horas más usuales de publicaciones del usuario, así como sus posibles amistades, todos ellos datos útiles para un ciberdelincuente.

La franja de edad de máximo empleo está entre los 18-29 años [36] (la mayoría son mujeres las que acceden a su uso). Destaca también que esta red social está más implementada entre las instituciones oficiales y que el nivel de estudios predominante entre sus usuarios son estudios superiores.

[39] Servicio que permite a sus usuarios enviar y publicar mensajes breves, generalmente solo de texto.

[40] (*National Security Agency* -Agencia de Seguridad Nacional): Es una agencia de inteligencia del Gobierno de los Estados Unidos que se encarga de todo lo relacionado con la seguridad de la información.

Se caracteriza también por ser una red donde la mitad de sus contenidos son de carácter informativo, aunque permite realizar conversaciones sobre temas propuestos por los usuarios(*hashtags*).

En cuanto a la seguridad para sus usuarios, Twitter usa desde 2010 la tecnología de identificación OAuth [44]. Consiste en delegar el proceso de identificación a otra aplicación. De esta forma, el usuario no tiene que recordar un número elevado de usuarios para sus distintas redes sociales, correos, etc. Sin embargo, este método de identificación supone un problema para el usuario, ya que tiene sus servicios dependientes de otros servicios. Es decir, si por algún motivo, estos fueran suplantados o eliminados, el resto también fallaría.

Esta red social ha sufrido ataques de robo masivo de cuentas, incluso la del propio creador de Facebook. A modo de anécdota, destaca el seguimiento de la ofensiva de ISIS[41] realizada por las Fuerzas Armadas Iraquíes tomando como base Twitter o el seguimiento de las operaciones de las Fuerzas Armadas Israelíes también tomando como base los tuits de los combatientes [45].

Consecuencia de lo anterior es por lo que dicha red social se encuentra vetada o su acceso será restringida en los mismos países vistos en el apartado anterior [34]. Por otra parte, Twitter ha estado relacionada en los escándalos de ciberespionaje relacionados con la NSA [43], viéndose también en entredicho su parcialidad tras los escándalos de WikiLeaks[42], donde se acusaba a la red social de ocultar o evitar que WikiLeaks se convirtiese en tema de actualidad entre los usuarios.

- Instagram: Es una red social y aplicación que permite compartir fotos y vídeos con el resto de usuarios. Permite retocar las fotos que se suben a la red, así como la interacción y compartición de fotos con el resto de redes sociales. Se basa en el formato de tamaño de fotos Polaroid, en cuanto a tamaño re refiere. El lanzamiento de la aplicación data de octubre del año 2010 y en la actualidad cuenta con más de 500 millones de usuarios, si bien se calcula que se conectan a esta e interactúan con esta, en torno a 300 millones de usuarios diarios [46] . Desde 2012 pertenece a Facebook.

  A continuación, en la Figura 2-15 se puede ver el logotipo de Instagram.

Figura 2-15 Logotipo de Instagram [47].

La banda de edad de más común empleo, se encuentra entre los 18 y los 29 años [36], siendo una red social más utilizada por mujeres que por hombres. En la actualidad, cobra especial importancia su uso entre corporaciones o empresas que quieren dar a conocer sus productos de forma visual. Dentro de las Fuerzas Armadas, su uso está más extendida a los usuarios más jóvenes, siendo en muchas ocasiones la plataforma de más empleo.

[41] *Islamic State of Iraq and Syria*-Estado Islámico de Irak y Siria.

[42] Es una organización mediática internacional sin ánimo de lucro, que publica a través de su sitio web informes anónimos y documentos filtrados con contenido sensible en materia de interés público, preservando el anonimato de sus fuentes.

Instagram en su desarrollo, ha ido añadiendo servicios que han sido duramente criticados por la similitud a redes sociales ya existentes [48]. Sin lugar a dudas han sido los términos de privacidad los que más inconvenientes y protestas han tenido por parte de los usuarios, ya que, en diciembre de 2012, Instagram publicaría los nuevos términos legales de privacidad, donde queda recogido que se otorga el derecho a vender las fotos de los usuarios a terceros sin notificación o compensación (a partir del 16 de enero de 2013 [49]). Esta medida sería recurrida por los usuarios, organizaciones, como "*National Geographic*", hasta el punto de llegar a dejar de usar sus cuentas o eliminarlas, y la consiguiente reacción de disculpas por parte de la dirección de la empresa, con la elaboración de unas nuevas condiciones de privacidad y uso.

Dentro de las medidas de privacidad y seguridad, la red social ha llevado acabo el borrado masivo de metadatos [39]. Esto significa que como hemos visto en apartados anteriores, una vez que se sube la foto queda registrado dentro de los servidores, Instagram borra cualquier información contenida en los metadatos de la foto. Esta medida también ha supuesto una controversia entre los usuarios de la red social, ya que aquellos usuarios, que suban una fotografía no podrán demostrar que es suya, o que ha sido realizada por ellos. Así Instagram ha aprovechado para explicar a sus usuarios que las medidas adoptadas no van en contra de la pertenencia o no de las fotos o videos subidos. Se debe simplemente a cuestiones de seguridad.

- LinkedIn: Es una red social enfocada a dar a conocer al resto de usuarios el currículum personal de un usuario. Realizado y modificado por cada usuario, permite además identificarse frente a instituciones o compañías. De esta misma forma las compañías se dan a conocer al resto de usuarios. Enfocada también a la búsqueda de mano de obra potencial por parte de las compañías, se permite el contacto entre usuario y posible contratante (se asimilaría a una bolsa de empleo cibernética). Como aspecto positivo la red social permite que otros usuarios indiquen si han trabajado con el usuario (potencial contratante) y recomendarle públicamente al resto de usuarios. Esta medida surge como solución al problema de los perfiles, ya que no existe ningún organismo de verificación sobre todo lo que ha puesto el usuario en el perfil. Esta red social abarca cualquier campo de empleo, sin distinción alguna.

  A continuación, en la Figura 2-16 se puede ver el logotipo de LinkedIn.

Figura 2-16 Logotipo de LinkedIn [50].

LinkedIn nace a finales del año 2002 [51] y cuenta con más de 450 millones de usuarios, de los que se calcula que solo un 25% [52] se encuentra activo y hace un uso habitual de la red. En España, el número de usuarios es de 8 millones de usuarios [53].

A lo largo de su desarrollo, la red social ha sufrido diversos ataques, siendo el más significativo el sufrido en el año 2012, en el que fueron robadas más de 6 millones de cuentas [54]. Dicho robo se relacionó con el fallo del algoritmo SHA-1[43](desarrollado por la NSA en la década de los 90) [55]. Más tarde, en el año 2016 se pusieron a la venta a

[43] Algoritmo de autenticación.

través de la Deep Web[44] 117 millones de cuentas de usuarios y sus contraseñas [56], dejando en evidencia la privacidad y seguridad que la compañía ofrecía a sus usuarios (al poder acceder a los perfiles se harían con información de carácter privado como correos y números de teléfono). Fueron numerosos los esfuerzos de la empresa por desmentir dichos rumores, adoptando como medida la sugerencia a los usuarios de cambios de contraseñas.

En 2016 Microsoft anuncia la compra de la red social LinkedIn.

LinkedIn, sin embargo, hace que todos los metadatos [39] de sus usuarios (como en ejemplos anteriores) sean eliminados de cualquier tipo de archivo que se quiera compartir. La red social se caracterizará por su carácter empresarial, siendo la franja de edad predominante en la red social de 30 a 49 años [36], enfocada a varones con estudios superiores.

- WhatsApp: Es una aplicación de mensajería instantánea, diseñada para enviar y recibir mensajes a través de Internet. Desde su creación ha conseguido que el uso de los SMS haya quedado prácticamente extinto. Además, dicha aplicación permite enviar texto, fotografías, vídeos y audios [57].

  A continuación, en la Figura 2-17 se puede ver el logotipo de WhatsApp.

Figura 2-17 Logotipo de WhatsApp [58].

Fue creada en 2009 [59] por Jan Koum, de origen ucraniano, que se trasladaría más tarde a Estados Unidos, donde hoy reside. WhatsApp cuenta en la actualidad con cerca de 1000 millones de usuarios, encontrándose por delante de otras aplicaciones similares como Telegram, que únicamente cuenta con 100 millones de usuarios. Su denominación como red social ha quedado en entredicho, si bien se la reconoce como red social debido al uso de grupos y estados añadidos recientemente.

Para comunicarnos con ella es necesario que el contacto se encuentre dentro de nuestra lista de contactos o al menos tengamos su número de teléfono.

En la actualidad, ofrece servicios de VoIP[45], permitiendo llamadas de audio y de vídeo. Fue adquirida en 2014 por Facebook, lo que supone que ambas aplicaciones se encuentran enlazadas. Esto explica que las listas de contactos apareciesen en posibles sugerencias de amistad (entre otras utilidades de su integración).

Sin embargo, WhatsApp en su evolución ha presentado múltiples problemas de seguridad. En 2011, debido a un fallo, las cuentas de los usuarios, quedaron expuestas para poder ser robadas. Además, WhatsApp en sus inicios no contaba con cifrado en las comunicaciones, lo que propició el nacimiento de Telegram [60], ya que, sin cifrado [61], cualquier ciberdelincuente podría acceder a las comunicaciones entre dos usuarios. Estos hechos propiciaron que la Oficina Alemana de Regulación de la Privacidad aconsejara a sus usuarios su no utilización debido a que dicha aplicación no se encontraba regulada por ninguna legislación europea, en lo que a seguridad y privacidad se refiere. En abril de 2016

[44] También conocida como Web Oscura, es la parte de la red que carece de regulación jurídica, y cuenta como máxima fundamental con el anonimato de sus integrantes.

[45] Voz sobre IP, es decir llamadas a través de Internet.

WhatsApp anunció el cifrado de las conversaciones, asegurando que ni desde la propia empresa serían capaces de leerlas (hecho que aprovechó "*Anonymus*"[46] para desmentirlo y señalar la posible existencia de una puerta trasera en la aplicación [61]).

En cuanto a la privacidad, debido a que las fotos que envía son previamente comprimidas, todas ellas carecen de metadatos, y, en ese sentido, respeta la privacidad. Sin embargo, muchos usuarios han elevado sus quejas a los desarrolladores de la aplicación, debido a que consideran que la privacidad se encuentra en entredicho cuando en un mismo grupo aparecen identificados todos los números, o cuando la aplicación informa de la ultima hora de conexión de sus usuarios. Estos hechos están siendo estudiados, como es el caso de los números, o han sido solucionados como la información de recibido o ultima conexión. Otro hecho que puede afectar a la privacidad, es la mejora que va a plantear WhatsApp para su próxima versión, al poder sus contactos estar geolocalizados tras enviar un mensaje de grupo [62].

En la actualidad, se le reconoce como uno de los métodos más rápidos de intercambio de información, tanto como para el envío de texto como para el envío de material gráfico. Dentro de las FAS, es uno de los métodos de comunicación empleados de manera personal en zona de operaciones, ya que el volumen de datos utilizados por dicha aplicación para enviar mensajes es de menor tamaño que el utilizado por otras aplicaciones o redes sociales.

A modo de ejemplo destaca que fue WhatsApp el medio de comunicación y coordinación empleado en el reciente fallido golpe de estado en Turquía por los elementos sublevados [63].

2.4.3 Organizaciones terroristas en redes sociales

Es importante señalar, debido a su completa actualidad, que la red no solamente se ha convertido en base sobre la que lanzar diferentes tipos de ciberataques, sino que además es el campo de actuación, en cuanto a propaganda y comunicaciones se refiere, de todas las organizaciones terroristas, tanto de carácter nacional como internacional. Es a través de ella donde se da a conocer su propaganda o se lanzan consignas para ese tipo de guerra asimétrica.

Ha sido precisamente la falta de control de la misma, la que las ha convertido en plataformas de uso delictivo.

En la actualidad, las organizaciones terroristas basan su actividad en la red en redes sociales y páginas web. Los beneficios que pueden obtener son difusión y propaganda del terror, reclutamiento y activismo, entrenamiento y concienciación, coordinación y planificación, conexión interna y por último conexión con otros grupos terroristas [2].

- Operación "Gallant Phoenix": Operación militar llevada a cabo en Jordania y países próximos. Está liderada por la Agencia de Inteligencia de la Defensa (DIA) estadounidense y junto a los efectivos de este país hay que sumarle los de muchos otros, entre ellos España.

  El objetivo de la misión es monitorizar la red, intentando recoger de la misma la máxima información relacionada con el ISIS o sus componentes.

  Una vez localizada la misma, se pasa a su explotación. Esto trae consigo la anulación de toda aquella relacionada con el ISIS como organización, o el aprovechamiento de la

[46] Conjunto de personas con conexión a internet, cuyo común ideal, por encima de cualquier otro, es la defensa de la libertad de expresión.

relacionada con sus miembros. Llegado este punto, se debe aclarar que "aprovechar una información asociada a un componente" es valorar si la misma es eficiente y concluyente para lanzar una operación de "destrucción" sobre el mismo.

Es importante señalar el juego tan importante que tienen en este proceso todos los sistemas de análisis de redes [45].

- Terrorismo Yihadista en la red: El año 2015, marca un antes y un después de la amenaza terrorista, la cual comienza a expandirse a través de la red. Los primeros en sumarse en una lucha pública contra el ISIS sería la corriente "*hacktivista*[47]" *Anonymous* con sus dos principales operaciones #OpCharlieHebdo y #OpISIS, guerra que comenzarían a librar a partir de la fecha de dichos acontecimientos [64].

  Es entonces, cuando las principales organizaciones de ciberdefensa mundial, ven una oportunidad clara para sumarse a la contienda; pero esperaban un enemigo menos potente, ya que el ISIS, contaría desde su origen con un ejército de *hackers*.

  Tras la declaración de guerra, "*Anonymous"*, saca a la luz cerca de 10.000 [65] cuentas de Twitter, Facebook y correos electrónicos de miembros y simpatizantes del ISIS. Esto causa malestar entre las principales agencias que también luchaban contra el ISIS, ya que con esta acción quedan al descubierto perfiles de personal de inteligencia que trataba de obtener información.

  Entre los principales ataques desarrollados por los *hackers* del ISIS (quienes estudiaron mayoritariamente en universidades europeas) destacan los sufridos por el Mando Central de Estados Unidos, que vio como sus cuentas de Twitter y YouTube eran "*hackeadas*", y donde se pudieron ver frases como la siguiente:

  "Soldados estadounidenses, vamos por ustedes, vigilen sus espaldas... Sabemos todo sobre ustedes, sobre sus esposas, sus hijos".

  En la Figura 2-18 se puede ver uno de los múltiples ataques sufridos por el CENTCOM[48] estadounidense por parte de los *hackers* del ISIS.

Figura 2-18 Captura de pantalla del "hackeo" del CENTCOM [66].

Además de acceder a archivos de personal del Departamento de Defensa de los Estados Unidos, también se filtraron listas de direcciones de Altos Mandos del ejército estadounidense.

[47] Individuo que lleva a cabo acciones de activismo a través de la red.
[48] *Central Command* – Mando central de los Estados Unidos

Durante el desarrollo de la contienda, los *hackers* del ISIS desarrollaron sus propias aplicaciones de mensajería, como Farachar. También desarrollaron videojuegos cuya temática consistía en degollar, asesinar y hacer explotar a individuos occidentales.

También impulsan su proceso de captación, diseñando portales destinados a uniones matrimoniales para "*sus guerreros".* El objetivo era atraer mujeres, "futuras esposas", a los lugares de la contienda.

Las principales potencias europeas reaccionan con la creación de unidades destinadas a frenar dichos fines. Ejemplos hay muchos: la unidad cibernética alemana, de reciente creación, o el Batallón 77 [65], perteneciente a la Armada británica con un total de 1500 efectivos. Israel cuenta a su vez con la denominada Unidad 8200 [18], cuyos integrantes se cuentan por varios miles de miembros y cuyos cometidos son hacer la guerra cibernética. España cuenta con el Mando Conjunto de Ciber Defensa con un total de unos 120 efectivos [18], número muy inferior a los anteriormente citados. Destaca como curiosidad que en cualquier estructura de inteligencia la ciberdefensa forma parte de la misma. Sin embargo, en España es diferente, hecho que ha propiciado un escaso desarrollo y una diversificación en la formación con el consabido aumento del gasto.

2.4.4 Infoxicación, privacidad y seguridad

Se define la *infoxicación* como una sobrecarga de información difícil de procesar [67]. En ese sentido, los medios de comunicación se han desarrollado hasta el extremo de producir una sobrecarga de información en la red. Las redes sociales también ayudan a que se propicie dicho fenómeno, y son los propios usuarios quienes de alguna forma lo facilitan. En la actualidad, se da el caso de un exceso en el volumen de información existente en redes sociales. Cuando los usuarios dan demasiada información sobre ellos, el hecho pasa a ser motivo preocupante respecto a la privacidad y la seguridad, incapaz de asimilar y gestionar semejante cantidad de información.

Se entiende por privacidad el nivel de protección de la información de un usuario y la capacidad con que se puede obtener dicha información [68]. Puesto que en la mayoría de los casos es el usuario el que puede regular dicho flujo de datos conviene generar cierta concienciación entre ellos. En esta memoria se recalca la necesidad de que el militar español llegue a concienciarse de que su grado de privacidad debe ser, al menos, el existente en otras FAS de países aliados. Esa capacidad la tienen exclusivamente ellos, como usuarios.

Es destacable situaciones vividas durante operaciones en el extranjero por parte de tropas españolas, en el que el enemigo realiza "*falsos secuestros de militares españoles"* [69]. Dichos secuestros parten de la obtención de información a través de redes sociales sobre los supuestos secuestrados. Con estos datos, el supuesto secuestrador contacta con las familias por teléfono diciendo que su familiar estaba secuestrado, que guarden silencio y depositen una cierta cantidad de dinero en una cuenta. Este y otros ejemplos son debidos a imprudencias de privacidad en los perfiles de las redes sociales y demás perfiles en la red.

El concepto de seguridad está relacionado con las herramientas disponibles para hacer un uso corriente de la red, sin caer en *malware* o elementos de "*phising"*[49]. Según recientes estudios del IEEE[50] la seguridad de un usuario en la red depende casi en su totalidad de él mismo, ya que procesos como la elección de contraseña, las URL maliciosas, softwares no oficiales y otros elementos de interacción en la red son elegidos por él mismo [70].

[49] Hacerse pasar por una persona o empresa conocida, con el fin de introducir un malware en la plataforma objetivo.
[50] Instituto Español de Estudios Estratégicos.

A día de hoy, en lugar de vivir en el siglo de las comunicaciones, estamos viviendo en el siglo de las "sobre-comunicaciones". Es la sociedad la que camina en el sentido de la interconexión y es ella misma, la que podría producir un colapso en sí misma. Así, en el momento en el que un individuo se vuelve vulnerable, la sociedad se vuelve vulnerable. Esta afirmación es extensible a las FAS. Si sus componentes son vulnerables, las FAS como organización pasará a serlo.

2.5 Personal de las FAS como víctimas de ciberataques

La OTAN estudia las amenazas bajo la perspectiva del concepto de TESSCO. Este concepto comprende las valoraciones de las amenazas que tienen su origen en el terrorismo, espionaje, sabotaje, subversión y crimen organizado. En la actualidad se contempla una quinta, aquellas que tienen su origen en las redes sociales y las relaciona con las anteriormente citadas.

En la auditoria de perfiles de redes sociales de este trabajo, nos ajustamos a estos estándares para comprobar hasta qué punto la información que hay en la red sobre un integrante de las FAS supone, o no, un riesgo para las FAS y su imagen.

Un sujeto se puede constituir como objetivo, en el ciberespacio, por dos motivos [18]:

- Porque es el objetivo en sí.
- Porque es parte de un objetivo general, en este caso las FAS.

Como consecuencia de toda la información vertida en la red cualquier atacante potencial podría obtener información para emplearla dentro de las amenazas contempladas en el concepto TESSCO. En algunos casos, la primera "víctima" puede ser el individuo, pero no hay que perder de vista, que mucha de la información depositada en la red atenta contra la institución, contra los componentes de la misma y contra su propia imagen [69].

3 DESARROLLO DEL TFG

3.1 Obtención de la información

3.1.1 Engaño en la conexión

Durante el desarrollo de este apartado, se ha observado que la red de la Escuela Naval Militar se encuentra bien protegida con su propio servidor DNS, cosa que no ocurre en las instalaciones Wi-Fi de las viviendas. Destacamos que la red de Defensa[51] cuenta también con su propio servidor DNS, lo que hace casi imposible dentro de la red realizar un ataque *"DNS spoofing"*.

Dentro de la red de la Escuela Naval Militar, como se ha señalado, la posibilidad de hacer "DNS *spoofing*" es prácticamente imposible, aunque, si se atacase al servidor DNS sería posible realizarlo. En cualquier caso, se encuentra más allá de los cometidos de este trabajo.

La solución llevada a cabo para hacer un *"DNS Spoofing"* ha consistido en la creación de un punto de acceso Wi-Fi falso con el mismo nombre que la red de la Escuela Naval Militar, aprovechando los cortes de luz sufridos durante la realización del trabajo. Con este sistema, es posible hacer "*DNS Spoofing*", ya que las peticiones DNS del usuario se pueden redirigir en cuanto se conecta al punto de acceso falso.

A continuación, en la Figura 3-1 y Figura 3-2 se puede ver la variación en la tabla de conexiones.

Figura 3-1 Tabla de conexiones antes.

[51] Es la red utilizada por los integrantes de las FAS, asequible a través de ordenadores corporativos que puedan acceder a dicha VPN.

Figura 3-2 Tabla de conexiones después.

Después de hacer esto, basta con esperar a que alguna víctima caiga dentro de la trampa. Se puede observar que el nombre de la red no es exactamente el mismo debido a que si la red trampa tiene el mismo nombre que el Wi-Fi de la escuela se pisarán las redes, haciendo que la trampa desaparezca. Durante el desarrollo, se observa que esa diferencia no llama la atención a los usuarios que se conectan, teniendo en cuenta que es un único punto de acceso que emite y su señal no es captada más allá del arco de emisión de este.

Si bien, como se vio anteriormente, la herramienta SET (*Social Engieneering Toolkit*), es capaz de crear dentro de una red un punto de acceso falso, esto no fue necesario, debido a que se aprovechó la caída de la red eléctrica en la que los encaminadores se desconfiguraban para poder crear un punto de acceso falso. Aunque se señala que existe más de una opción para este proceso, otra de las opciones es la utilización de *Pineapple*.

Como se demuestra a continuación en la Figura 3-3, dicho ataque de ingeniería social tuvo éxito haciendo que en las proximidades del punto de acceso, se conectasen hasta 5 usuarios.

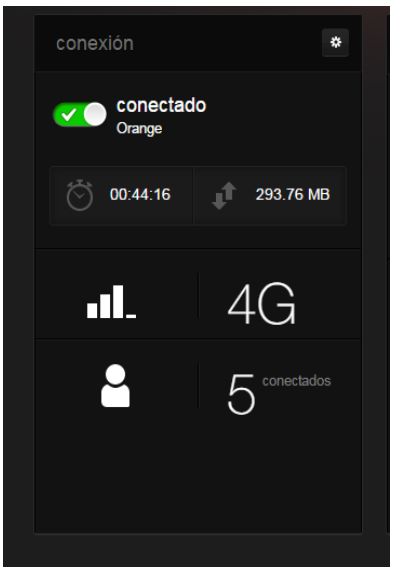


Figura 3-3 Usuarios conectados a falsa red.

Es sobre alguno de estos cinco usuarios sobre los cuales se lleva a cabo el *"DNS Spoofing"*, con la intención de obtener credenciales o información valiosa.

3.1.2 Realización del "DNS Spoofing"

Por motivos de seguridad y éticos, realizamos el ataque sobre un sistema propio, demostrando que es fácilmente realizable, llegando a poder obtener diversas cuentas y usuarios.

Para el proceso de clonación de la página utilizaremos la herramienta SET (*Social Engineering Toolkit*).

Durante el proceso de prueba se ha utilizado una página con protocolo HTTPS, demostrando que sobre estas también vamos a poder ser capaces de hacerlo y recordando siempre que estamos haciendo la prueba en la red falsa.

A continuación, en la Figura 3-4 se puede ver los pasos seguidos para la realización del ataque *"DNS spoofing"*.

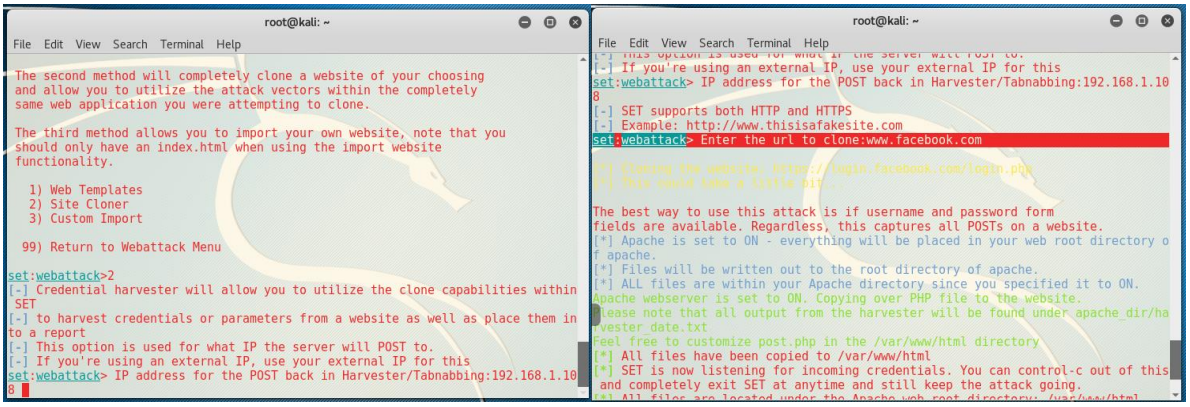


Figura 3-4 Realización de un ataque *"DNS Spoofing"*.

Como ejemplo, si el usuario realiza un acceso a la página Facebook, la herramienta redirecciona la conexión a una página clonada (Figura 3-5) creada para este propósito donde se capturará el nombre de usuario y su clave.

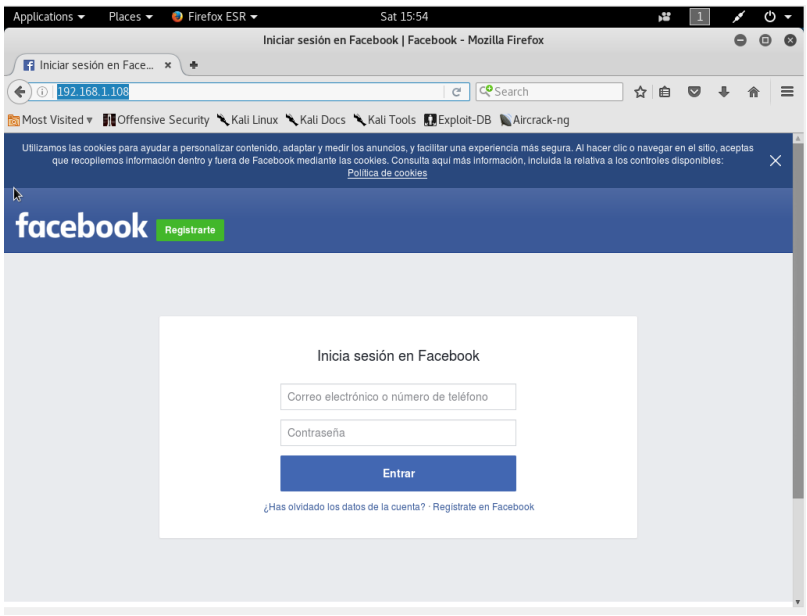


Figura 3-5 Página de Facebook clonada.

Si el usuario no es experto no se dará cuenta de que la dirección de la URL no coincide con la que se ha introducido.

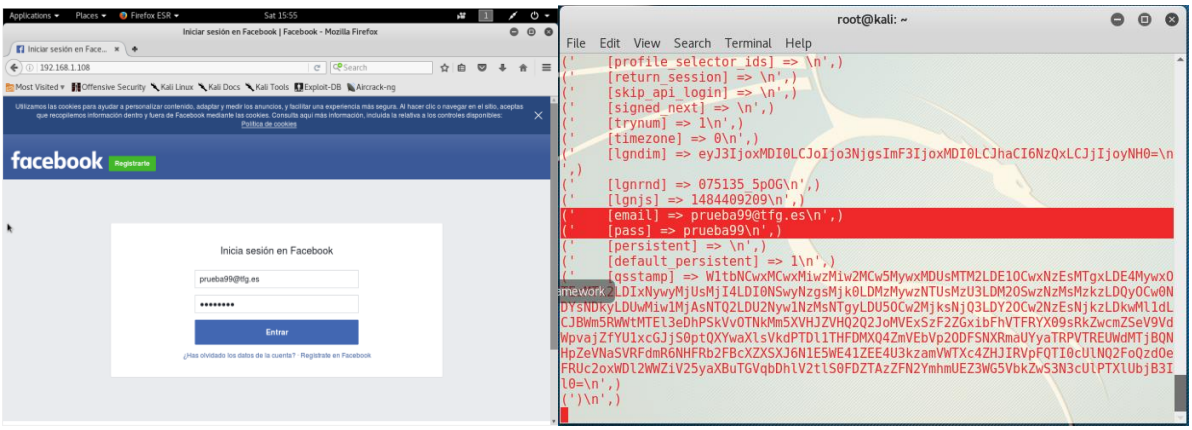


Figura 3-6 Usuarios y contraseñas obtenidos.

Tras introducir los datos (Figura 3-6), el usuario estaría entregando los datos de usuario y contraseña. De esta forma, tras hacerlo por primera vez, obtendría un error en pantalla y sería redireccionado a la página real, quedando en un hecho aislado como se puede ver a continuación en la Figura 3-7.

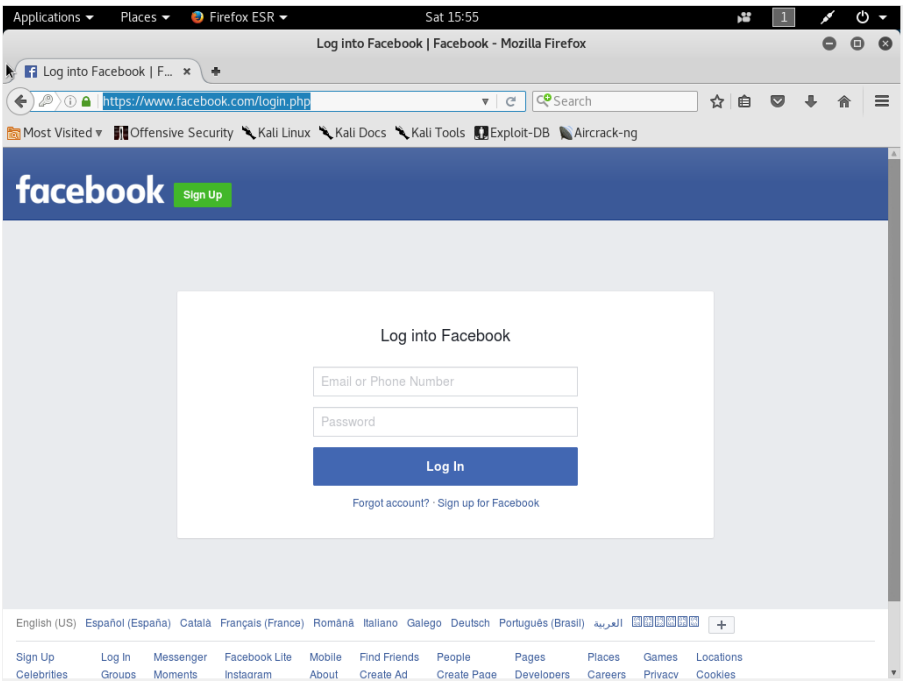


Figura 3-7 Redirección a página real.

Para solucionar el problema de la detección de la URL falsa, podríamos efectuar junto a este ataque el proceso de desviar direcciones IP con "ettercap"[52]. Sin embargo, no sería válido para páginas con HTTPS, pero sí valido para páginas sin cifrado, como la página de Faitic (el servicio de teledocencia de la Universidad de Vigo).

[52] Herramienta que sirve como interceptor/sniffer/registrador para LANs. Soporta direcciones activas y pasivas de varios protocolos.

El proceso de configuración de "ettercap" se puede ver a continuación en la Figura 3-8.

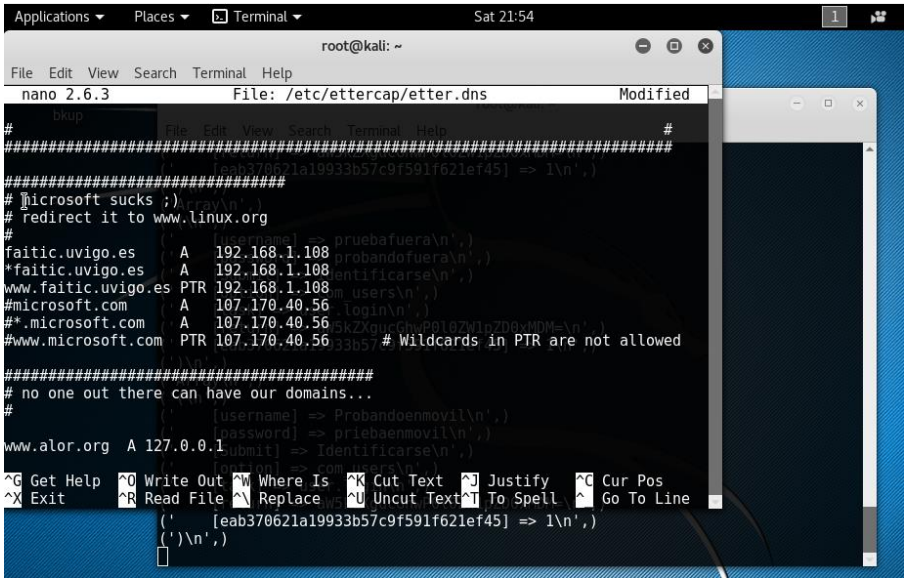


Figura 3-8 Configuración de "ettercap".

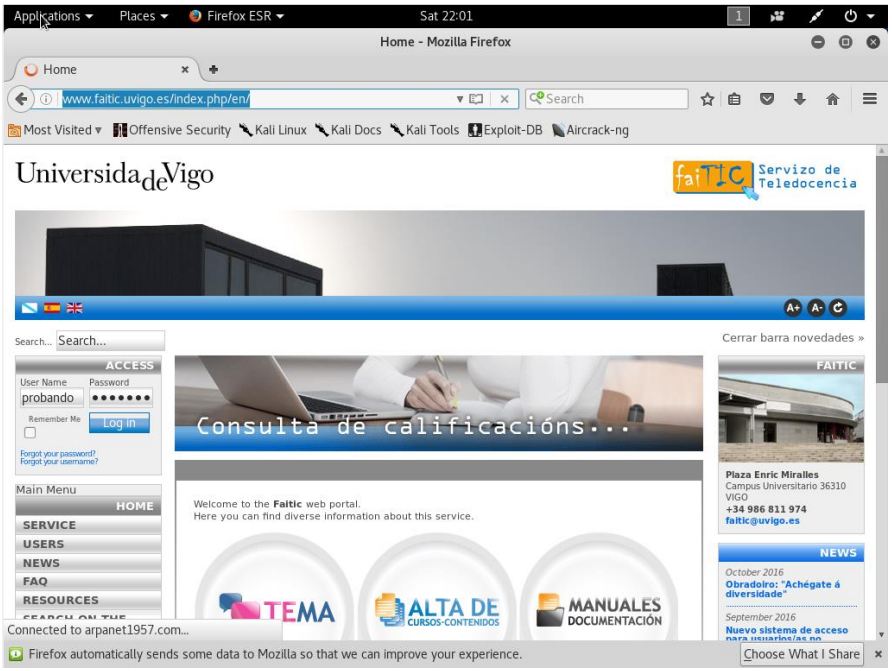


Figura 3-9 Acceso de prueba a la página de Faitic [71].

Cada vez que un usuario acceda a Faitic, "ettercap" capturará el tráfico intercambiado y como resultado será posible obtener nombres de usuario y contraseñas. El proceso de captura se puede ver en la Figura 3-10.

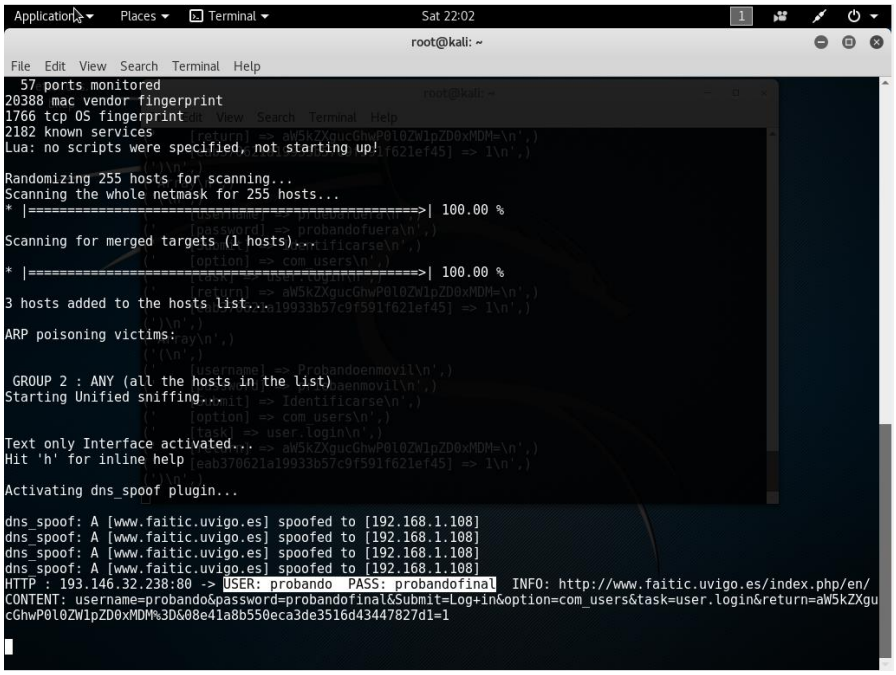


Figura 3-10 Resultado sobre Faitic.

Otra buena solución para que no aparezca la dirección IP en la URL es el empleo de acortadores de URL como "tinyurl" pero todavía muy lejos de la URL original a utilizar(Figura 3-11). Sin embargo, cuando el usuario la introduzca y entre en la página, se observará que de nuevo en la URL aparece la dirección IP. Así la utilidad de dicho método está en enviar el enlace por correo para que alguien lo pulse y sea redireccionado a él. Este método puede utilizarse tanto con HTTP como con HTTPS.

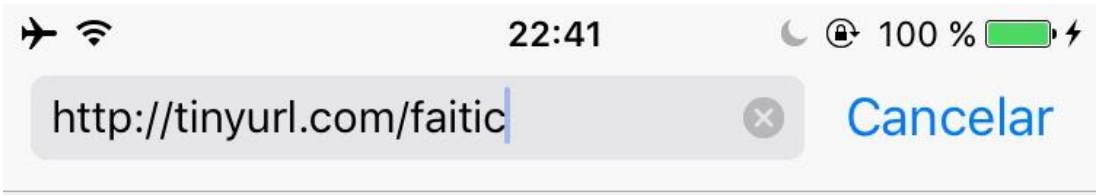


Figura 3-11 Probando con "tinyurl".

3.1.3 ¿Por qué no hacer "DNS Spoofing" en la red de Defensa?

La red interna de Defensa se asemeja mucho a la conexión de la Escuela Naval Militar. Sin embargo, Defensa utiliza servidores DNS propios antes de realizar la petición a servidores DNS externos. Es decir, antes de buscar la IP en un servidor externo se consulta en uno interno para ver si este nombre ya existe en la memoria caché.

La arquitectura de la red de Defensa y de los equipos dispone de una serie de políticas y medidas para que este tipo de ataque no se pueda realizar:

- El usuario no es administrador del equipo ni del servidor, con lo cual no puede cambiar las IP que apuntan al DNS interno en el equipo, ni tampoco puede cambiar la resolución de nombres de dominio.
- Si el usuario administrador de equipo hubiese sido comprometido se podría cambiar la dirección del DNS interno, pero tendría que haber un servidor de DNS alternativo para realizar el ataque. Esto último resulta complejo pues habría que introducirlo en el dominio, y para ello no basta con conectarlo a la red.

Tras analizarlo, el funcionamiento de un servidor de nombres DNS en Defensa será de la siguiente forma:

- Si un usuario en una UCO (Unidad Centro u Organismo) "A" realiza una petición, esta va a su servidor local de nombres DNS. En el caso en el que dicha petición no se pueda responder, se reenvía a un nivel superior pudiéndose realizar saltos hasta llegar a servidor principal de nombres DNS como se ve en la Figura 3-19. Sin embargo, puede suceder que otro usuario de una UCO "B" no necesite hacer tantos saltos como el del anterior UCO. Esto es debido a que las peticiones DNS de la segunda UCO sea resuelven en cualquiera de los servidores existentes.
- De esta forma se comprende que la única forma de hacer un "*DNS Spoofing"*, es siendo administrador del equipo o servidor o introduciendo algún tipo de *malware* el cual que pueda escalar privilegios hasta llegar a administrador.

Ante todo lo expuesto anteriormente, por seguridad, para que un equipo pueda pedir a un servidor DNS una resolución IP de una página debe pasar al menos dos filtros de seguridad:

- Que el equipo debe estar en el dominio de Defensa. Para ello, el usuario necesita usuario y contraseña para entrar.
- Que la petición a Internet de la página debe pasar por un *proxy*, por lo que debe tener usuario y contraseña para poder navegar.

3.2 "El sujeto"

3.2.1 Adquisición de información del sujeto

Si se obtiene el nombre y usuario de un correo es posible realizar ataques para obtener información confidencial. En este sentido, es importante resaltar los peligros de conectarse a un Wi-Fi abierto y hasta qué punto puede el atacante infringir daño en el atacado.

Para este desarrollo del trabajo se simularán las acciones, ya que se ha demostrado la capacidad de robo de información a través de los distintos métodos citados.

De esta forma supongamos que el atacante ha podido acceder al correo electrónico del atacado.

Lo primero que hace el atacante es buscar información que le permita obtener más información, como correos de redes sociales, correos bancarios o facturas electrónicas.

Tras un análisis, el atacante ha dado con un correo como el de la Figura 3-12.

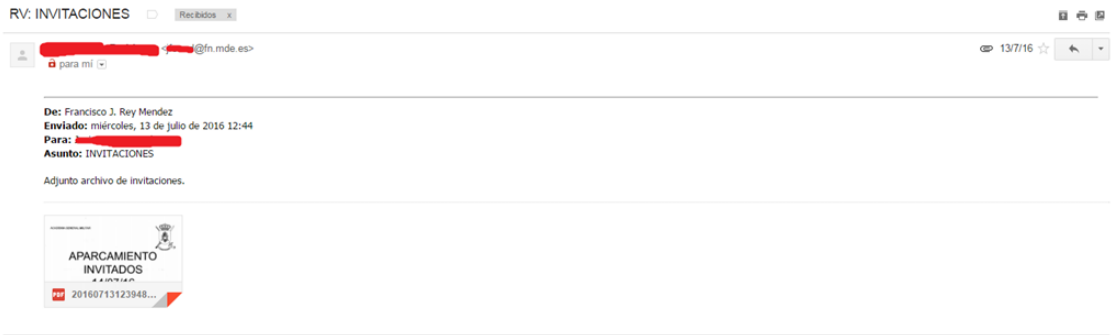


Figura 3-12 Correo interceptado a una víctima.

Un correo con dominio militar enviado a un correo civil y de especial importancia, ya que en otro de los mensajes se le relaciona como Oficial de la Armada Española (más adelante se demuestra). Esto

lleva al atacante a realizar una exploración de dicho correo. Para lo cual, al ser un correo de Gmail, ayudado de la pestaña que permite mostrar más información del correo se muestra el texto original (Figura 3-13).

Entre los datos de interés, se observa una IP que no necesariamente es la del ordenador desde el que se envió el correo. En este caso, la IP hace referencia al servidor de correo del Ministerio de Defensa.

Otra de las opciones como atacante es analizar los metadatos que ese documento aporta. Tras analizarlo con FOCA, la única información relevante es la fecha y el usuario que creó el documento. Destaca que, en la actualidad, los únicos archivos de los que es posible obtener información relevante de metadatos son aquellos archivos de los que no se ha modificado su estructura (subiéndolo a las redes sociales o haciendo compresión sobre ellos).

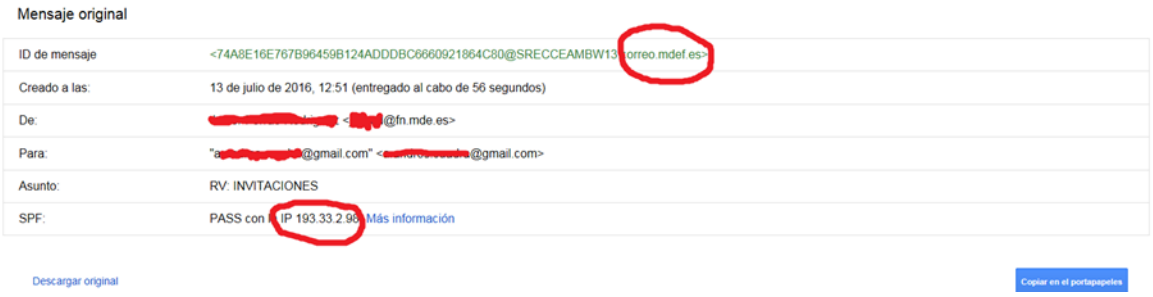


Figura 3-13 Texto original del correo.

3.2.2 Información del sujeto utilizando herramientas de OSINT

Dentro del mensaje del apartado anterior se observa que el dominio corresponde al Ministerio de Defensa y también la dirección IP desde la que se relaciona el correo. Con los datos obtenidos, IP, nombre y dominio, procedemos a hacer uso de las herramientas de fuentes abiertas. Así, cuantos más datos iniciales se tenga de la víctima mejores resultados arrojará la búsqueda.

La aplicación Foca no encuentra información relevante en el mismo. Se utiliza Maltego sobre los datos y arroja la siguiente información de la Figura 3-14.

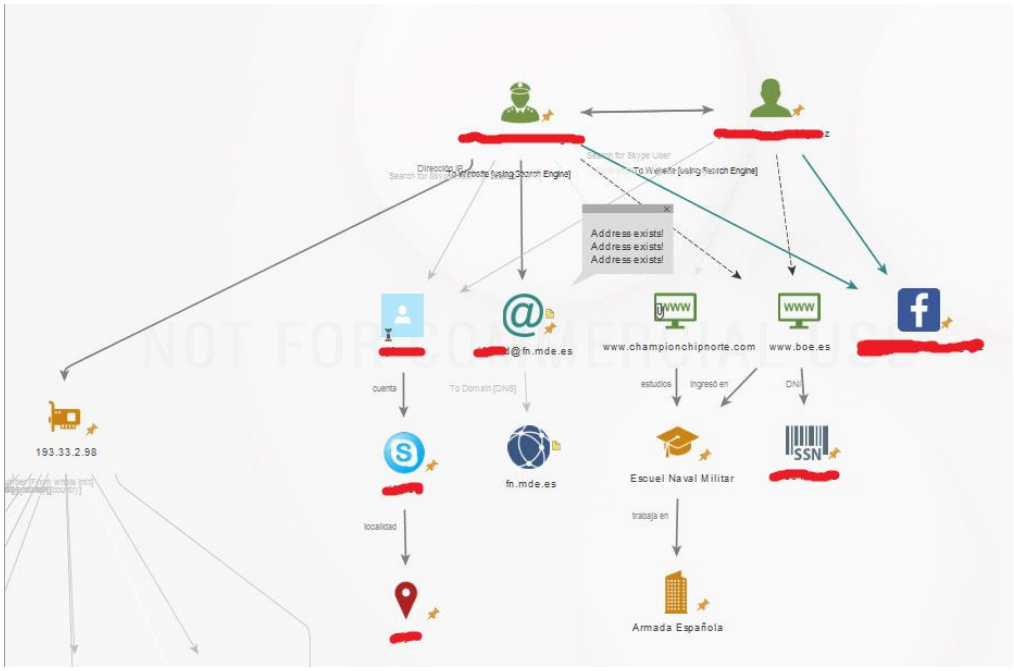


Figura 3-14 Exploración entorno al sujeto.

Mediante el análisis de los resultados, se puede observar que:

- En el primer nivel, se ha colocado al sujeto como Oficial de las Fuerzas Armadas, siendo esto una hipótesis basada en correos que como atacante se han interceptado. No es del todo erróneo comenzar una búsqueda por la realización de una hipótesis, aunque se tiene que desarrollar y demostrar.
- Para facilitar las búsquedas, se añade la dirección IP, que es información adquirida a través del correo.
- Al desarrollar las transformaciones sobre ambos (militar-persona y dirección IP), la información arrojada es reseñable. La herramienta indica que este usuario tiene cuenta de SKYPE (indicando su nombre de usuario) y cuenta en la red social Facebook, que posteriormente desarrollamos para ver hasta qué punto la estructura de seguridad que el propio usuario le da a su red social es vulnerable.
- En el segundo nivel, también se puede ver que se le relaciona con la Escuela Naval Militar, despejando la duda de si es un Oficial de las Fuerzas Armadas. Además, se puede apreciar el número de ingreso en la Armada Española. Cabe destacar que, al salir en el Boletín Oficial del Estado y estar colgado en la red, dicha información es de dominio público y puede utilizar cualquier usuario de la red.
- En el tercer nivel podemos observar los datos más relevantes. Entre los cuales, destacar el número de DNI con letra (objeto que puede ser fácilmente utilizado para la realización de un ataque de ingeniería social). Aun así, debido a la informatización de la información, a día de hoy es posible saber introduciendo el DNI si el usuario atacado tiene multas de coche como se puede ver en la Figura 3-15.

Figura 3-15 Localizador de multas del sujeto.

Con la información obtenida y utilizando las distintas fuentes abiertas, como Google, podemos basarnos en una multa para efectuar un ataque de ingeniería social para obtener el número de cuenta de la víctima, así como una compensación económica u otros fines.

Antes de hacer cualquier acción que pueda destapar los fines perseguidos, es necesario elaborar un correo cuya apariencia tenga credibilidad suficiente para que la víctima caiga en la estafa.

Citamos para este caso la noticia “La estafa (africana) a Luis con la falsa herencia de un tío muerto en China” en la que el atacante se aprovecha de la información obtenida del objetivo para, ayudado de los principios de ingeniería social, se lleve a cabo el ataque. La Figura 3-16 muestra una prueba de cómo podría hacerse un ataque de ingeniería social.


ITO:
n de datos al titular para
tación del conductor.
INFORMACIÓN
E ABONAR LA MULTA:
NTERNET: en la página
r.dgt.es, apartado
imites y Multas:
ATURA VIRTUAL".
as oficinas de Correos,
ntando esta notificación.
cualquier oficina del
nco Santander,
ntando esta notificación.
ICACIONES A TRAVÉS
INTERNET Y MÓVIL
recibir las notificaciones
iones y avisos a través
rnet y opcionalmente con
e a móvil suscribiéndose
rección Electrónica Vial
lgt.es).
consultar edictos de
es en el Tablón Edictal
inciones de Tráfico
RA).
MINISTERIO DEL INTERIOR
Centro de Tratamiento de
Denuncias Automatizadas
Apartado de Correos 505
24080-LEON
1.FECHA
HORA
NÚMERO EXPEDIENTE
13/1/2017
17:51
2. PRECEPTO INFRINGIDO
Artículo
48
REGLAMENTO GENERAL DE CIRCULACION
Importe total multa
100.00 EUROS
3. LUGAR DENUNCIA
Vía PO-11 DIRECCIÓN PONTEVEDRA
Importe abonado
0.00 EUROS
4. HECHO QUE SE NOTIFICA
CIRCULAR A 102 KM/H, ESTANDO LIMITADA LA VELOCIDAD A 80 KM/H. EXISTE UNA VELOCIDAD GENÉRICA EN VIA INTERURBANA. VELOCIDAD MEDIDA POR CINEMÓMETRO MULTANOVA 6FMR, ANTENA 1572, CUYO PROPÓSITO FUE APROBADO POR RESOLUCIÓN DEL 20/05/2004 DE LA DIRECCIÓN GENERAL DE INDUSTRIA, ENERGÍA Y MINAS (B.O.E. NÚM. 159 DE 02/07/2004) "PRIMERA PRÓRROGA". PARA LA GRADUACIÓN DE LA SANCIÓN SE HA TENIDO EN CUENTA LOS MÁRGENES DE ERROR ADMITIDOS REGLAMENTARIAMENTE.
5. DATOS VEHÍCULO
Matrícula...:
Clase.....:
Marca.....:
Modelo.....:
6. DATOS DEL INTERESADO
PONTEVEDRA
r, fecha y hora arriba señalados ha sido detectada la circulación de un vehículo de su titularidad a una velocidad superior a la legalmente establecida. Est
one una infracción grave a lo dispuesto en la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial (art. 65.4.a). Esta infracción no llev

Figura 3-16 Ejemplo de multa falsa al sujeto.

En esta prueba, los campos de fecha, hora, número de expediente, lugar de la denuncia, hecho a notificar, así como los datos del interesado han sido realizados por el atacante. Este ejemplo se ha llevado a cabo debido a la gran cantidad de individuos que muestran sus denuncias en la red, las cuales han servido como base para la realización de la misma. El proceso de conseguir los datos del coche puede ser:

- Realizando otro ataque de ingeniería social en el que nos haríamos pasar por alguna entidad adjunta a la DGT que pide datos del usuario, como el asegurador del seguro del coche de la víctima. si se le notificase algún problema con el coche del usuario, este mismo tendería a solucionarlo (basándonos en los principios de ingeniería social).
- Otra manera, que sería la más sencilla de realizar, trataría de pedir un informe a la DGT en el que únicamente se tiene que abonar unas tasas para poder acceder a dicha información.
- Por último, otra forma, la cual se realizaría físicamente, implicaría conocer la identidad del atacado, y, sobre este, realizar un *trashing*[53] o bien realizar una vigilancia donde se sepa que el atacado trabaja.

Como se puede ver, las alternativas son múltiples y todas y cada una de ellas válida.

Además de ser utilizado como ataque de ingeniería social se puede aumentar el nivel en lo que a complejidad se refiere. Esto va a consistir en que, en lugar de enviar el documento y esperar una respuesta del atacado (la cual puede que nunca se llegue a producir), podemos hacer que una vez que el atacado abra el documento se ejecute un archivo autoejecutable (*malware*). Con ello se crearía una puerta trasera (*backdoor*) en el sistema. Este ejemplo se ha sido probado y se muestra más adelante.

Una de las ventajas que este sistema conlleva es que no establece una comunicación bidireccional. Esto se debe a que hay que esperar la respuesta del atacado para obtener sus datos. Con el segundo método se puede acceder a la máquina de la víctima y obtener toda la información que tenga en su sistema.

Se trata de una práctica ilegal, y, en función del tipo *exploit* y *payload* puede ser detectable por algún antivirus.

[53] Obtención sin autorización de información privada a partir de la recuperación de archivos, documentos, directorios e, incluso, contraseñas que el usuario ha enviado a la papelera de reciclaje de su equipo.

Una manera de realizarlo es mediante la utilización de la herramienta SET. Esta herramienta permite la realización de ataques, y, en el caso de que queramos efectuar un proceso más elaborado, es posible utilizar distintos *encoders*[54].

Durante este proceso podemos ayudarnos de páginas que indican si los *malwares* son detectables. Debemos tener en cuenta al realizarlo que, si se sube un archivo a una página, como https://www.virustotal.com lo analiza, pero, al analizarlo, vierte a la red las cabeceras identificadoras de los virus. Así si el atacado actualiza la base de datos de virus, se detecta el malware, haciendo que salten las alarmas de los antivirus.

Otra solución más efectiva pero que escapa a las competencias de este trabajo es la utilización de software tipo RAT (*Remote Access Trojan*) como TheFatRat, que corre sobre cualquier distribución de Linux. Este software permite la creación de un RAT, cuya principal utilidad radica en la utilización de un servidor, donde se vierte la distinta información obtenida. Este método es más seguro y menos detectable que las soluciones ofrecidas por SET, ya que los *payloads* de esta herramienta se encuentran identificados en la mayoría de las bibliotecas de los principales antivirus conocido.

Si se desea hacer el experimento sobre Windows existen distintos softwares cuya funcionalidad es similar. Al tratarse de software que corre sobre Windows las limitaciones del usuario serán mayores que las de Linux. En cualquier caso, por ahora, nos centramos en la información que podemos obtener del usuario atacado.

A partir de la dirección IP, la información adquirida es abundante, por lo que hay que hacer una síntesis de la información obtenida. Los datos que se observan en la Figura 3-17 son diversos. Destacan el servidor al que redirecciona, el controlador del nodo, los teléfonos y la posición física del servidor.

Figura 3-17 Exploración entorno a la IP del correo.

A través de Maltego se analiza la imagen de la Figura 3-17.En ella, se sigue corroborando que el usuario pertenece al Ministerio de Defensa, y arroja información de localización de los servidores

[54] Programa utilizado para convertir una información de un formato a otro.

utilizados. En este caso, la información de los servidores no es de gran utilidad, pero lo puede ser en el caso de investigar a una pequeña empresa o similares.

Otra información de carácter destacable es que la herramienta indica los controladores del nodo, incluso sus posibles teléfonos de contacto. Entre estas personas físicas identificamos a *sujeto número 69* y *sujeto número 88*, de los que se habla más adelante.

Como curiosidad de esta transformación (de la que se ha eliminado mucha información con el fin de no caer en la infoxicación), cabe puntualizar la transformación que nos lleva a la página de *"forocule"*. Como curiosidad, su tema de conversación en una de sus publicaciones versa sobre la detección de intrusión en su foro de una IP proveniente del Ministerio de Defensa como se puede ver en la Figura 3-18 . Esto demuestra que cualquier usuario puede realizar los pasos hasta ahora citados.

Figura 3-18 Conversación "forocule" [72].

Mediante el estudio de las transformaciones se obtiene incluso la forma en la que se encuentra estructurado el Ministerio de Defensa, en lo que a disposición de servidores se refiere. Como curiosidad, destacan los dos servidores de correo (Figura 3-19). Esto se puede deber al enorme volumen de correos que gestiona o como elemento de apoyo en caso de necesidad.

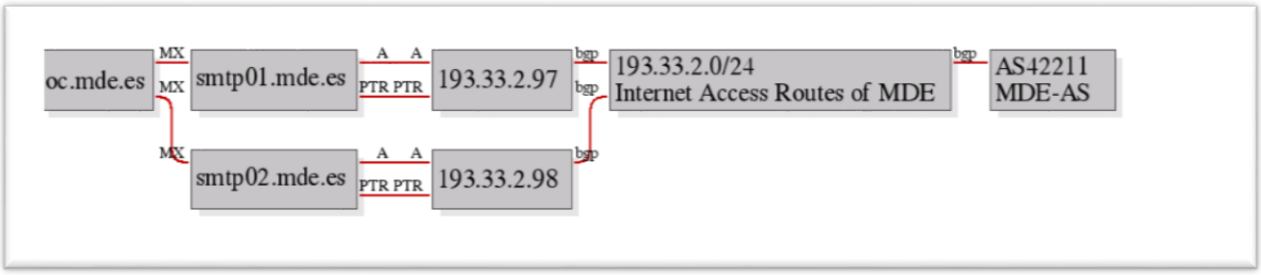


Figura 3-19 Estructura red de Defensa.

Destaca también que la información vertida por la herramienta Maltego se puede conseguir a través de https://www.ripe.net accesible en línea (solo ofrece información de la IP).

3.3 Estudio del entorno del sujeto

El desarrollo de las herramientas de OSINT, permite analizar al sujeto de estudio y su entorno. Lo que se consigue es aumentar la información del sujeto facilitando la intrusión en su entorno.

Las redes sociales han sido el vector esencial para dicho estudio. En la actualidad, existen aplicaciones para estudiar páginas de dichas redes sociales, estableciendo relaciones entre todos los usuarios que pertenecen a esta. Esto es otro condicionante para continuar el estudio, tanto del sujeto como de su entorno.

En el caso del sujeto de estudio, se observó que usaba la herramienta de SKYPE. En este caso es una información poco útil, a no ser que el ataque vaya dirigido a través de dicha plataforma y se utilice para acercarse a la víctima. En la actualidad, la utilización de esta herramienta es menor entre los usuarios que unos años atrás. Un buen elemento de estudio son las transformaciones que se pueden hacer sobre la red social Facebook, ya que el sujeto de estudio no cuenta con la privacidad y seguridad necesaria para su protección y la de su entorno.

Durante el presente trabajo en el que se ha realizado un minucioso estudio de las distintas redes, cabe señalar la enorme cantidad de datos de carácter personal o incluso hasta cierto punto privado que los usuarios, relacionados con el sujeto inicial de estudio, han vertido a las distintas redes sociales.

Es interesante e importante destacar como la "sociedad de la información" ha desarrollado sus potenciales hasta tal extremo que, en muchos de los casos la privacidad y la seguridad es prácticamente nula.

En la transformación llevada a cabo se muestran únicamente los contactos relacionados con el sujeto, pero, como atacante y en lo que a trabajo de investigación se refiere, únicamente nos centramos en los objetivos de carácter militar.

Durante la realización del presente trabajo se observa y analiza que los usuarios mostrados a continuación no solo violan su propia seguridad, así como su propia privacidad. Muchos ellos pueden poner en evidencia la imagen de las Fuerzas Armadas, así como poner en peligro a sus familiares, allegados o contactos más cercanos.

Relacionado con lo citado, recordamos la filtración por parte de un grupo de *hackers* del ISIS, en la que se llevó a cabo el vertido a la red de datos de carácter personal de miembros oficiales generales y comandantes del ejército de los Estados Unidos. La Figura 3-20 muestra el mapa social del atacado, únicamente obtenido a través de la plataforma Facebook.

Mediante el análisis de la red, destaca que está formada por un total de 28 miembros de las Fuerzas Armadas (los cuales son identificables o se reconocen como tal a través de redes sociales). Sobre estos somos capaces de obtener informaciones tales como teléfonos móviles, comentarios sobre productos comprados en la red, direcciones de correo, alias, direcciones de sus residencias, junto con teléfonos fijos, información sobre su estado civil, aficiones y, sobre todos ellos, su número de DNI.

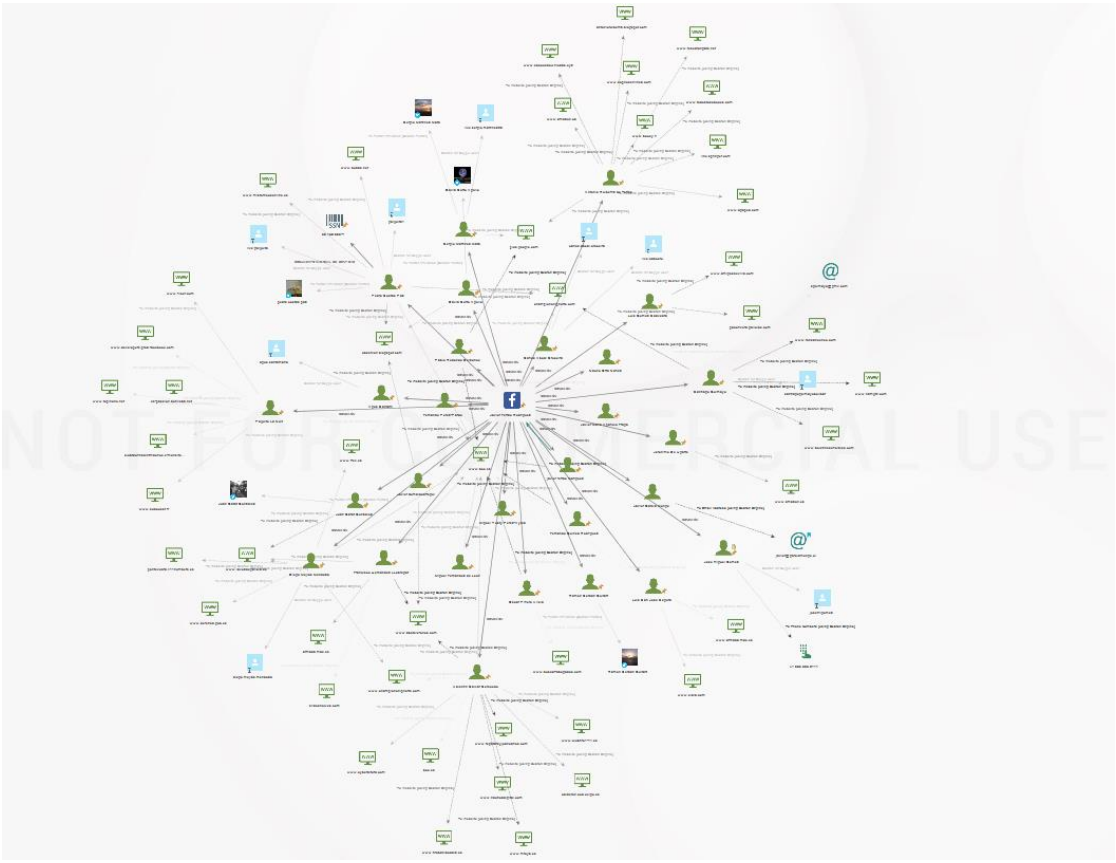


Figura 3-20 Entorno militar del sujeto de estudio.

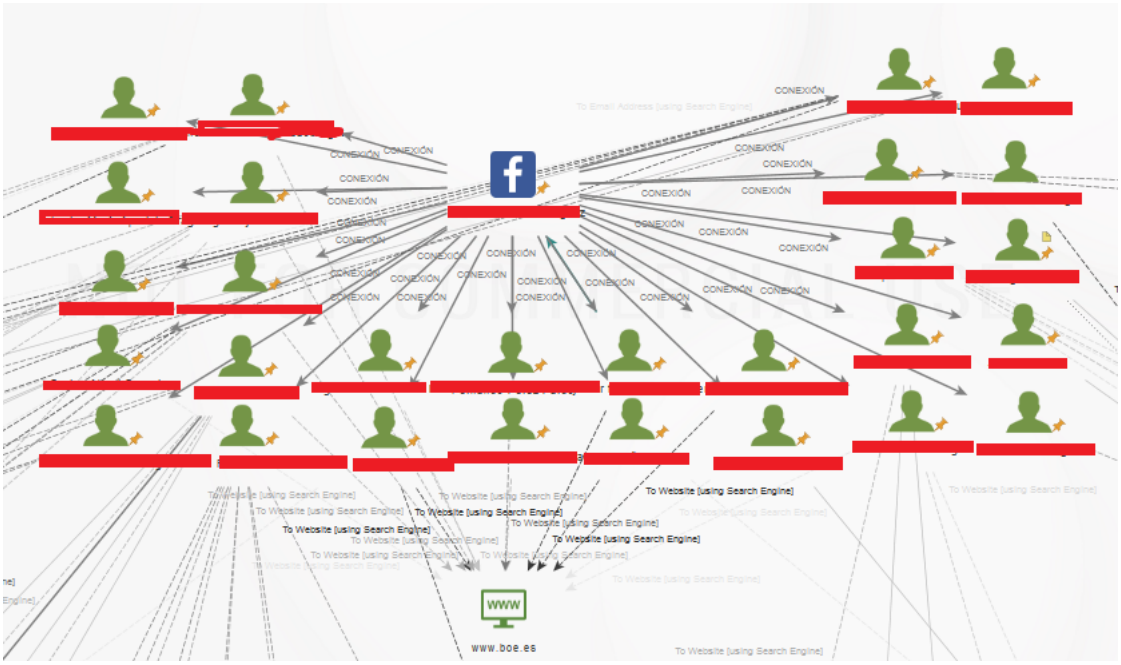


Figura 3-21 Entorno militar del sujeto de estudio.

Sobre estos se puede incluso ver sus perfiles en otras redes sociales, de las cuales su nivel de seguridad será bajo dentro de los estándares de seguridad que ofrecen estas plataformas.

De la Figura 3-21 destaco la relación que guardan la mayoría de los contactos de la víctima con las publicaciones del Boletín Oficial del Estado, pudiendo destacar de esta que todos aquellos que aparecen en la misma publicación del Boletín se les encuadra en la misma promoción de oficiales.

También se destaca de estos el uso de SKYPE, desde donde se puede obtener el lugar de residencia, aunque en la mayoría de los perfiles investigados son los propios usuarios los que facilitan esta información.

Cabe destacar de la auditoria de los perfiles realizada, la falta de concienciación respecto del material que el personal de Fuerzas Armadas tiene subida a la red. Se deber recordar que la red es accesible para todos los usuarios, sean o no contactos conocidos. Además de la posible mala imagen que se pueda dar de las Fuerzas Armadas, la exposición en redes sociales de información personal, o enaltecimiento del pensamiento político-ideológico y religioso son hechos que pueden ir en contra de las Fuerzas Armadas.

A continuación, se cita información relevante de distintos sujetos y ejemplos de ataques que se podrían realizar sobre ellos.

3.3.1 Sujeto 1

Del sujeto 1 deducimos que se trata de un Oficial de la Armada Española y se puede obtener hasta la especialidad del mismo. Es un piloto de avión. Entre otra información, podemos obtener las aficiones del mismo, su DNI y sus cuentas de Twitter, SKYPE y Google Plus.

Figura 3-22 Ejemplo indecoroso sujeto 1.

Debido a la confidencialidad que ha de darse a la imagen (Figura 3-22) no se muestra la imagen real pero se puede observar al sujeto con el uniforme de vuelo y los pies encima de la mesa, y con el galón de empleo en el parche de pecho, junto con nombre y grupo sanguíneo del mismo.

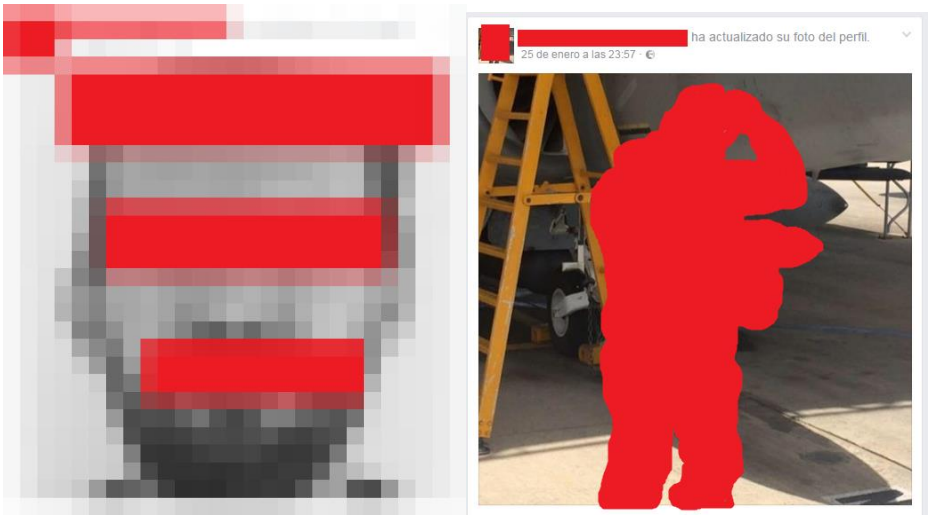


Figura 3-23 Rasgos faciales y pre vuelo del sujeto 1.

Mediante el estudio sobre las imágenes obtenidas, la conclusión a la que se puede llegar, es que puede ser un posible blanco de ingeniería social, al reflejarse el mismo usuario como piloto de la Armada Española en la red. Un atacante, lo primero que haría sería ver dónde tiene la base el arma aérea de la Armada. Tras esto y debido a la facilidad de información gráfica del sujeto, se le podrá reconocer fácilmente a través de las fotos.

La forma más efectiva demostrada durante los últimos años [73] ha sido la elaboración de perfiles falsos en redes sociales haciendo que soldados israelíes cayeran en diversas trampas planteadas por el grupo terrorista HAMAS[55] con el fin de obtener información confidencial de los mismos. En el caso de este usuario, por su margen de edad, las principales plataformas serán Facebook, Twitter, Instagram. Si hubiese que acercarse a dicho usuario, sabiendo donde poder encontrar al objetivo, situándonos en las cercanías de la base de Rota, se podría utilizar "*Tinder"* (aplicación destinada a la búsqueda de pareja) con un perfil falso (en el caso de que no tuviera pareja) o, como entusiasta de los aviones, ofreciéndole empleo o realización de una exhibición aérea.

De esta forma, con un perfil falso en una red social, se intentaría ganar la confianza de la víctima. Además, como ya sabemos la plataforma que utiliza el usuario, al menos la plataforma móvil obtenida mediante la herramienta "*Creepy"*, se podrá diseñar un *malware* ajustado al mismo con el fin de ser introducido en la plataforma objetivo. De la Figura 3-24 podemos deducir que el uso que este usuario le da a Twitter es escaso y que lo hace desde web o desde iPhone.

User has been using the following clients :

Client Application	Count
Twitter Web Client	6
Twitter for Websites	3
Mobile Web (M2)	2
Twitter for iPhone	1

Figura 3-24 Plataformas desde las que se usa Twitter.

El método de ataque más recomendable sería enviar a la víctima un archivo con extensión .pdf, .doc o.jpg que usando un *binder* (pequeño programa que une dos archivos en uno con archivo ejecutable).

[55] Grupo terrorista que lucha por la imposición de un estado islámico en palestina.

Es reseñable, después de analizar al sujeto la Ley Orgánica 8/2014, de 4 de diciembre, de Régimen Disciplinario de las Fuerzas Armadas, que clasifica de falta grave en su punto 27 todos aquellos actos que dañen la imagen de las Fuerzas Armadas.

3.3.2 Sujeto 2

Del sujeto 2 se deduce que se trata de un Oficial de la Armada Española y podemos obtener la especialidad del mismo. Es un piloto de helicópteros (Figura 3-25).

Figura 3-25 Fotografía de perfil de Facebook.

Como se ha comentado, en muchas ocasiones ciertas imágenes vertidas a redes sociales hacen que no solo se deje en entredicho la imagen de las Fuerzas Armadas, sino que, información, con grado de confidencialidad, se expongan en la red.

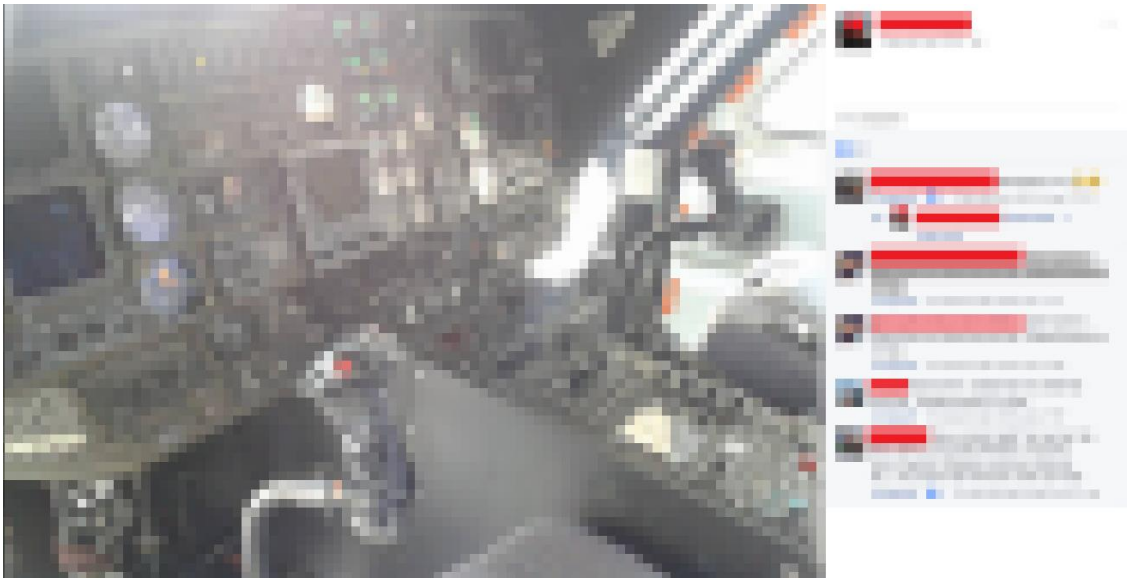


Figura 3-26 Fotografía de portada de Facebook (nacional secreto).

En la Figura 3-26, se puede ver el tablero instrumental de un helicóptero de la Armada Española, cuya clasificación de seguridad en este caso es *secreto*. Dicha información podría ser utilizada para realizar un sabotaje sobre el aparato, chantaje sobre el piloto o similares. Como el ejemplo anterior, los pilotos de la Armada manejan cierta información que, por su grado de confidencialidad, requieren un especial cuidado a la hora de ser manipuladas.

Debido a la franja de edad que se le estima al usuario (mediante el BOE.), la forma de acceder al usuario sería la misma que la citada en el ejemplo anterior.

3.3.3 Sujeto 3

El sujeto 3, es un Oficial, cuyo fallo de seguridad ha sido verter a las redes sociales los puertos por los que ha pasado o iba a pasar su barco (en este caso una fragata). Destaca que dichos mensajes (Figura 3-27) van con fecha y hora. En vista a un sabotaje se podría calcular la llegada y la salida del barco.

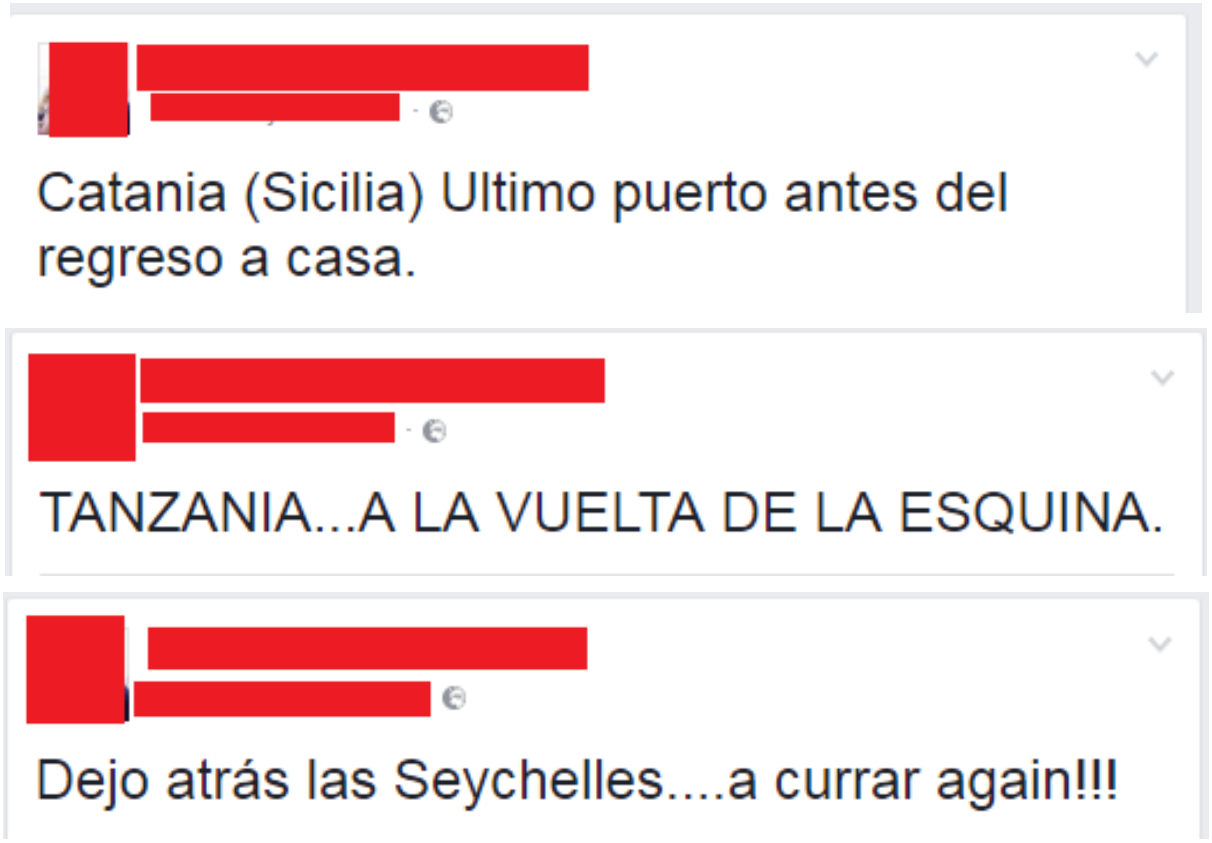


Figura 3-27 Derrota de su buque publicada en Facebook.

Mediante la exploración de las fotos, es posible ver quién son sus familiares y podemos verlo con el uniforme (y nombre en la uniformidad). Esto corrobora que sus apellidos son los que corresponden con su perfil y corrobora el empleo del mismo.

Resulta oportuno destacar el mensaje de un soldado israelí en 2010 a través de Facebook en el que cito su contenido: *"Limpiaremos Katana y el jueves volveremos a casa"; Katana es un pequeño pueblo cercano a Ramala (Cisjordania)* [43]. Por dicho motivo, se tuvo que suspender la operación que iba a llevar a cabo por el ejército israelí.

En este caso, desvelar la posición de una unidad puede producir, que haya que realizar un cambio de puerto precipitadamente debido a que se pueda poner en riesgo a dicha unidad.

3.3.4 Información de otros sujetos adyacentes

Llegados a este punto de exploración del entorno del sujeto, cabe destacar la cantidad de información que se ha podido obtener de forma aislada. Es decir, se ha encontrado información de los sujetos del entorno, pero no la necesaria para poder ser desarrollado como sujeto aparte. En cualquier

caso hemos querido destacar la información susceptible de sufrir un ataque, adjuntando el razonamiento y el porqué de realizar dicho ataque.

Figura 3-28 Fotografía obtenida del Facebook del sujeto.

La Figura 3-28 es una foto que puede pasar desapercibida, en la que el usuario denuncia un hecho en su ubicación. Esta imagen arrojaría información de interés para un atacante.

Si se observa bien y se analiza la fotografía, somos capaces de percibir el pase de un coche en el reflejo del cristal. También observamos, que la fotografía está tomada desde el lado del conductor, por lo que es muy probable que el pase que se refleja en el cristal sea del mismo sujeto que está realizando la fotografía.

Al ser un reflejo, se ve que la imagen está dada la vuelta, el atacante realizaría una depuración de la imagen para obtener el resultado de la Figura 3-29:

Figura 3-29 Pase de la Base Naval de Rota.

Un atacante tendría la información de la matrícula del coche del sujeto a atacar y la utilizaría para conocer la identidad de su coche. Sabiendo esto, se puede relacionar un coche con una matrícula y puede ser utilizarse para futuros ataques sobre el individuo, ya que también conocemos su DNI y, mediante sus fotos, su apariencia física.

Otra información, que la búsqueda en fuentes abiertas nos vuelca sobre este último individuo es los posibles gustos, ya que se pueden encontrar a través de la página de Amazon (Figura 3-30) distintos comentarios suyos, que como atacante se puede utilizar para aproximar a la víctima.

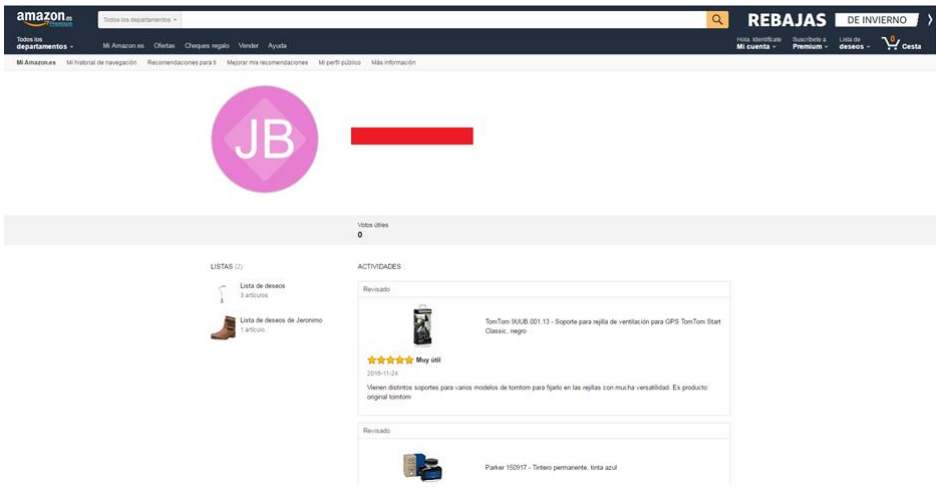


Figura 3-30 Comentarios en Amazon.

Como el sujeto ha compartido comentarios en Amazon (Figura 3-31), se puede falsear la información para enviarle una encuesta sobre un producto o calificar su comentario de provechoso una empresa ficticia y querer recompensar a la víctima ofreciéndole cualquiera de sus productos. Para esto último, le pediría que corrobore los datos de recepción con el fin de que acceda a proporcionar la suya.

Figura 3-31 Comentarios en Amazon.

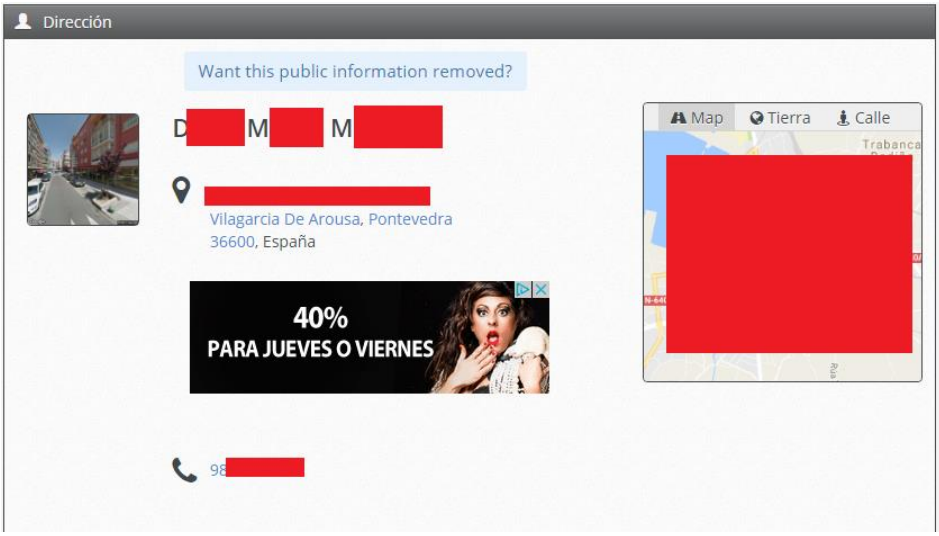


Figura 3-32 Dirección de la vivienda.

Como se puede apreciar en la Figura 3-32, se tiene la dirección de la vivienda de uno de los sujetos del entorno, Un Oficial de la Armada Española y, antiguo comandante de un patrullero de la Armada Española (información asequible a través de BOD).

Al tener la localización de un comandante de un barco, se puede pensar cualquier tipo de ataque pues ya se tiene mucha información sobre el atacado, del que sabemos, localización de su vivienda, empleo, nombre de la esposa, familia, DNI, así como sus últimos destinos.

Llegados a este punto, destacamos que información parecida vertida a la red sobre otros componentes de las Fuerzas Armadas ha propiciado ciertas complejidades en zona de operaciones, tales como falsos secuestros de personal de Fuerzas Armadas.

El hecho de que este tipo de información sea asequible por fuentes abiertas hace que no solo el comandante de la Unidad se encuentre en peligro, sino que la propia unidad se encuentre también en peligro. De esta forma, se puede aprovechar un despliegue de la unidad para chantajear con infringir daño a la familia del mismo o amenazar a la misma. Esto hará que el éxito de la misión se pueda comprometer, así como la propia unidad y sus integrantes.

3.3.5 Sujeto 88 y sujeto 69

Ambos dos son los encargados y controladores de la red del Ministerio de Defensa. En este caso, llevamos a cabo un pequeño estudio sobre ellos, ya que el puesto que desempeñan tiene cierto carácter "comprometido" debido a que, el control de la red del Ministerio de Defensa es un hecho que hace que ambos individuos tengan la responsabilidad de esta (al menos jurídica). Así, la red en la que van a ser explorados por su presumible margen de edad es LinkedIn.

- Sujeto 88: Se aprecia según la herramienta Maltego que carece de cualquier tipo de relación con las redes sociales al menos utilizando su nombre real, lo cual sería una medida positiva para cualquier miembro e integrante de las Fuerzas Armadas, aunque no se puede decir con total certeza que este sujeto sea miembro de las Fuerzas Armadas, o que la procedencia del mismo no sea a través del procedimiento de escuelas oficiales (se sabe que lo es porque fue corroborado por el CIFAS).

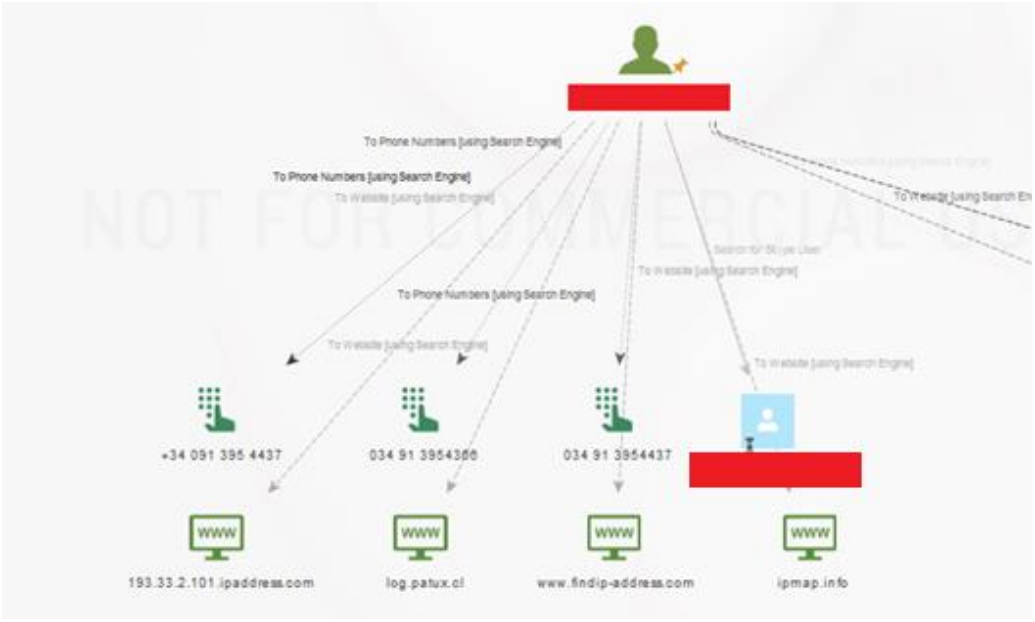


Figura 3-33 Exploración del sujeto 88 a través de Maltego.

Los teléfonos que se reflejan en la Figura 3-33 son los que se pueden obtener de la red del Ministerio de Defensa y que sirven de contactos con los mismos.

- Sujeto 69: A diferencia del sujeto anterior, dicho sujeto se encuentra presente en las distintas redes sociales como se puede ver reflejado por la herramienta Maltego (Figura 3-34).

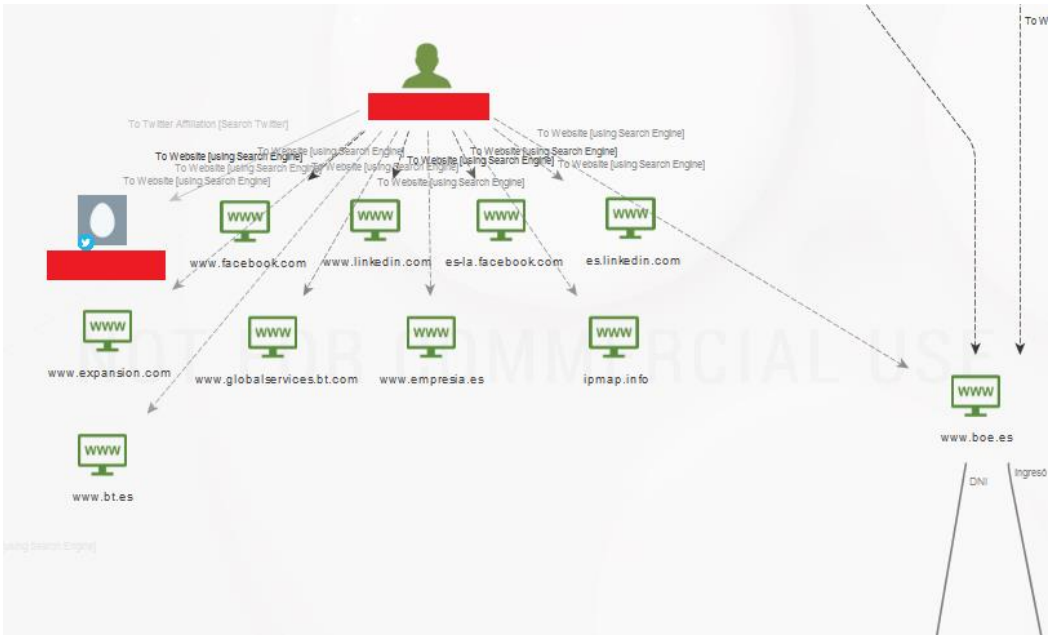


Figura 3-34 Exploración del sujeto 69 a través de Maltego.

Como se puede identificar en la imagen, el sujeto 69 forma parte del personal de las FAS, ya que se puede comprobar en el BOE, que proporciona el DNI.

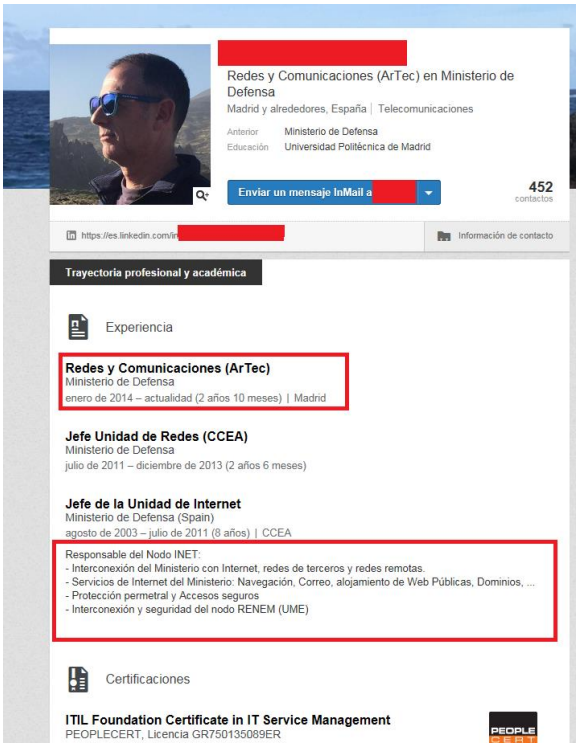


Figura 3-35 Presentación del sujeto 69 en LinkedIn.

Como se puede apreciar en la Figura 3-35, además de la información obtenida en los nodos de la red, su perfil de LinkedIn expone públicamente todos los destinos y elementos de mando que ha ejercido.

Este sujeto no es el único, ya que se ha apreciado durante la realización del presente trabajo que la red social LinkedIn es la más utilizada en ese margen de edad.

3.4 Exploración fuera del entorno-exploración en redes sociales

Uno de los grandes fallos de seguridad encontrados en el desarrollo de este trabajo ha sido ver la enorme cantidad de información que el personal de las Fuerzas Armadas, vuelca voluntariamente a las redes sociales, con el fin de colaborar con páginas cuya temática está relacionada con las Fuerzas Armadas. Sin embargo, se trata de páginas no oficiales que trabajarán para ensalzar o alabar la figura de los ejércitos de España y son los propios miembros de las Fuerzas Armadas quienes complementan o incluso rellenan el material disponible en dichas páginas.

Tras la investigación en las distintas páginas de dicha temática, se ha observado que se cumplen los estudios iniciales, en los que se destacaba la participación principalmente de integrantes de corta o mediana edad, en los que se comprendería hasta el empleo de capitanes/tenientes de navío, pasando por alumnos de escalas de soldado profesional, escala de suboficiales y escalas de oficiales de todos los ejércitos de España.

Durante dicha exploración, el guion que se ha seguido ha sido el desarrollo de la búsqueda en torno a dichas páginas. Es de especial relevancia resaltar que casi en su totalidad, estas páginas se encuentran abiertas al público y que es el boca a boca lo que las hace famosas, ya que no cuentan con el amparo del Ministerio de Defensa.

También, es de especial relevancia destacar, que el principal hecho motivante de la publicación en las distintas redes sociales es el *ego* [74] [75]. Este puede relacionarse directamente con unos de los principios de un ataque de ingeniería social. De esta forma, el desconocimiento por parte de la

sociedad española sobre el personal de las Fuerzas Armadas es el iniciante del proceso que, conducido por el *ego*, lleve a la imprudencia de publicar material en redes sociales de forma que se publiquen fotos o información que puedan comprometer a la persona/unidad o sus integrantes.

Dentro de las Fuerzas Armadas existen distintos gabinetes de prensa cuya misión fundamental (entre otras) es dar a conocer las labores de las FAS. La publicación de material independiente no hace más que poder causar el efecto contrario, en lo que a marketing e imagen de las FAS refiere, así como al vertido de información innecesaria.

3.4.1 Exploración en redes sociales

A continuación, se exponen distintos casos encontrados en las redes sociales, en los que su publicación puede suponer un riesgo importante y se encuentra reflejado su negativa en el código penal militar.

- El caso del Teniente piloto: Este sujeto tiene una cuenta de Instagram en la que fácilmente se puede ver su día a día que muestra orgulloso. Esta no es su labor, ya que en la mayoría de las imágenes se vuelve susceptible de ser víctima de un ataque.

Figura 3-36 Fotografías obtenidas a través de Facebook del teniente piloto junto con la aviónica de F-18 y apaga incendios en segundo lugar.

En la Figura 3-36, en la primera foto, el piloto se encuentra volando en un F-18 (biplaza, lo que hace pensar que no es piloto habitual de dicho aparato). En los comentarios, se puede leer incluso su nuevo destino que sería Torrejón de Ardoz (donde se encuentran el Ala 12 y el Ala 43), información de por sí interesante, si bien la importancia radica en el cuadro de la aviónica del F-18, cuya clasificación de seguridad es *secreto*. En cuanto a la segunda foto, dicho piloto festeja su actividad en los incendios de Galicia (lo reseña en la foto, es piloto del Ala 43). Destaca de esta foto que los mandos del avión de incendios, utilizados por el ejército del aire, carecen de clasificación de seguridad *secreto*.

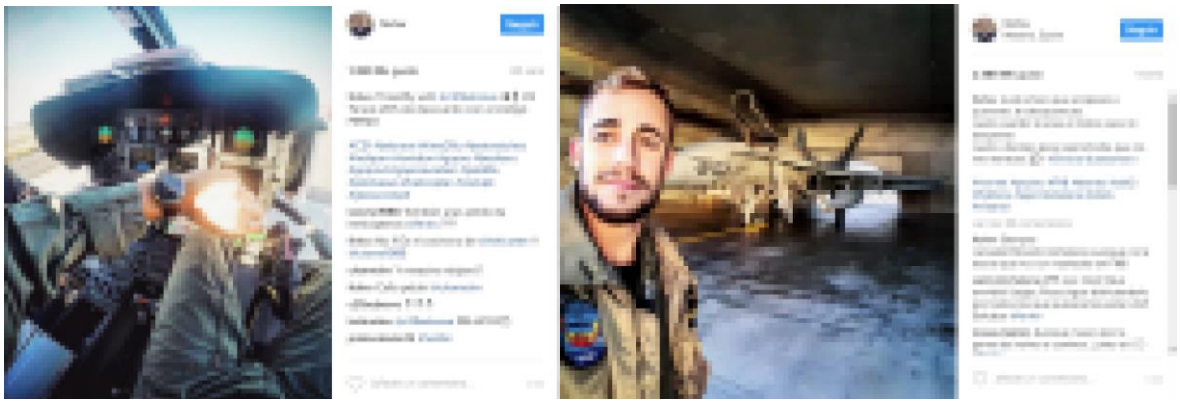


Figura 3-37 Fotografías de aviónica de helicóptero y avión F-18 en bunker de espera.

Se puede plantear que quizás en la fotografía sea difícil sacar información. Anteriormente, ya se han utilizado fotografías para saber qué tipo de armamento pueda llevar o no una plataforma. Destaco el ejemplo del debate [19] suscitado por la capacidad real de los submarinos israelíes de la clase *Dolphin*. Dichos submarinos fueron construidos por los astilleros alemanes Howaldtswerke-Deutsche Werft, cuyos planos fueron clasificados de confidenciales, únicamente conocidos por astillero y cliente. Sobre esta clase de submarinos se especularía sobre la capacidad de portar misiles de más calibre que el calibre estándar de 533 mm. Sin embargo, a través de una foto vertida a fuentes abiertas se pudo apreciar a ojo experto que montaba cuatro lanzadores cuyo calibre era superior, de 650 mm, lo que produjo que dicho submarino se le presumiesen distintas capacidades de las inicialmente especuladas.

Otro ejemplo, relacionado con el armamento desplegado o con potencial de ser desplegado, fue el motivo de réplicas a nivel internacional a Rusia, ya que se descubrió que, en contra de lo declarado una semana antes, en el que declaraban que retirarían los aviones de Siria movieron los aviones de ubicación para que no pudieran tomar fotos satélites del lugar y aumentaron el número de estos [76].

Ambos ejemplos citados pueden ser perfectamente relacionados con las imágenes anteriormente mostradas. Además, este sujeto podría ser objeto de ataque mediante vectores como la confianza de la víctima para subir acompañantes a cabinas del avión (Figura 3-38).

Este vector utilizado por HAMAS contra soldados israelíes, aprovechándose de la confianza de estos para obtener información [73].

Figura 3-38 Piloto con personal civil en cabina de uso militar.

Como conclusión final de dicho sujeto, destaca la facilidad con la que se sube material *secreto* a las redes sociales así como el poco trato de cuidado que se les da a estas.

Como último ejemplo, se muestra la cabina de un AC-130, obtenida del mismo sujeto (Figura 3-39).

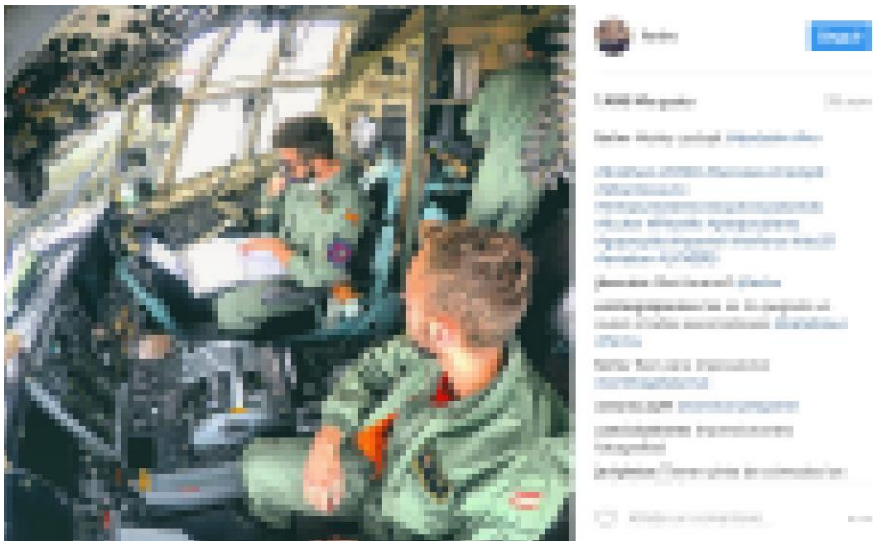


Figura 3-39 Cabina de un C-130.

- El caso del Capitán piloto: En este caso, se trata de un piloto que no tiene dificultad para subir cualquier tipo de información a páginas relacionadas anteriormente. A diferencia del anterior piloto cuyas publicaciones eran prácticamente escasas, no tiene ningún problema en compartirlo todo.

  Se graba con su móvil en la cabina (Figura 3-40 y Figura 3-41), realizando despegues o muestra maniobras realizadas con el avión. A diferencia del anterior, no muestra el instrumental de los aparatos que maneja, aunque facilita su apellido (al igual que el anterior). Sabiendo esto, se puede hacer minería de datos sobre este sujeto con el fin de obtener información.

  A través de sus fotos sabemos que estuvo desplegado en el aeropuerto de Trapani, que se encuentra en Sicilia que es uno de los aeropuertos utilizados por la OTAN, como alerta temprana y del cual sabe, a través de Internet, que España cuenta con F-18 desplegados allí.

Figura 3-40 Fotografías obtenidas a través del Instagram del piloto.

Resulta de especial importancia destacar que este piloto se muestra activo a la hora de contestar preguntas que los distintos usuarios le hacen en sus fotos. Destaca el número de vuelos que realiza el sujeto, aparte de indicar a través de etiquetas información como su destino, el aparato que vuela o similares.

Destacamos también que el F-18 es un avión que tiene modelo monoplaza y biplaza. Resulta curioso que el otro piloto del avión es el del ejemplo anterior. Por lo tanto, se podría obtener la dotación de dos pilotos de la aeronave de prácticas (ya se ha reseñado que

el primer piloto se trata de un piloto de otro Ala), ya que las biplaza son utilizadas con esa finalidad. Además de saber sus dos nombre y apellidos, por fotos anteriores se puede obtener la numeral del avión volado.

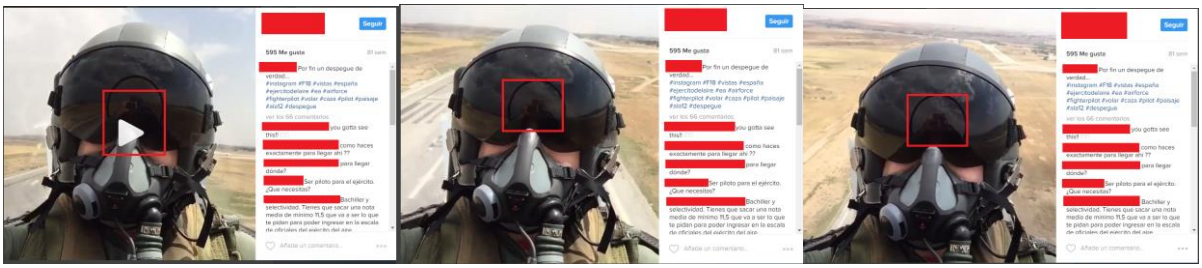


Figura 3-41 Fotografías tomadas desde móvil del piloto despegando en solitario.

Las etiquetas se utilizan para proporcionar la mayor cantidad de información. Aunque las preguntas contestadas puedan pasar desapercibidas, resultan de especial interés cuando el piloto se encuentra desplegado en la zona de operaciones como en el ejemplo del aeropuerto de alerta temprana utilizado por la OTAN. Destacamos de este, que fue utilizado por los pilotos de la OTAN para realizar misiones sobre el suelo de Libia.

Figura 3-42 Fotografía del piloto junto a su avión.

De la fotografía de la Figura 3-42 destacamos la situación donde fue tomada, así como la cantidad de etiquetas que nos pueden volcar información y la numeral del avión.

- El soldado de Canarias 50: Se identifica como tirador de precisión de dicha unidad y vuelca a las redes sociales, información tal como su especialidad, misiones y demás.

Figura 3-43 Fotografía obtenida a través de Instagram de las maniobras del tirador.

Estas imágenes (Figura 3-43) que pueden dañar la imagen de las Fuerzas Armadas y pueden ser utilizadas como chantaje para no ser publicadas en un periódico o medio similar. Además, se ha conseguido el nombre y apellidos del sujeto.

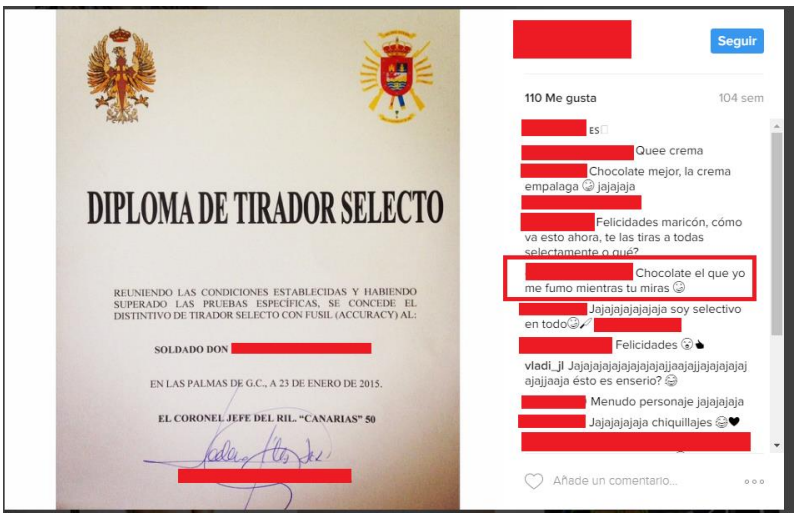


Figura 3-44 Diploma tirador selecto.

En la Figura 3-44 se puede apreciar la firma y el nombre del Coronel del regimiento.

- El caso del agente del CNI: Las redes sociales no perdonan a cualquiera. Es el caso del sujeto de estudio, del que se presupone una forma de actuar sigilosa y alejada del ego de las redes sociales, aunque proporciona nombre y apellidos, e incluso su alias (Figura 3-45).

  Aunque protege su perfil de una forma que él considerá provechosa. Sin embargo, se puede deducir ciertos lazos o relaciones con personal adyacente.

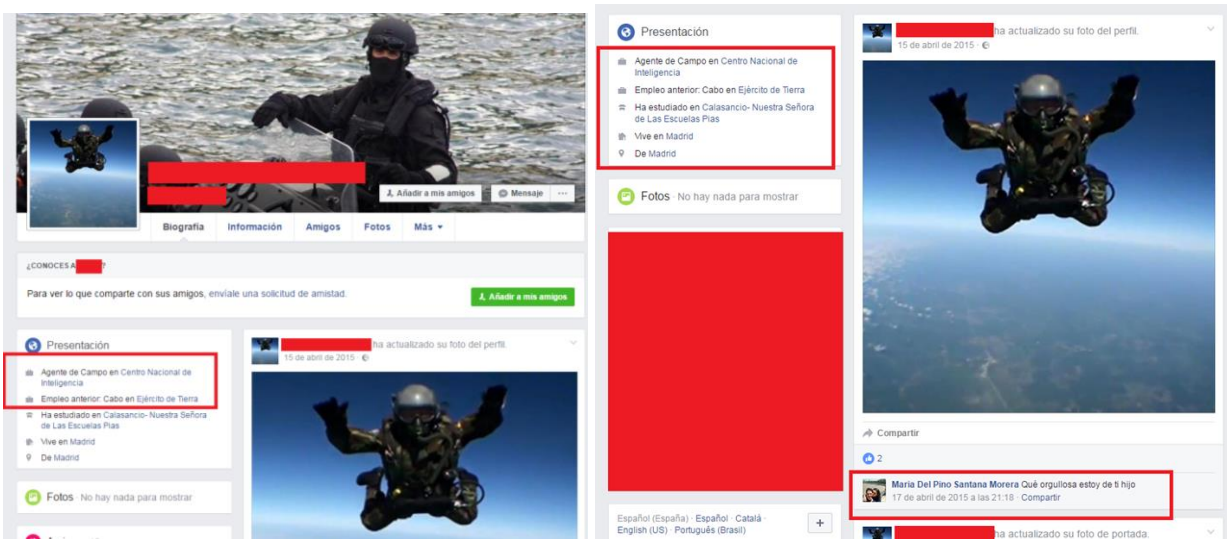


Figura 3-45 Perfil del miembro del CNI.

Otro hecho a destacar es que una mujer comenta sus fotos. Si se investiga el perfil, se descubre que siempre tiene fotos con el que se presupone su pareja y que el sujeto nunca se encuentra etiquetado en esas fotos y nunca comenta. Esto se puede deber a que guarden cierta relación o que la relación sea inexistente. Sea como sea, existe datos suficientes para continuar investigando a dicho sujeto.

3.4.2 Utilización de herramientas OSINT

- Creepy: Durante la utilización de esta herramienta, el modo de actuar ha sido mediante la cuenta de Twitter de alguno de los sujetos o mediante la exploración de zonas donde haya personal de las FAS.
  En el primero de los casos, se procede a explorar el Arsenal de Cartagena. Cabe destacar que debido a la movilización y repulsa en las distintas redes sociales se ha recortado las capacidades de dicha herramienta, no permitiendo su uso en la red de Instagram. Por otra parte, destacamos que dicha red es de la más utilizadas por el personal de las FAS. De esta forma utilizamos un *plug in* de Twitter que ofrece la herramienta.
  Así al efectuar dicha herramienta sobre la posición del Arsenal de Cartagena se puede apreciar que la publicación de la Figura 3-47 se ha realizado justo en frente del Arsenal de Cartagena (Figura 3-46). En consecuencia, se procede a estudiar el objetivo.

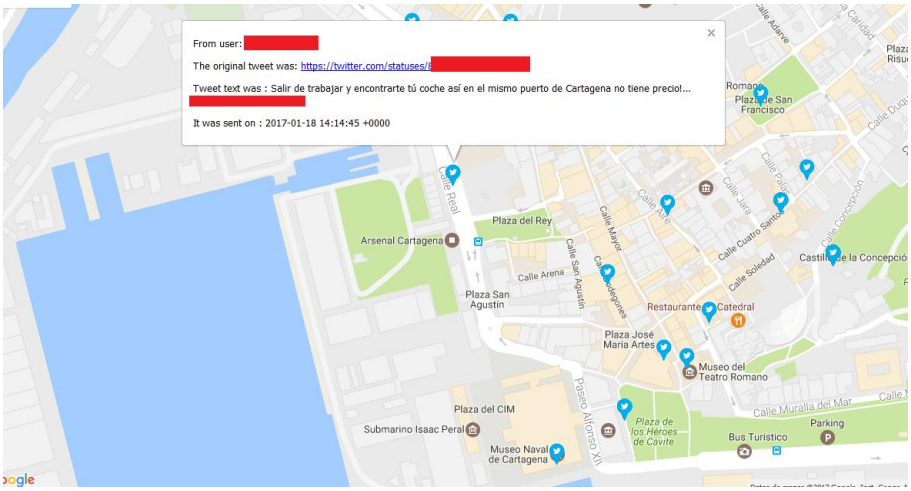


Figura 3-46 Creepy sobre Cartagena.

Figura 3-47 Tuit del sujeto a estudio.

Tras ver en su perfil, se puede observar que se trata de un marinero. El mismo sujeto es capaz de darnos a través de su perfil los datos de teléfono, correo y ubicación. Es decir, ahorra un gran trabajo a la hora de poder preparar cualquier tipo de ataque sobre dicho objetivo.

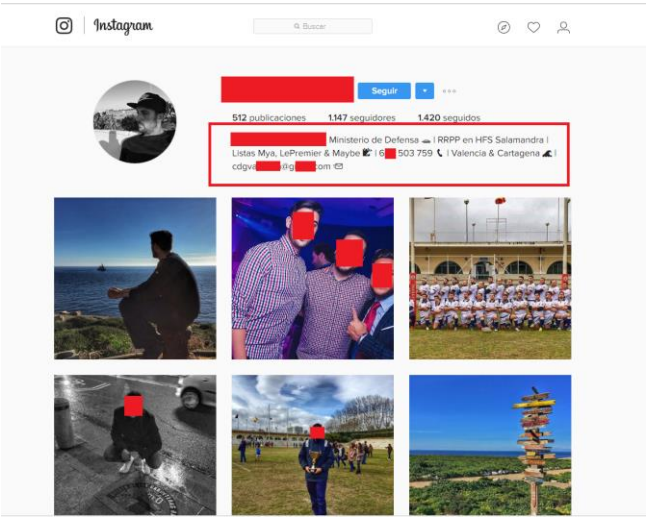


Figura 3-48 Confirmación de identidad mediante Instagram.

Entre otras de las curiosidades, se puede obtener de su perfil la matricula junto con el modelo de su coche (Figura 3-49).

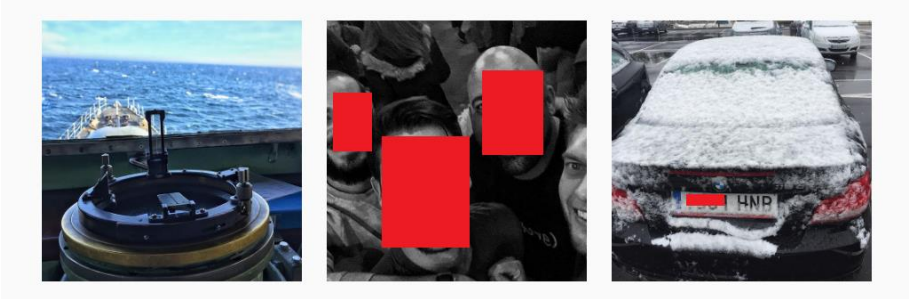


Figura 3-49 Información del sujeto.

Si se quisiera efectuar cualquier tipo de ataque sobre dicho sujeto, se pasaría dentro de la herramienta Creepy a buscar información del sujeto en lugar de hacer una búsqueda de área.

De esta forma, al focalizar la búsqueda sobre un objetivo, somos capaces de ver la rutina del sujeto, la ubicación actual o incluso si va al gimnasio seriamos capaces de conocer la ubicación del mismo. Tras efectuar dicho tipo de búsqueda, obtenemos la ubicación del trabajo del mismo, gimnasio, la ubicación de su vivienda, o su vivienda en Valencia, lugar de origen del sujeto. También se obtiene su lugar de estudios, tanto militares como civiles.

Figura 3-50 Patrón de movimiento.

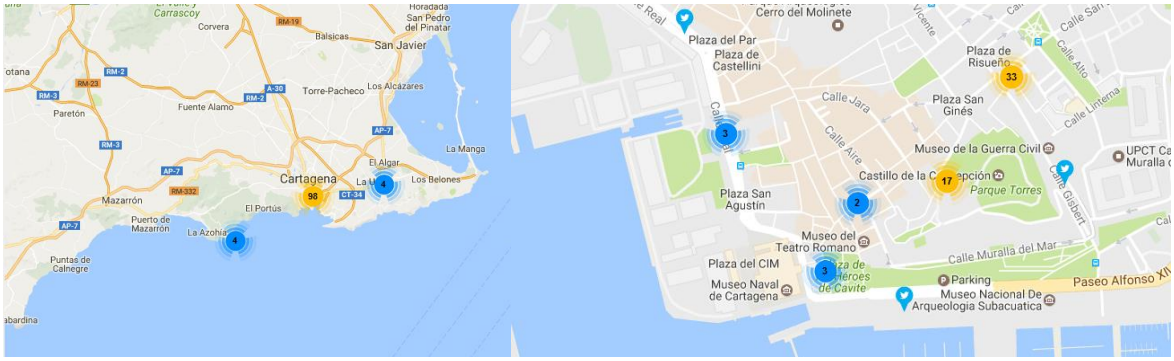


Figura 3-51 Máximos puntos de emisión.

Se puede apreciar en la Figura 3-50 y Figura 3-51 los patrones de movimiento del sujeto.

En su caso, de Cartagena se puede saber lugar de trabajo, el cual se sabría mediante el *tuit* inicial. En la Figura 3-52 se observa el lugar de la vivienda y el gimnasio.

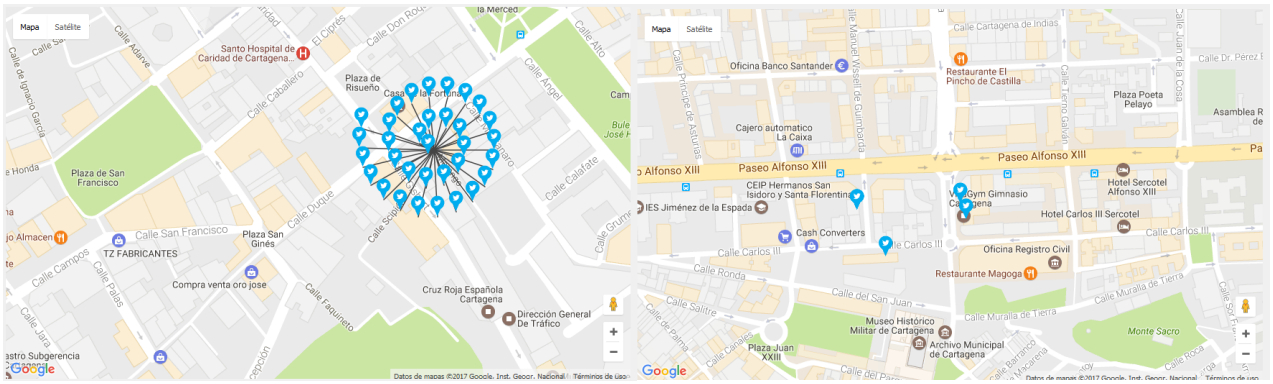


Figura 3-52 Vivienda desde donde se envían los tuits y gimnasio del sujeto.

Al ejecutar la herramienta sobre la posición de la Escuela Naval Militar no se obtiene ningún tuit sobre la localización. Aunque en los aledaños si se ha encontrado material de personal de la Armada Española, siendo más preciso el de uno de los alumnos de la Escuela Naval Militar, cuyo contenido versaba sobre imágenes del adiestramento a flote de los alumnos de la escuela.

- Foca: La unica forma de usar esta herramienta es mediante la obtención de metadatos que no hayan sufrido alguna clase de modificación, como imágenes obtenidas de Google Drive, Dropbox o correo electrónico.
  Así, se utiliza Foca para ver la información que se podría obterner mediante el correo inicial en el archivo que acompaña al correo *"interceptado"*. Es decir, es una herramienta de mucha ayuda si se intercepta un correo o bien se ejecuta alguna clase de *malware* dentro de una plataforma y se obtienen archivos que puedan ser analizados. La Figura 3-53 muestra una imagen de una captura de Dropbox.

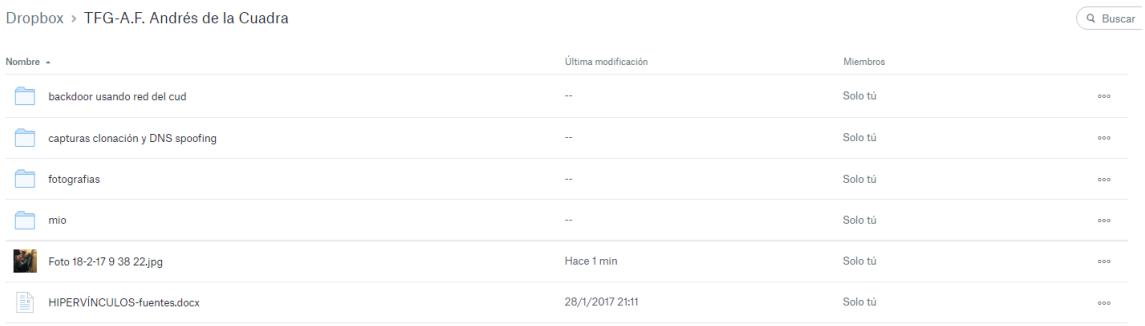


Figura 3-53 Ejemplo de imagen en Dropbox.

En este caso, se observa una de las imágenes con título de fecha. Procedemos a analizarla mediante la herramienta y seobtiene el resultado de la Figura 3-54.

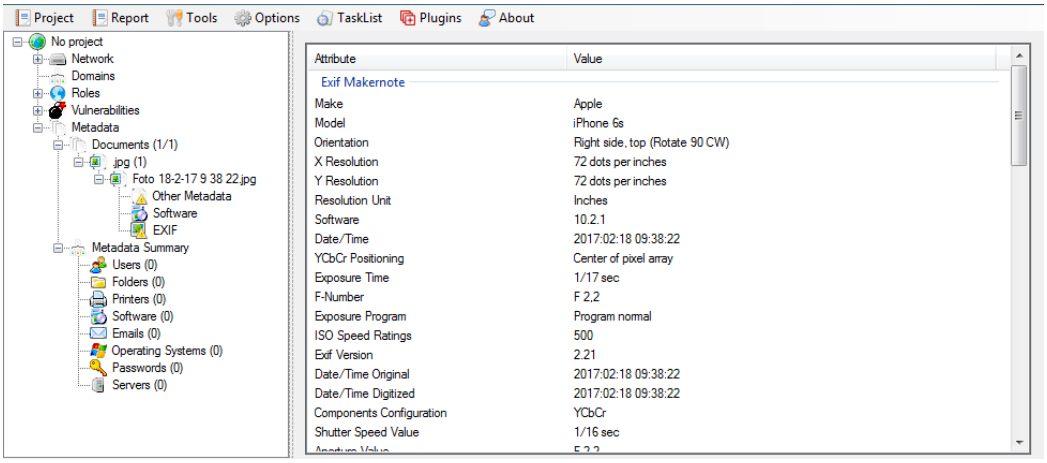


Figura 3-54 Datos a destacar de la extracción.

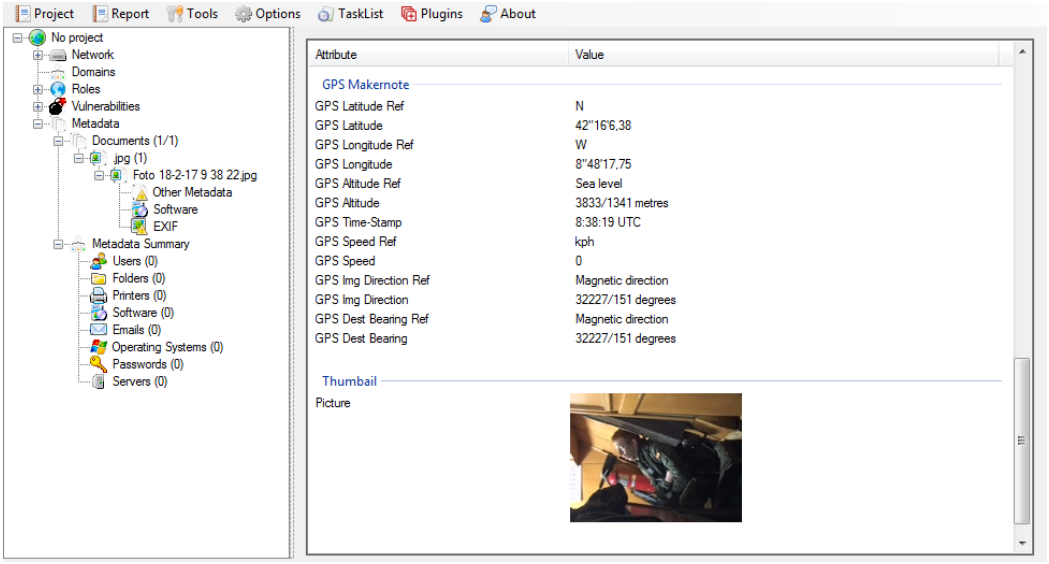


Figura 3-55 Geolocalización destacable.

Como se aprecia de la información obtenida, se puede obtener el modelo de plataforma desde el que se ha tomado la imagen. Si se quisiera realizar un ataque mediante *malware*, saber el tipo de plataforma a atacar facilitaría la estrategia a seguir. En este caso, la plataforma es un IPhone 6S. Otro dato interesante es la fecha, en el caso de ser un documento de texto, aparecería la fecha original y nos mostraría otra fecha en el caso de que el documento haya sido modificado.

Entre los otros datos de la Figura 3-55 destaca la latitud y longitud de donde fue tomada dicha foto, lo que puede ser un problema a la hora de subir cualquier tipo de foto o enviarla por correo de forma anónima. También muestra la altura de la foto, cero, ya que fue tomada dentro de un patrullero a nivel del mar.

- Google Dorks: Durante la utilización de Google Dorks, no se ha obtenido ningún tipo de perfil que guarde relación con personal de las FAS. Sin embargo, durante el presente trabajo, se han realizado búsquedas con Google Dorks y obtenido diversa información de interés como usuarios y cuentas de redes sociales, de almacenamiento en la red y plataformas intermediarias monetarias. La Figura 3-56 muestra como una empresa real y contrastada vuelca a la red información de usuarios y contraseñas de sus empleados, entre otras informaciones.

Client	Domain	Internet Service Provider	Domain Access			File Transfer Protocol	
Information	Registrar	Server Hosted by	Internet Domain Name	Login ID	Password	FTP Host Name or IP Address	
Dempsey Communications, LLC	Web.com	Infinology.com	www.mirandapub.com	DJDEMPSEY	DJD353	win7.infinology.net	
Main: 770.392.7100 **David J. Dempsey** Home: 770-569-5199 DJDempsey@coleman-dempsey.com Suite-1257 #2 Ravinia Atlanta, GA 30348 AX: 372718399911004 Exp: 07/05 **1st Year: $95.40**	? years Acct# yyyymmmdd	Premium Plan - 1st yr. Acct# 2004MAR30 to 2005MAR31 help@infinology.com dns2.infinology.net 38.118.142.212 dns1.infinology.net 38.118.142.211 POP3: mail.mirandapub.com SMTP: mail.mirandapub.com	WebMaster@mirandapub.com PostMaster@mirandapub.com MLCarter@mirandapub.com DJDempsey@mirandapub.com MCollins@mirandapub.com Kathy@mirandapub.com help@infinology.com ../faq/ ../cpmanual/	email email email email	[redacted]	Login: djdempse Password: [redacted]	
Dempsey Communications, LLC	Web.com	Infinology.com	www.legallyspeak.com	DJDEMPSEY2	DJD3532	win7.infinology.net	
Main: 770.392.7100 **David J. Dempsey** **Home: 770-569-5199** DJDempsey@coleman-dempsey.com Suite-1257 #2 Ravinia Atlanta, GA 30348 AX: 372718399911004 Exp: 07/05 **1st Year: $95.40**	? years Acct# yyyymmmdd	Premium Plan - 1st yr. Acct# 2004MAR28 to 2005MAR29 help@infinology.com dns2.infinology.net 38.118.142.212 dns1.infinology.net 38.118.142.211 POP3: mail.legallyspeak.com SMTP: mail.legallyspeak.com	WebMaster@legallyspeak.com PostMaster@legallyspeak.com MLCarter@legallyspeak.com DJDempsey@legallyspeak.com MCollins@legallyspeak.com help@infinology.com ../faq/ ../cpmanual/	email email email	[redacted]	Login: djdemps0 Password: [redacted]	

Figura 3-56 Ejemplo de fichero extraído por Google Dorks.

La Figura 3-57 enseña como una persona muestra información personal y de los perfiles de su empresa.

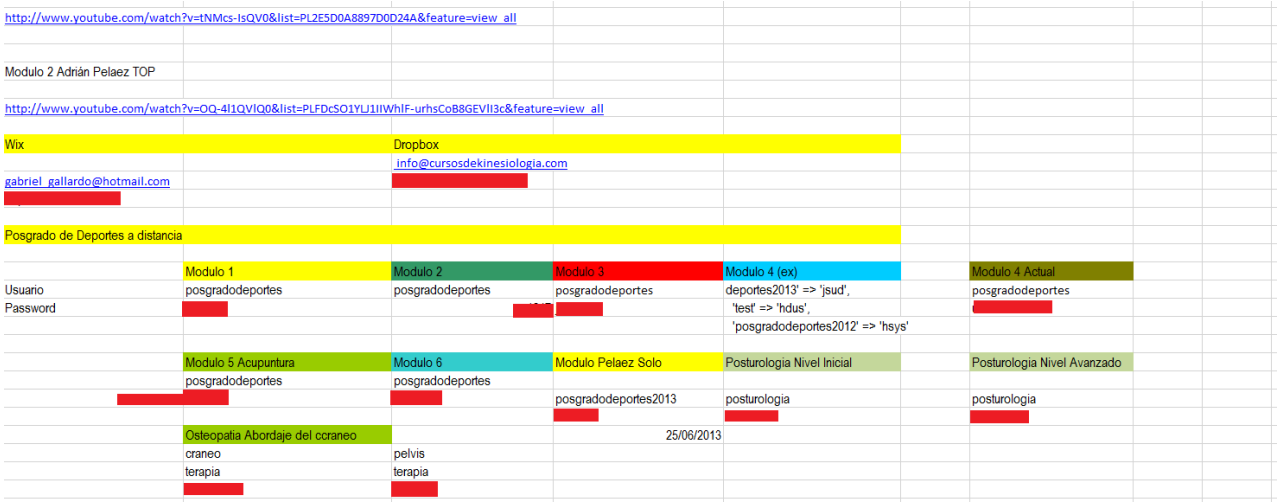
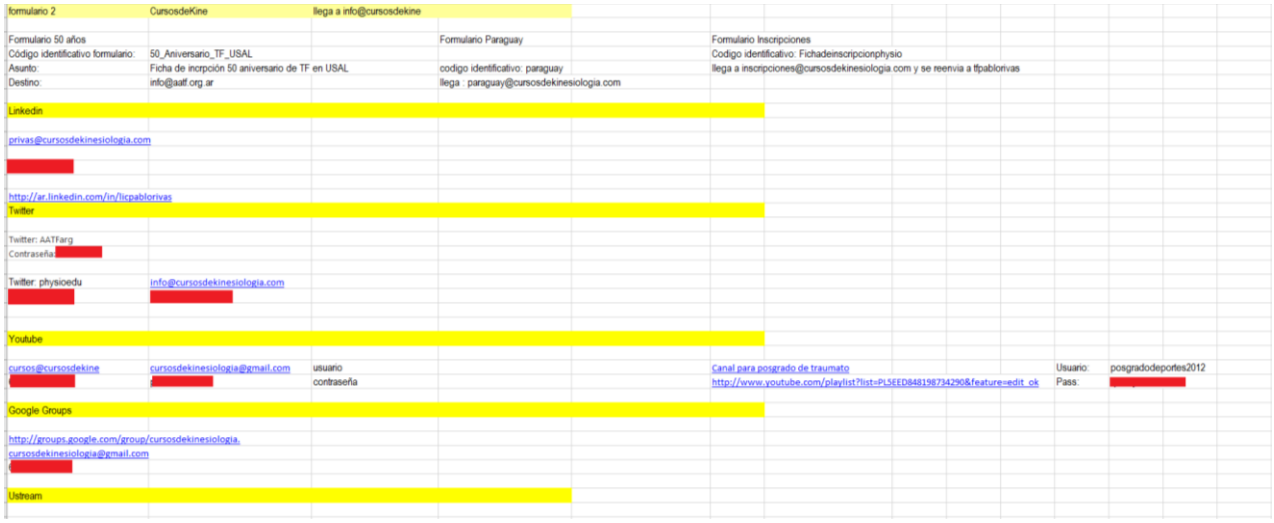


Figura 3-57 Ejemplo de cuentas extraídas por Google Dorks.

Se observa que entre las cuentas destaca el empleo de Dropbox, por lo que la opción de investigar al sujeto mediante el empleo de metadatos es factible. En cuanto a la Figura 3-58, se pueden apreciar las distintas plataformas utilizadas por el usuario teniendo acceso a todas ellas.



formulario 2	CursosdeKine	llega a info@cursosdekine			
Formulario 50 años			Formulario Paraguay	Formulario Inscripciones	
Código identificativo formulario:	50_Aniversario_TF_USAL			Codigo identificativo: Fichadeinscripcionphysio	
Asunto:	Ficha de incrpción 50 aniversario de TF en USAL		codigo identificativo: paraguay	llega a inscripciones@cursosdekinesiologia.com y se reenvia a tfpablorivas	
Destino:	info@aatf.org.ar		llega : paraguay@cursosdekinesiologia.com		
Linkedin					
privas@cursosdekinesiologia.com					
[redacted]					
http://ar.linkedin.com/in/licpablorivas					
Twitter					
Twitter: AATFarg					
Contraseña [redacted]					
Twitter: physioedu	info@cursosdekinesiologia.com				
[redacted]	[redacted]				
Youtube					
cursos@cursosdekine	cursosdekinesiologia@gmail.com	usuario		Canal para posgrado de traumato	Usuario: posgradodeportes2012
[redacted]	[redacted]	contraseña		http://www.youtube.com/playlist?list=PL5EED848198734290&feature=edit_ok	Pass: [redacted]
Google Groups					
http://groups.google.com/group/cursosdekinesiologia,					
cursosdekinesiologia@gmail.com					
[redacted]					
Ustream					

Figura 3-58 Ejemplo 2 de cuentas extraídas por Google Dorks.

Se puede pensar para qué se pueden usar estos perfiles, ya que los sujetos no son miembros de las Fuerzas Armadas. Sin embargo, dichos perfiles cuentan con unos años de servicio dentro de las distintas redes sociales. Además, también cuentan con seguidores (Figura 3-59) y ambas cosas pueden ser muy valiosas si se decidiera a usarse vector de ataque para acercarse a otras víctimas. Así, se ahorrará el paso de hacer un perfil creíble.

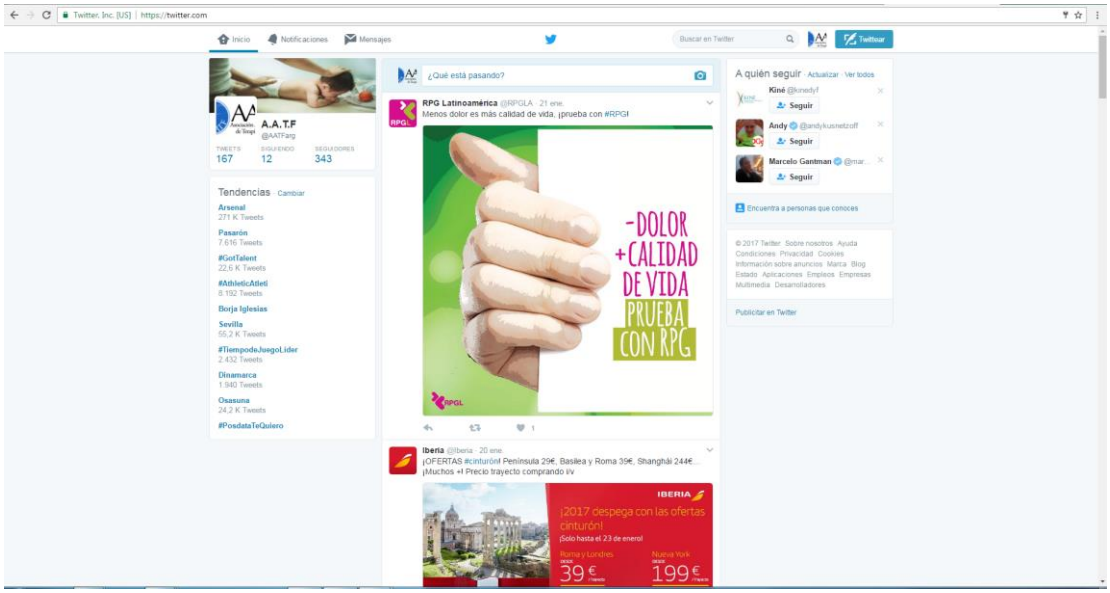


Figura 3-59 Inserción en cuenta de Twitter extraída por Google Dorks.

A modo de conclusión sobre Google Dorks, sirve como facilitador para hacer ataques. Además, también en Google Dorks se puede acceder a imágenes de seguridad de centros comerciales, comercios, viviendas, urbanizaciones e incluso acuartelamientos.

Dentro de la obtención de imágenes por parte de Google Dorks, destaca que es necesario que el servidor de imágenes donde se vuelca la información esté conectado a la red. Esto no pasa con los acuartelamientos militares españoles. En la Figura 3-60 las principales cámaras encontradas.

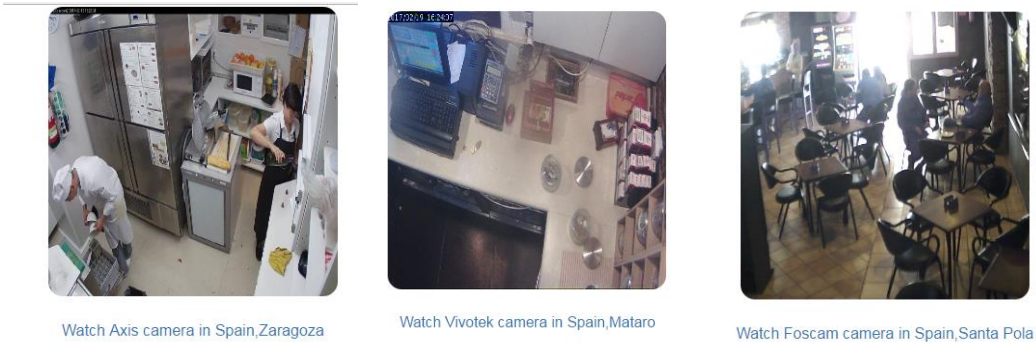


Figura 3-60 Imágenes extraídas por Google Dorks.

3.5 Ejemplo de ingeniería social y ciberataque

Durante este apartado se explica el ciberataque dirigido sobre un compañero.

En este caso, el ataque se efectúa dentro de la red de la Escuela Naval Militar. A continuación, se explican los pasos y de cómo se realiza y de cómo se realizaría si se tratase de uno de los sujetos anteriormente citados.

3.5.1 Creación de una necesidad en el sujeto

Durante este proceso, es necesario entrar dentro de la atmósfera de control del sujeto. Es decir, si queremos efectuar un ataque, no es tan fácil como llegar y decirle al sujeto que introduzca un *pendrive* o que ejecute un programa. Si se hace de esa forma el ataque está abocado al fracaso, ya que puede suscitar dudas o desconfianza en el sujeto.

Para el ejemplo efectuado, he elegido un compañero de la quinta brigada.

Para crear una necesidad puede ayudar conocer los gustos del sujeto. En los ejemplos anteriores, los sujetos a estudio exponían públicamente sus gustos, *hobbies*, deseos y demás.

Para ello, aprovechando la realización del TFG, se le propondrá a la víctima la instalación del nuevo Microsoft Word, motivación suficiente para que caiga en la trampa. A simple vista será un ejecutable, pero, a partir de este, comenzará el ciberataque dirigido sobre dicho sujeto.

3.5.2 Creación de un ciberataque dirigido

El método de ataque elegido es la creación de un *backdoor*, que nos permitiré el acceso a cualquier información que el sujeto tenga en su ordenador. Como curiosidad, la mayoría de los antivirus, detectan el troyano y no dejan abrir el archivo o directamente lo borran. en este caso, el antivirus del sujeto no ha sido capaz de detectarlo. Más adelante se explica cómo camuflarlo a través de un simple *binder*.

Para la creación del *backdoor*, se utiliza el sistema operativo Kali Linux. Sobre este, se ejecutan una serie de comandos que se describen a continuación.

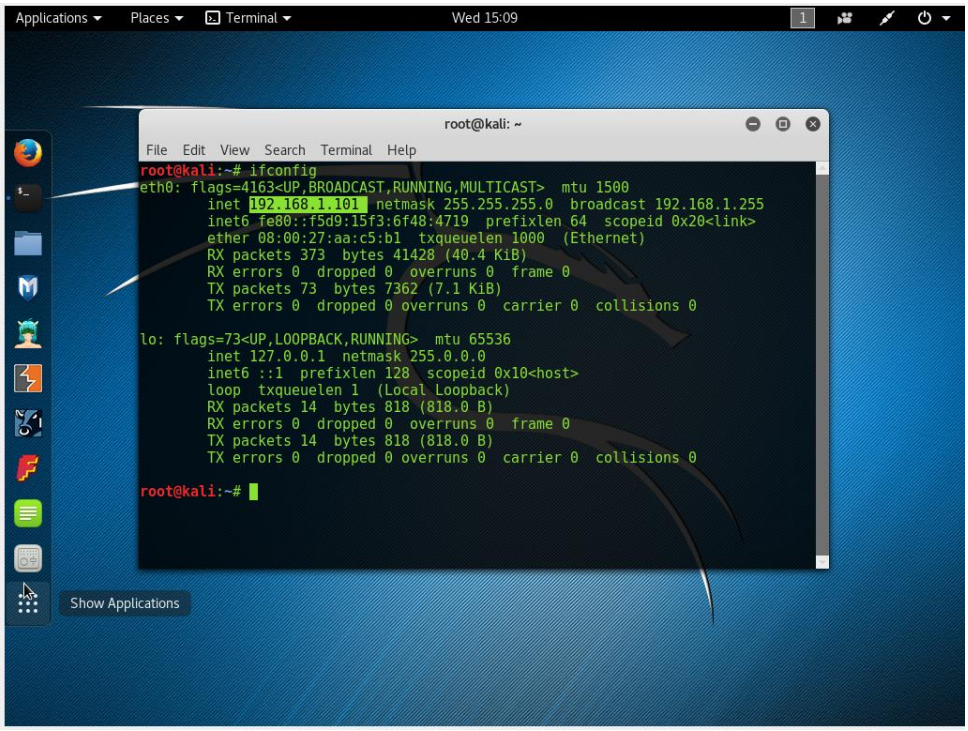


Figura 3-61 Obtención de la IP en Kali Linux.

A pesar de que Kali Linux es un sistema operativo muy versátil para estudiar la seguridad de una plataforma, lo único que se utiliza será el Metasploit Framework.

Por ahora, lo único que hacemos es obtener la dirección IP de la máquina con la finalidad de que la información sea vertida sobre dicha dirección (Figura 3-61).

Llegados a este punto, es necesario conocer los puertos que el sujeto atacado tiene disponibles. De esta forma, se destaca que una buena práctica a realizar por los usuarios es controlar los puertos que estos puedan estar abiertos.

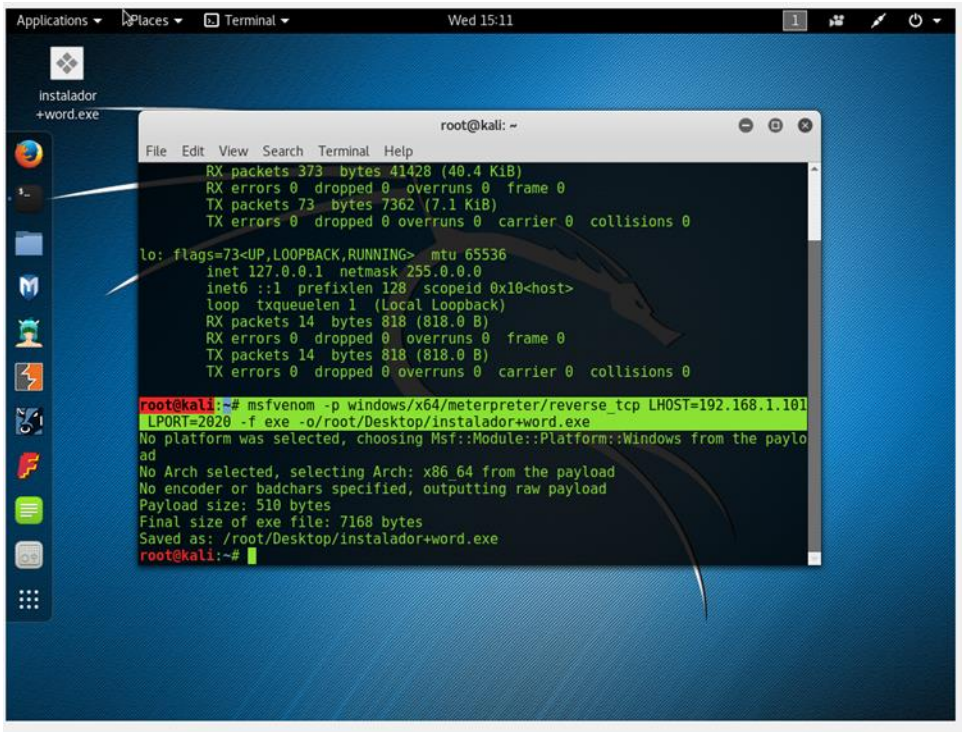


Figura 3-62 Uso de comandos en Kali Linux.

Como se puede ver (Figura 3-62), utilizamos la herramienta de *msfvenom* (herramienta dependiente de Metasploit Framework), para generar un *payload* en una plataforma Windows de 64 bits.

A continuación, se indica el tipo conexión entre la plataforma atacante y la atacada. De esta forma, se indica mediante LHOST, la dirección IP que recibe la información, el puerto y, tras esto, creamos el fichero ejecutable y su dirección física.

Otra opción, dentro de las múltiples que existen, es añadir un *encoder*, cuya función es camuflar el *payload*. De esta forma, la función del *encoder* es aumentar el grado de dificultad de poder localizarlo. Siempre que se quiera realizar un ataque de forma profesional es necesario que vaya acompañado de distintos *encoders*. Una vez que el antivirus analiza el archivo, su es nula, porque ya queda registrado en las bibliotecas de *malware*.

Para facilitar el ataque se llama al ejecutable "Instalador+ Word.exe". Es curioso que el Microsoft Word tenga una extensión .exe y con tan poco tamaño. En la Figura 3-63 se puede ver dicho ejecutable creado en el escritorio del sistema.

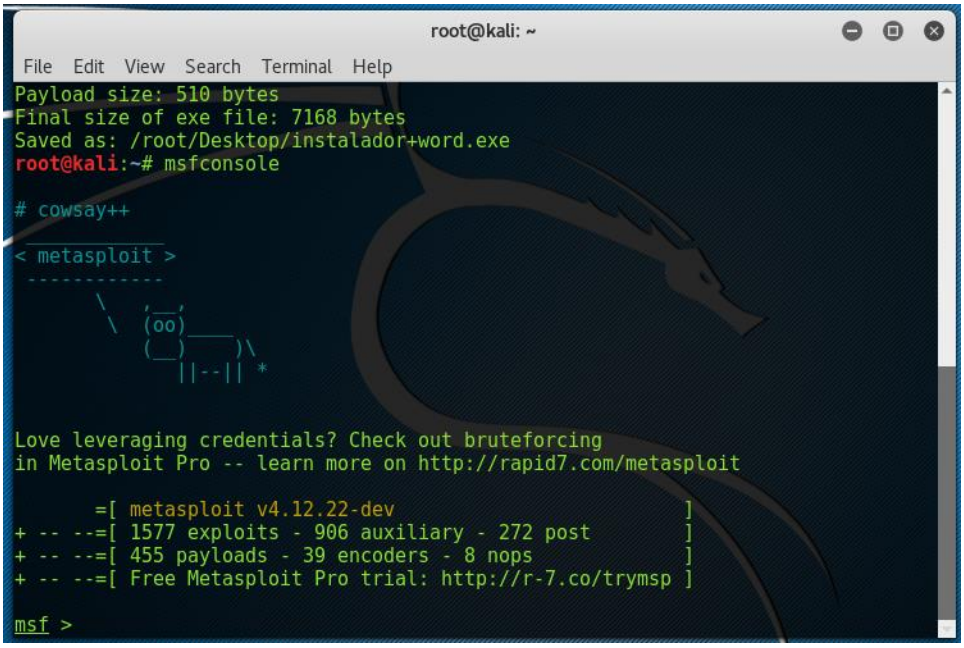


Figura 3-63 Apertura de *Metasploit* en Kali Linux.

Una vez generado el fichero, abrimos la herramienta Metasploit Framework, que ofrece una cantidad considerable de *payloads*, y *exploit*s.

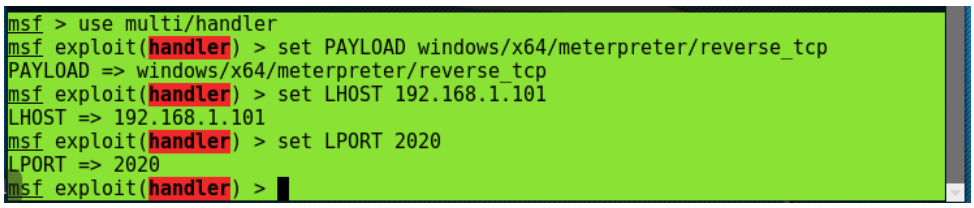


Figura 3-64 Uso de comandos dentro de *Metasploit*.

Dentro de Metasploit Framework utilizamos la herramienta *multi/handler*, que permite conectar con el *payload*. Dentro del mismo se establece el equipo local (LHOST) y su puerto (LPORT)como se ve en la Figura 3-64.

El siguiente paso es hacer el archivo accesible a la víctima. Para ello subirlo a una plataforma como Dropbox puede servir como buen punto de intercambio (Figura 3-65). Otra forma de transferirlo es mediante una memoria USB.

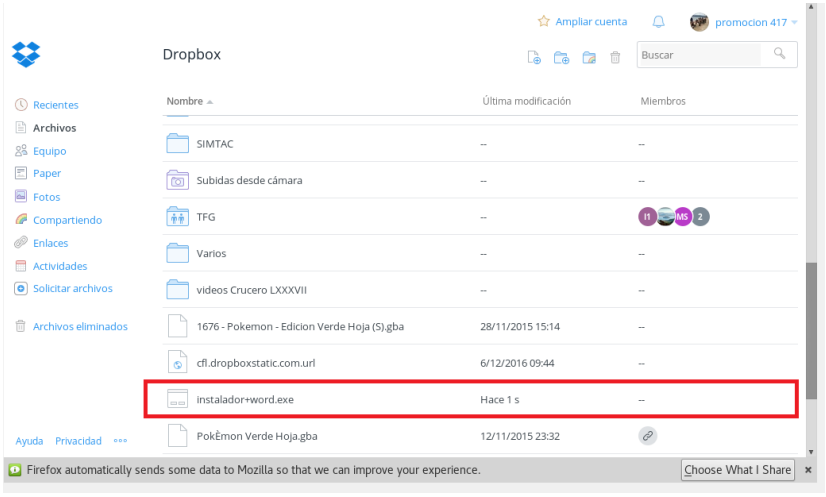


Figura 3-65 Archivo *malware* subido a Dropbox.

Ahora solo es necesario que la víctima descargue el archivo.

Tras descargarlo, solo queda esperar que su antivirus no detecte el *malware*. A continuación, en la Figura 3-66 se puede ver la eficacia del *malware*, baja, ya que es detectado por los principales antivirus.

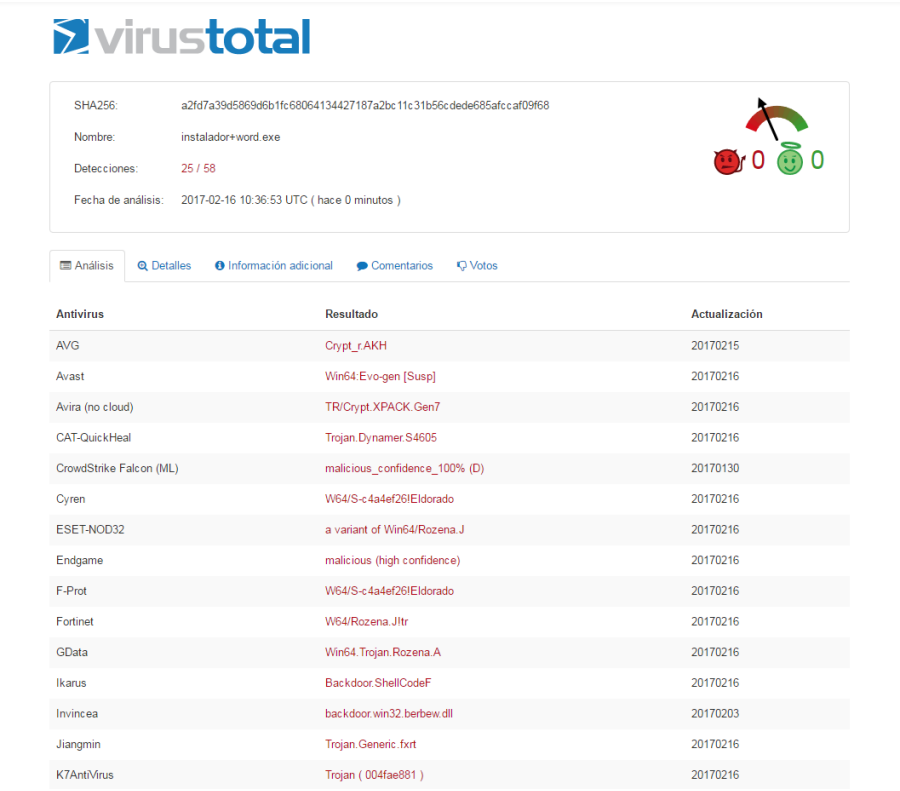


Figura 3-66 Captura de pantalla de Virustotal efectuado sobre archivo malware [77].

Solo tendremos que esperar a su ejecución, no sin antes haber ejecutado el *exploit* en el terminal de *Metasploit* (Figura 3-67).

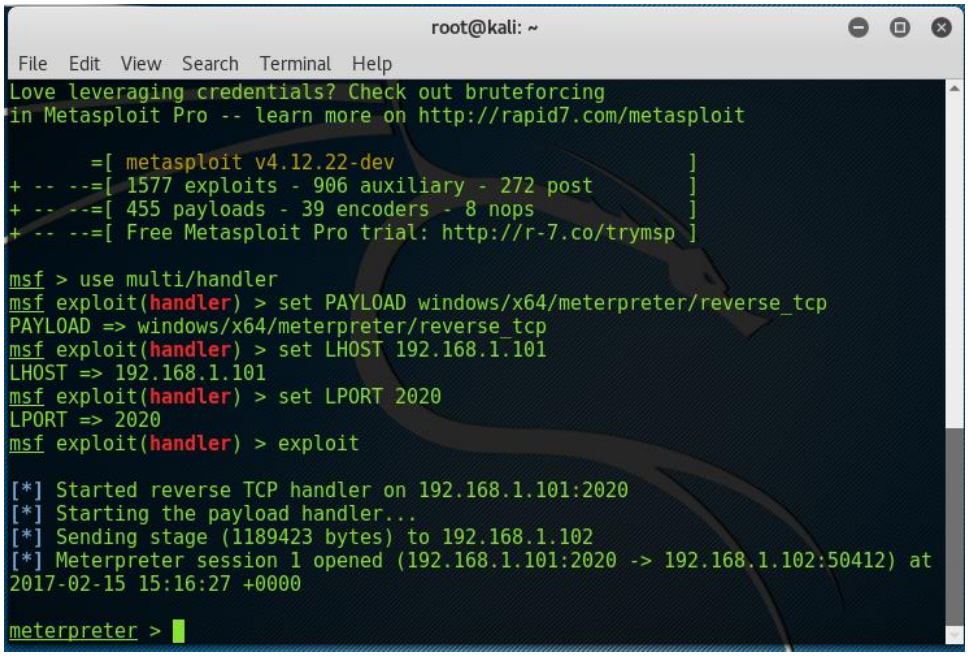


Figura 3-67 Apertura de *backdoor* en terminal.

Se puede apreciar que, tras ejecutar el *exploit*, la comunicación queda establecida.

Cabe destacar, que el archivo, puede ejecutarse en distintas plataformas al mismo tiempo, de forma que se encuentren distintas sesiones iniciadas a la vez, pudiendo ser esta alterada en cualquier momento.

Una vez ejecutado, la victima percibirá que no ha ocurrido nada tras la ejecución. Sin embargo, si accede al administrador de tareas, verá que se está ejecutando el archivo en segundo plano. De esta forma si para el proceso, el *backdoor* desaparece.

Como solución a ello, una vez abierta la conexión, se puede acceder a su administrador de tareas, y migrar el proceso a otro proceso necesario del sistema. Un ejemplo sería "explorer.exe".

El siguiente paso es ejecutar el comando killav. Dicho comando permite, terminar con cualquier proceso relacionado con sus antivirus.

Los pasos citados son recomendables siempre que se quiera realizar un *backdoor* de forma correcta.

Una vez ejecutado esto, desde el menú *meterpreter* (del *payload* que se encuentra en uso) podemos escalar privilegios de administrador.

En la Figura 3-68 se puede ver la plataforma víctima con el nombre de usuario. Se puede incluso conocer el tipo de plataforma usado. Esto es útil a la hora de preparar otro ataque sobre la víctima. Hay que destacar que el directorio variará en función de donde tenga guardado el archivo la víctima. En este caso, el lugar donde se encuentra albergado el archivo es el escritorio.

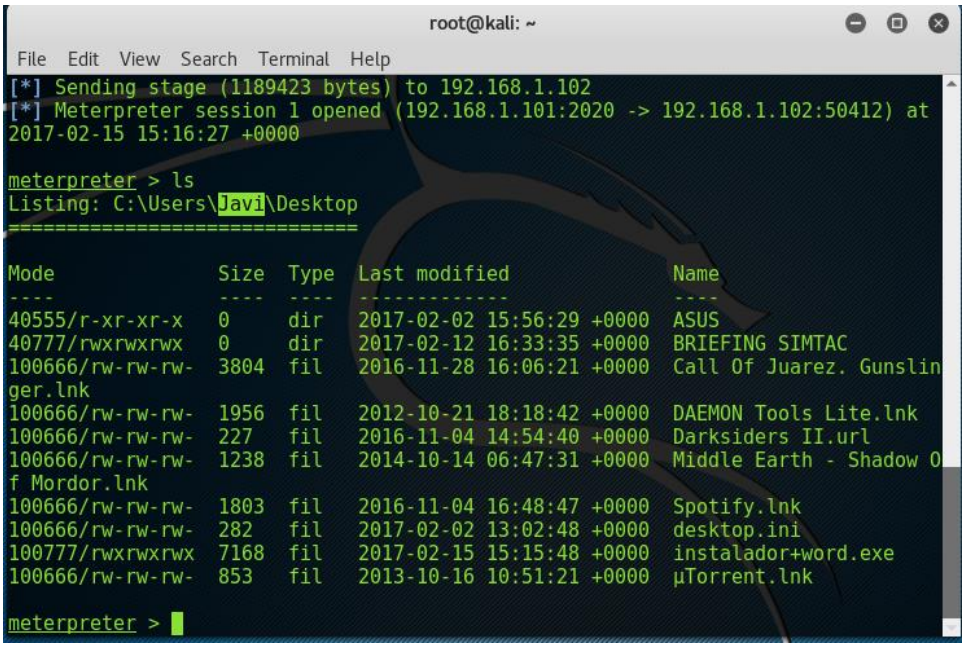


Figura 3-68 *Backdoor* en la máquina objetivo.

Dentro del escritorio, se puede ver la distinta información del usuario. Para navegar por las carpetas basta con los comandos básicos de Linux. Dentro del escritorio se pueden apreciar varios juegos, un montador y lector de imágenes, el ejecutable creado y un BRIEFING SIMTAC [56] (simulador táctico).

Como curiosidad, si el usuario atacado tratase de eliminar el ejecutable obtendría un error y la única forma de borrarlo sería como se ha explicado anteriormente.

El objetivo es obtener el máximo de información. En este caso, el usuario tiene información que puede resultar provechosa.

Es momento de pensar qué puede ocurrir si se realiza este tipo de ataque sobre un miembro de las FAS, desplegado en zona de operaciones donde la información manejada a diario puede causar graves trastornos en el personal.

Si un terrorista accediese a información de las patrullas españolas en dicha zona podría planear un ataque sobre las unidades. Para ello solo es necesario que el usuario atacado esté manejando información sensible en un ordenado no destinado para ello.

Nos centramos en ver la posible información que pueda contener el *briefing* (Figura 3-69).

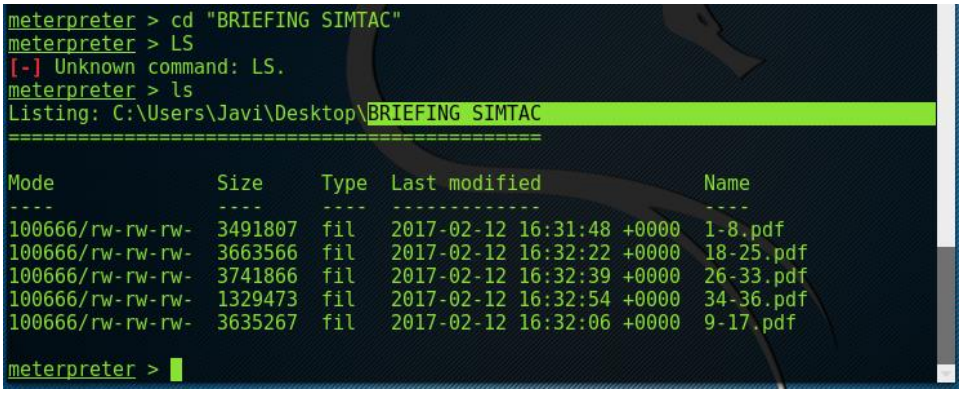


Figura 3-69 Accediendo a carpetas del ordenador del objetivo.

[56] Exposición de una operación en el simulador táctico, en la mayoría de ocasiones, va acompañado de información confidencial.

Una vez dentro de la carpeta BRIEFING SIMTAC, podemos acceder a la información que se encuentra dentro de ella. En este caso, descargamos la carpeta entera con uno de los comandos disponibles (Figura 3-70).

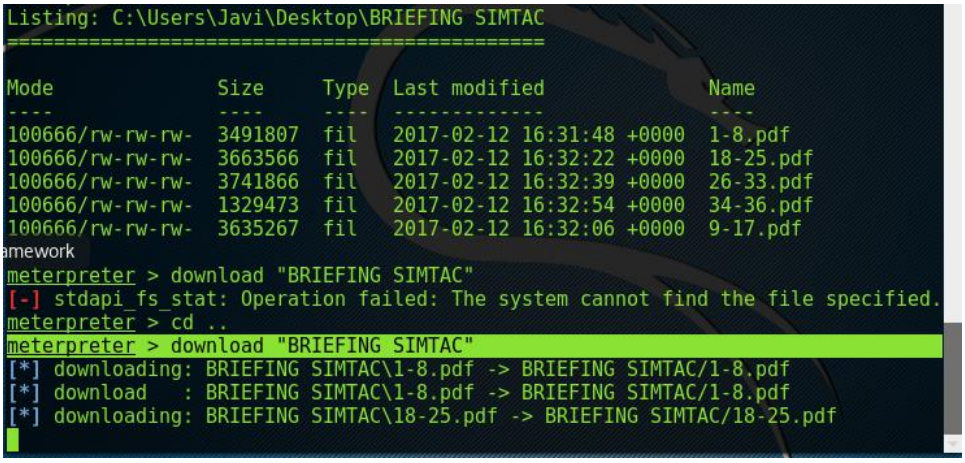


Figura 3-70 Descarga de archivos del ordenador objetivo.

Como se puede ver, mediante el comando *download*, se puede descargar todos los archivos que se encuentran dentro de la carpeta (Figura 3-71). Encontrada la carpeta, se procede a ver los documentos descargados.

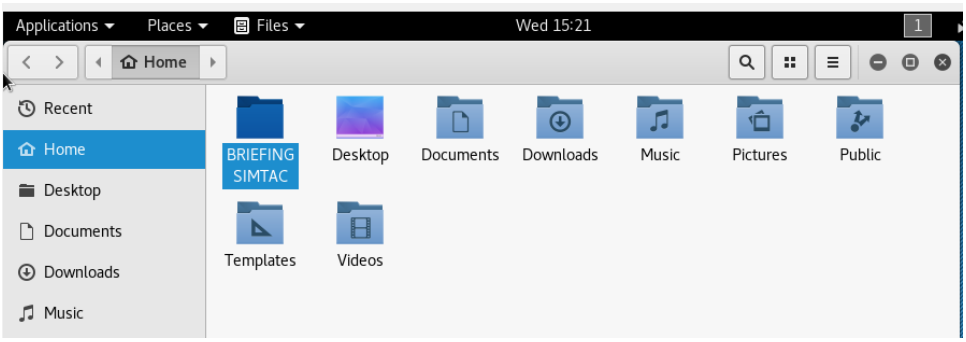


Figura 3-71 Muestra de la carpeta descargada en nuestro sistema.

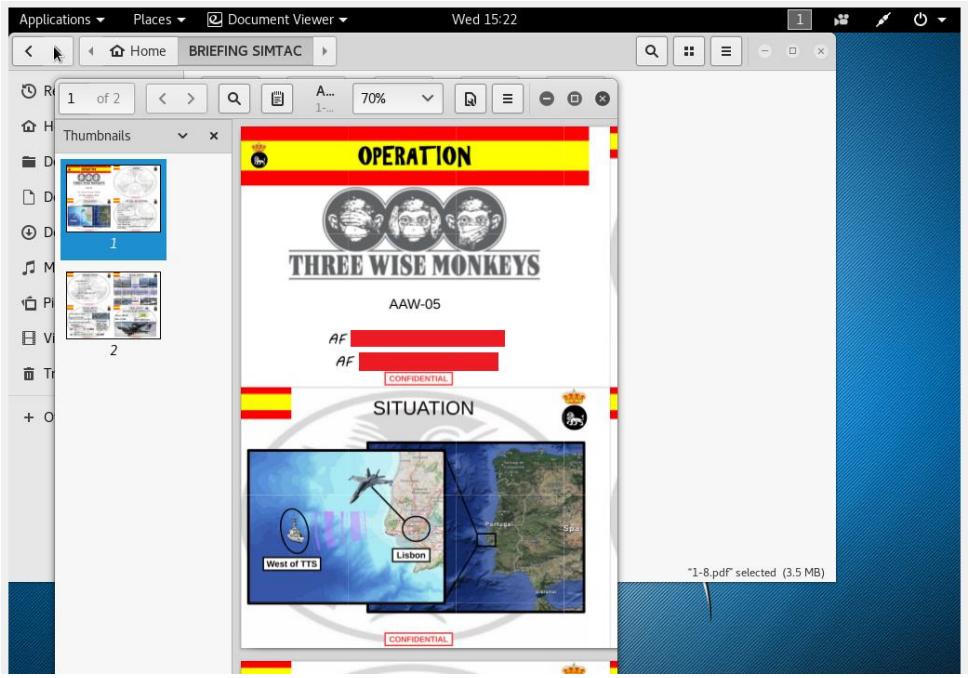


Figura 3-72 Captura de los documentos confidenciales descargados.

Como se puede ver en la Figura 3-72, se trata de una exposición de las operaciones a desarrollar. El carácter de dicho documento es confidencial. en otra ocasión podría haber sido una publicación o similar, de forma que la repercusión podría haber sido mucho mayor.

Otra de las acciones que se puede llevar a cabo entre las muchas existentes, podría ser acceder a sus contraseñas almacenadas, iniciar un *keylogger* con el que almacenaríamos todo lo tecleado por la víctima, así como acceder a su micrófono, su cámara en vivo o sus documentos eliminados (*trashing*).

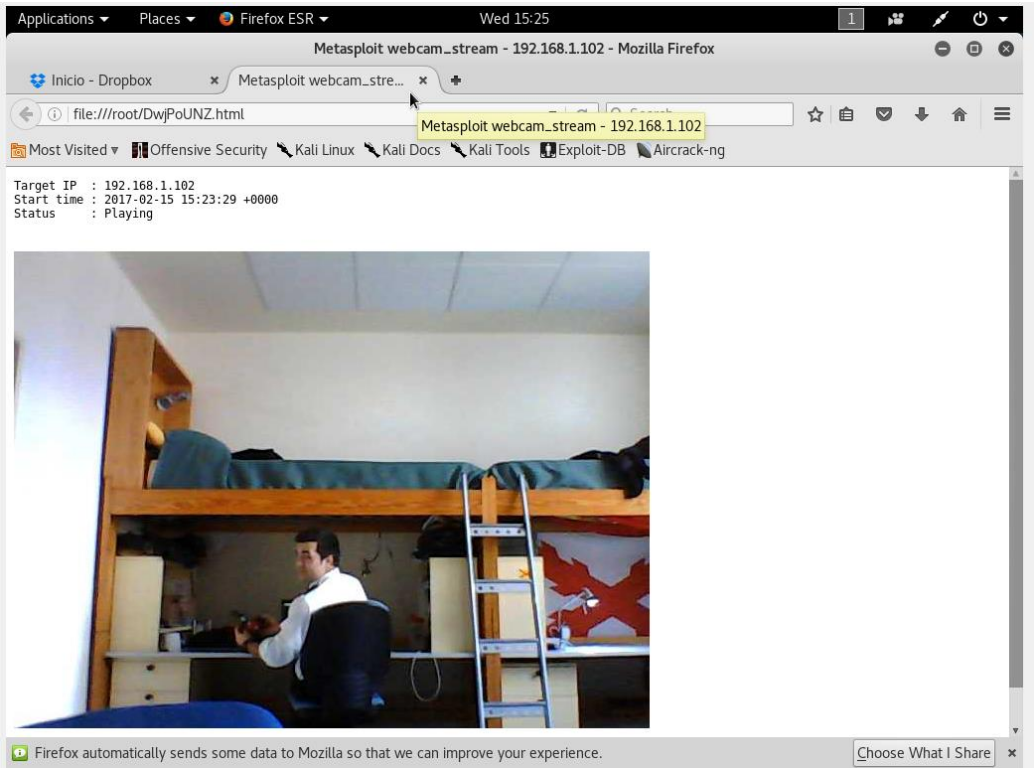


Figura 3-73 Captura de la webcam objetivo.

Si se puede acceder a la cámara (Figura 3-73), existiría la opción de tomar fotografías del mismo, incluso obtener material con el que se le pueda hacer chantaje a la víctima, así como hacer uso del micrófono para acceder a información privada. Otra opción distinta pero útil es la de modificar o crear archivos de texto, carpetas y opciones similares en el equipo de la víctima.

También se pueden realizar capturas de pantalla del escritorio de la víctima (Figura 3-74). Se observa que la víctima no ha eliminado el ejecutable creado y también la carpeta con la información que ha sido descargada.

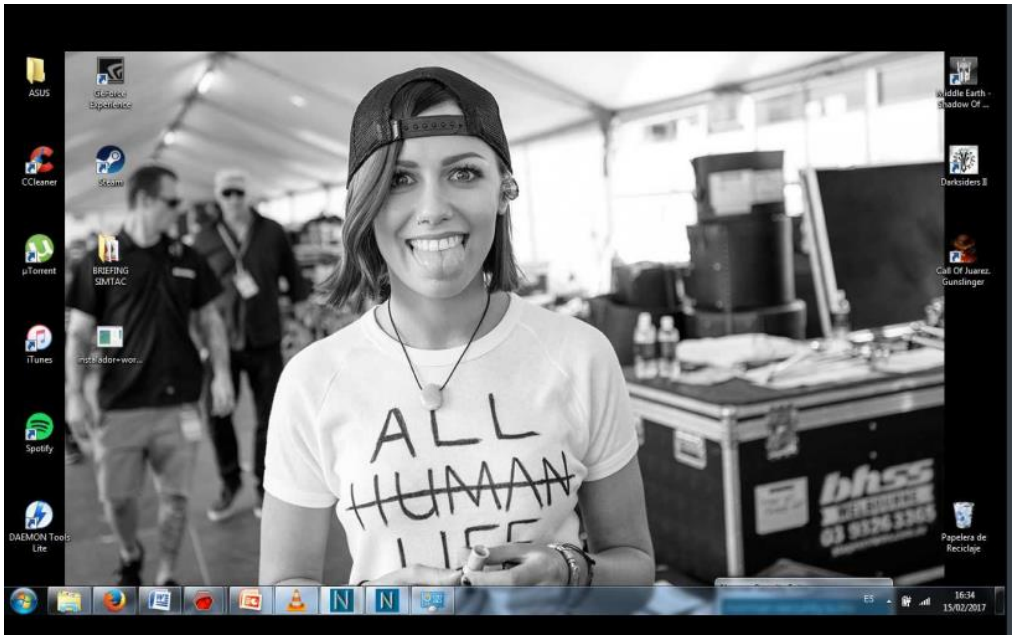


Figura 3-74 Captura del escritorio víctima.

También se puede crear y modificar carpetas (Figura 3-75). Esto puede ser útil si se quisiera atribuir algún tipo de delito a la víctima. Al igual que se puede descargar archivos de la máquina víctima, también se puede importar archivos a la máquina de la víctima.

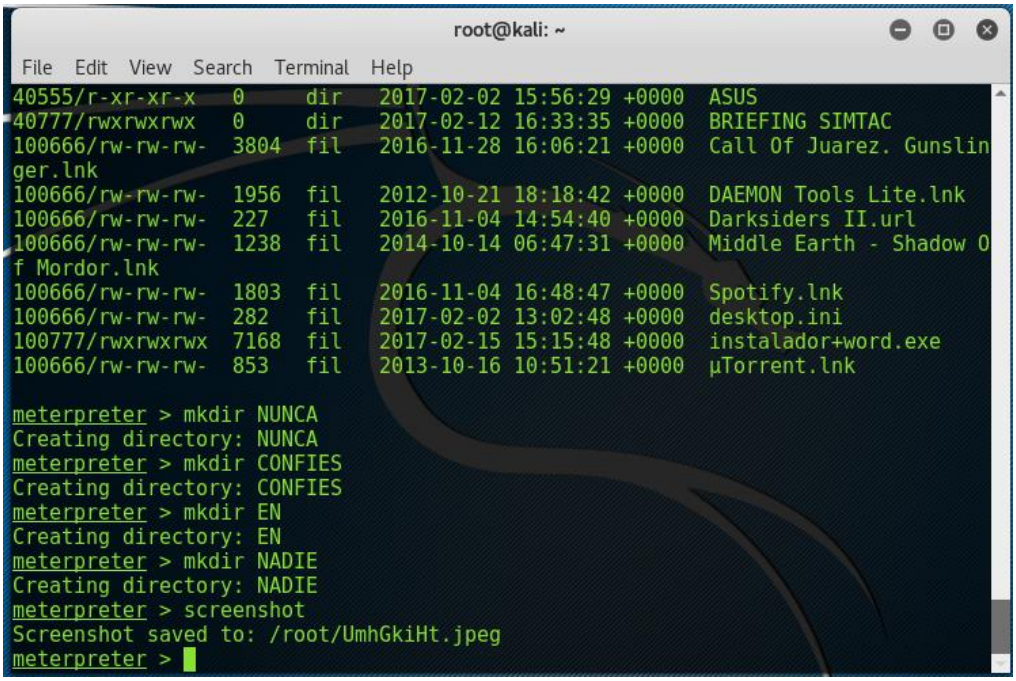


Figura 3-75 Creando carpetas en el escritorio víctima.

En este caso se crean una serie de carpetas con la intención de saber si la plataforma objetivo se da cuenta de que está sufriendo una intromisión dentro de su sistema (Figura 3-76).

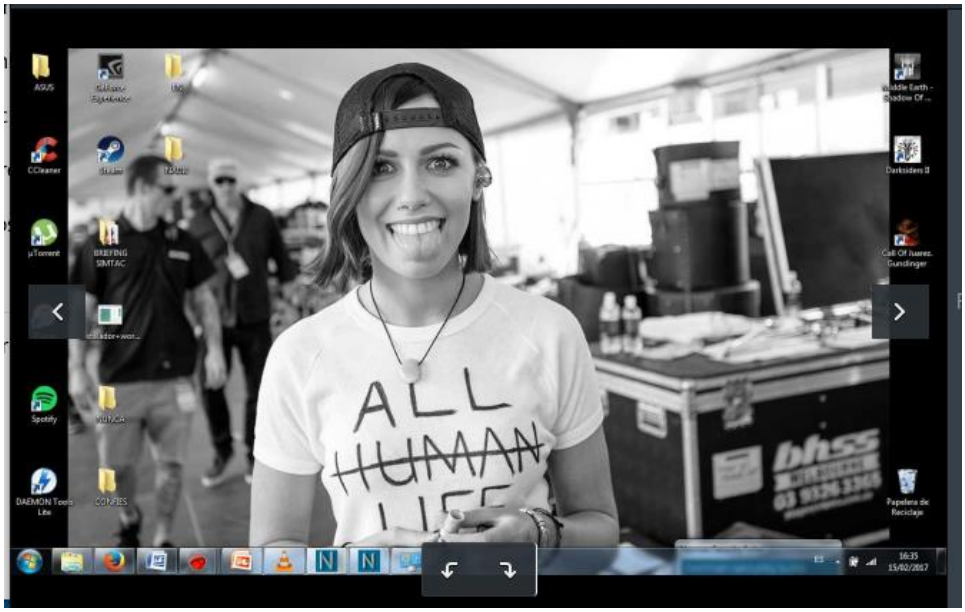


Figura 3-76 Resultado de la creación de carpetas en el escritorio objetivo.

Así finaliza el ejemplo de cómo acceder a una plataforma del sujeto en cuestión. En comparación con los sujetos vistos anteriormente, las pegas que se podrán encontrar durante la realización del proceso son las siguientes:

- Disponibilidad de puertos: este ejemplo se llevó a cabo mediante la utilización del puerto 80. Sin embargo, no se pudo completar con normalidad mediante la utilización de este puerto.
- Que a la ejecución del archivo el antivirus haga saltar una alerta y bloquee o elimine el archivo.

Como solución a estos problemas, se vio que o bien se cambiaba la técnica de realización del mismo, con aplicaciones como TheFatRat que correrá sobre Linux, o mediante la utilización de las macros de las hojas de un archivo Excel.

Otra solución más sencilla, es la utilización de un *binder* (Figura 3-77).

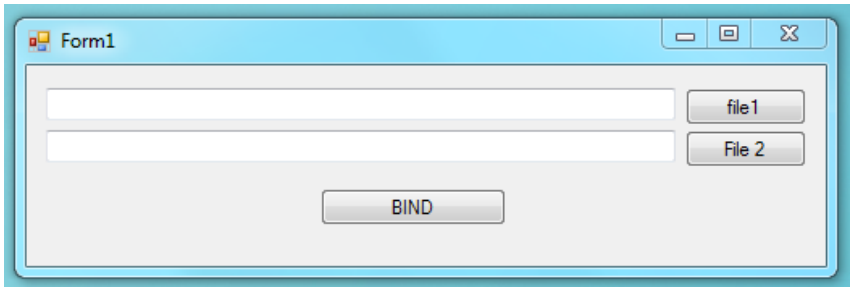


Figura 3-77 *Binder* utilizado.

La particularidad del *binder* utilizado es que hay que introducir por un lado el ejecutable deseado y por otro lado un archivo con PDF.

Para este ataque, es necesario crear otro tipo de necesidad en la víctima. Es decir, ya no se puede engañar a la víctima con el ejecutable de un supuesto programa.

Para la realización de este proceso, se eligió el nombre *examen robado* (atractivo para alumno). El nombre debe variar en función del público destinado.

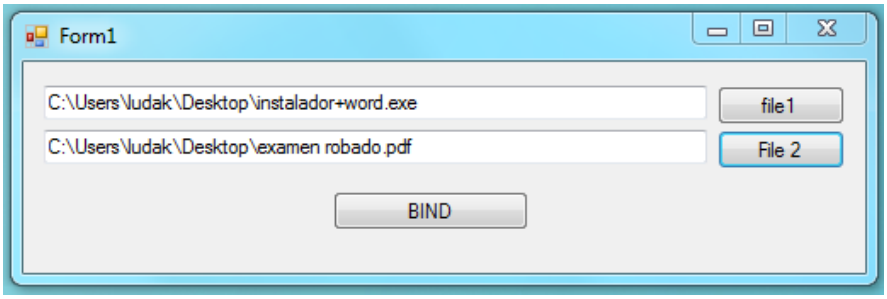


Figura 3-78 Realizando *binder* en archivos.

En la Figura 3-78 se puede visualizar el proceso de creación del ejecutable.

Comprobamos cuántos antivirus detectan este método introduciéndolo de nuevo en la página https://www.virustotal.com/es .

Como se puede apreciar, este método es más detectable que el anterior. Se debe a la utilización del *binder*, ya que se detecta un archivo dentro de otro archivo y son los propios antivirus los que califican esta acción como potencialmente peligrosa.

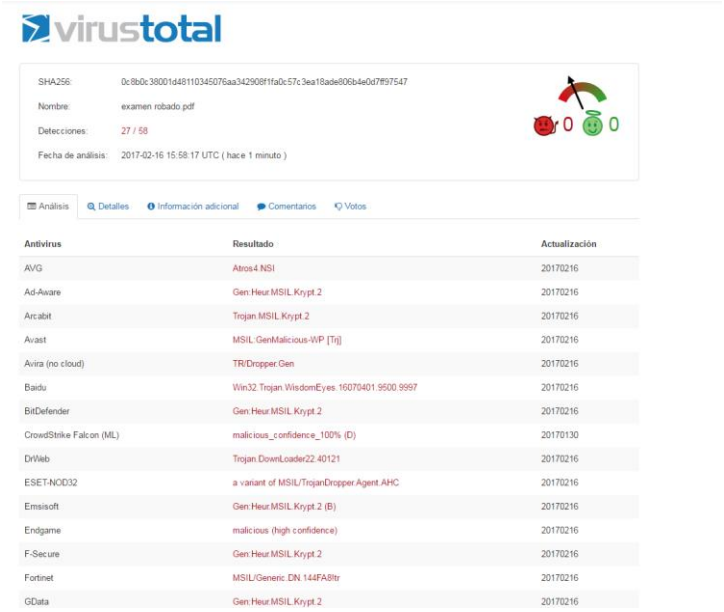


Figura 3-79 Resultado de virus total sobre nuevo archivo [77].

4 INTERPRETACIÓN DE LOS RESULTADOS

4.1 Justificación del proceso seguido

Durante el proceso de obtención de información se ha visto que son diversas las formas a través de las cuales puede obtener diversa información y también se han podido apreciar los distintos grados de configuración de privacidad que los distintos usuarios realizan en las redes sociales. Desde un sujeto que carece de información o red social hasta aquellos de los que se puede obtener domicilio, teléfono, familiares y demás información de interés.

El elemento clave para obtener información es la obtención de una cuenta de correo, aunque podría ser en otros ejemplos la obtención de un teléfono móvil, correspondencia privada o toda aquella información que abra la puerta a más información.

A día de hoy se hace prácticamente imposible que el personal de las Fuerzas Armadas no se pueda llegar a encontrar expuesto. Aun así, el personal de las FAS tiene dentro de sus posibilidades la privacidad y seguridad que se puedan dar dentro de las redes sociales, y pueden dar a aquellos a quien les rodea.

Llegados a este punto es necesario puntualizar que toda información se contrasta varias veces resulta más fructífera y verídica que aquella que solo venga de una fuente.

Durante la exploración con la herramienta Maltego no se esperaba que el volumen de información de los sujetos adyacentes fuera tanto. De esta forma se pasa de tener un único sujeto de estudio a 29. Así, en el caso de querer llevar a cabo cualquier tipo de acción sobre un sujeto de las FAS, las posibilidades que se otorgan son mucho mayores, pudiendo elegir entre los distintos sujetos para poder efectuar el ataque. Esto haría que el estudio se diversificase y fuese un conjunto de personal perteneciente a las FAS. Con esto se conseguiría uno de los objetivos de este trabajo, demostrar la cantidad de información asequible a través de las distintas fuentes abiertas. En este sentido, se observó que el personal de Fuerzas Armadas se encuentra interrelacionado, lo que facilita que a partir de un único sujeto se pueda obtener más información del personal adyacente al mismo.

En cuanto a la exploración en redes sociales, destaca que, en la actualidad, pueden representar el método más fiable a la hora de encontrar un sujeto. Durante el desarrollo del estudio, se advirtió de los distintos tipos de protección en los distintos perfiles de redes sociales. Por dicho motivo, se muestra la Tabla 4-1, de forma que se utilizará a la hora de estudiar los distintos estándares OTAN para valoraciones TESSCO.

Otro de los elementos a destacar es la facilidad con la que el personal accede a ser una víctima de un ataque de ingeniería social. Es decir, el personal de las FAS carece de cualquier tipo de defensa ante

la ingeniería social. Además, estos facilitan dichos posibles ataques mediante el vertido de información susceptible.

El ejemplo del *backdoor* es el ejemplo más claro de cómo la falta de experiencia en un tema puede llegar a comprometer al individuo e incluso a las FAS. También se puede ver esta vulnerabilidad cuando, en una de las múltiples ocasiones que se fue la luz, el personal que se encontraba dentro del acuartelamiento accedía a una red que desconocían, que no tenían guardada y que únicamente compartí el nombre con la original.

A la gran cantidad de información que se encuentra accesible en la red y con las distintas herramientas OSINT se le une la falta de concienciación que tiene el personal de las FAS. Es importante destacar que la gran mayoría de los sujetos son objetivos potenciales de sufrir un ataque. en nuestro caso, se estudiará sujeto a sujeto basándonos en la posibilidad del sujeto a que pueda ser objetivo de terrorismo, espionaje, subversión, sabotaje y crimen organizado y al que se ha añadido como objeto de estudio la presunción de que pueda sufrir un ciberataque.

4.2 Grados de protección en redes sociales

Para la ayuda al posterior análisis se ha desarrollado unas categorías de grado de protección en redes sociales (Tabla 4-1).

Grado 1	**El sujeto no tiene redes sociales.**
Grado 2	El sujeto solo tiene foto de perfil, y no deja ver información, fotos, amigos, etc.
Grado 3	El sujeto presenta foto de perfil, amigos, pero no información personal.
Grado 4	El sujeto presenta foto de perfil, información, acceso a amigos, pero no permite interacción.
Grado 5	Sujeto con perfil libre y que permite interacción.

Tabla 4-1 Grados de protección en redes sociales.

4.3 Análisis según los estándares OTAN para las valoraciones TESSCO

4.3.1 Sujeto inicial

Durante la exploración del sujeto inicial se vio la vulnerabilidad apreciable en todo el personal de las Fuerzas Armadas. Esta vulnerabilidad consiste en que los miembros de las Fuerzas Armadas, al menos los explorados durante este trabajo, quedan reflejados como tal, de esta forma es el sistema con las distintas publicaciones del BOE el que comienza vulnerando la privacidad del personal de las FAS. Otra vulnerabilidad advertida es la interconexión de un ordenador de la red de Defensa con un ordenador que se encuentra fuera de la misma.

Este sujeto presenta un grado 3 en lo que a protección en redes sociales se refiere. Carece de cualquier tipo de seguridad en dar su nombre y a apellidos, favoreciendo así su búsqueda y etiquetación. También se aprecia que es posible acceder al nombre de usuario de SKYPE, que coincide con su usuario de MINISDEF.

La Tabla 4-2 muestra su valoración TESSCO.

	Alta	Media	Baja
Terrorismo		X	
Espionaje		X	
Sabotaje			X
Subversión			X
Crimen organizado		X	
Víctima de ciberataque		X	

Tabla 4-2 Sujeto inicial.

Fundamentos: El presente sujeto presenta una valoración terrorista media debido a su posible empleo y el posible destino que pueda presentar. Dicho concepto va unido con la capacidad de espionaje que se pueda hacer del mismo. En este punto, la información del mismo son nombre y apellidos, DNI y coche con matrícula y modelo. Esto hace que la valoración de espionaje sea media. En cuanto al sabotaje, el puesto que desempeña el sujeto debido al destino que se le presupondría tras el espionaje no sería un objetivo que corra el riesgo de ser saboteado. Del mismo modo ocurre con la subversión. El sujeto presenta una vulnerabilidad en cuanto a crimen organizado se refiere y, debido a la falta de conocimientos y concienciación por parte del mismo, presenta una valoración media a la hora de poder ser víctima de ciberataque. En este caso se desecha que la víctima pueda ser valorada de forma alta debido a que usa la red de Defensa.

4.3.2 Sujeto 1

La forma de llegar a dicho sujeto fue mediante la exploración del sujeto anterior. Presenta las mismas vulnerabilidades en lo que a la publicación de nombre, apellidos y DNI en el BOE se refiere.

Sin embargo, este sujeto interacciona más con las distintas redes sociales, calificando su grado de protección como grado 4.

Entre la distinta información que le hace ser un sujeto vulnerable se advierte, el nombre y apellidos, DNI, cuerpo, especialidad, empleo, rasgos faciales, *hobbies*, usuarios de otras redes sociales, e incluso ideología política. Todo ello favorece según TESSCO a situar a dicho sujeto como un sujeto potencialmente vulnerable (Tabla 4-3).

	Alta	Media	Baja
Terrorismo	X	X	
Espionaje	X		
Sabotaje		X	
Subversión		X	
Crimen organizado		X	
Víctima de ciberataque		X	

Tabla 4-3 Sujeto 1.

Fundamentos: El sujeto 1 presenta una valoración media-alta en lo que a terrorismo se refiere. Esto se debe al puesto que desempeña y la facilidad en territorio nacional con la que se lo puede encontrar.

La valoración en espionaje produce que dicho sujeto tras hallar el lugar donde los pilotos de la Armada tienen su base, ayudado de distintas fotografías e información del mismo, eleve la valoración del mismo a un grado alto.

Además, el desempeño de las funciones de piloto en la armada facilita el uso de información confidencial, lo que hace que mediante un ciberataque dirigido se pueda acceder a información confidencial y facilite a una valoración media el grado de sabotaje que pueda sufrir dicho sujeto. Las fotografías pueden llegar a utilizarse en su contra por parte de cualquier otro usuario, así como medio de comunicación actual o propaganda antimilitarista. Esto hace que la valoración de subversión adquiera un grado medio, así como la de crimen organizado, debido a la escasa protección que dicho sujeto se da en las redes sociales.

En cuanto a la valoración en lo que a un ciberataque se refiere, se desconocen las habilidades informáticas del mismo. Se presupone que, por la facilidad del mismo por subir distinto material no apto a la red y su interacción en las distintas redes sociales, puede llegar a ser víctima de un ciberataque con una valoración media.

4.3.3 Sujeto 2

La forma de llegar a dicho sujeto fue mediante la exploración del sujeto anterior y presenta las mismas vulnerabilidades.

En cuanto al grado de protección, se trata de un grado 3 de protección. Sin embargo, es con su foto de perfil y la de portada únicamente con la que se saca mucha más información que de sujetos anteriores.

En cuanto a la exploración mediante las distintas herramientas OSINT, destaca la obtención del nombre y apellidos, correo electrónico, redes sociales, especialidad, empleo, rasgos faciales y demás. En cuanto a la valoración TESSCO (Tabla 4-4) presenta distintos grados debido a que se encuentra menos accesible a través de redes sociales.

	Alta	Media	Baja
Terrorismo		X	X
Espionaje	X		
Sabotaje	X		
Subversión		X	
Crimen organizado		X	X
Víctima de ciberataque		X	

Tabla 4-4 Sujeto 2.

Fundamentos: El sujeto 2 presenta una valoración media baja en lo que a terrorismo se refiere. Se debe a su empleo. Sin embargo, es importante resaltar que, entre las distintas fotos asequibles a través de redes sociales, destaca la Figura 3-26. Se trata de una imagen con calificación de seguridad a nivel nacional como secreto. Dicha imagen es el tablero de la aviónica de un helicóptero. Además de estar penado por el código disciplinario de las Fuerzas Armadas, dicha clasificación puede poner en riesgo los intereses de España como nación, así como los intereses de las Fuerzas Armadas. Por este motivo, el grado de espionaje y sabotaje es una valoración alta.

En cuanto a la subversión es necesario puntualizar que sería la imagen y el correo facilitado el motivo por el que adquiere un grado medio de valoración. Sin embargo, como se ha mencionado antes,

el empleo es un factor condicionante a la hora de ser o no una posible víctima. En este caso, se le otorga un grado medio bajo a la valoración para el crimen organizado.

La facilidad con la que el usuario proporciona su correo a través de la red y siendo uno de los factores más importantes a la hora de realizar un ciberataque le otorga una valoración media.

4.3.4 Sujeto 3

La forma de llegar a dicho sujeto ha sido mediante la exploración del sujeto anterior.

En cuanto al grado de protección se trata de un grado 4, ya que vierte una cantidad de información relevante, como su familia, en la que se destaca mujer e hija.

Este sujeto presenta su vulnerabilidad a través de la familia. Otra vulnerabilidad que presenta es que indica cuando se encuentra fuera de casa realizando una misión, hecho que aumenta su valoración TESSCO.

De esta forma, a través de redes sociales y herramientas OSINT, es posible sacar nombre, apellidos, DNI, información familiar, empleo y destino del mismo (Tabla 4-5).

	Alta	Media	Baja
Terrorismo		X	
Espionaje		X	
Sabotaje	X	X	
Subversión		X	
Crimen organizado		X	
Víctima de ciberataque			X

Tabla 4-5 Sujeto 3.

Fundamentos: El sujeto 3 presenta una valoración media en lo que a terrorismo refiere. Se debe a la clase de comentarios e interacción que el sujeto publica en redes sociales y que, al tratarse del pasado, no suponen una valoración alta en la actualidad. Sin embargo, es necesario puntualizar que dicha clase de comentarios pueden comprometer la unidad, ya que, en la mayoría de los casos, esa clase de información en un buque de guerra no suele compartirse con tanta facilidad.

Este comportamiento puede facilitar el espionaje de una unidad, pudiendo llegar a obtener los patrones de movimiento de la misma a través de una simple red social y, con ello, sabotear las distintas unidades que se vean comprometidas.

Dicha valoración sobre los factores anteriormente citados produce que se le otorgue una valoración media de subversión y, que debido a los datos familiares a través de las redes sociales, es una posible víctima del crimen organizado. En cuanto a que el sujeto sea víctima de un ciberataque se le presupone una valoración baja.

4.3.5 Sujetos adyacentes

Aunque no se puede tratar como un único sujeto ya que la información corresponde a más de un sujeto, se continúa realizando las valoraciones TESSCO (Tabla 4-6) oportunas.

Destaco durante la exploración del resto de perfiles que el grado de protección en redes sociales suele estar estandarizado en grado 3, si bien se han encontrado varios perfiles de grado 5, y varios perfiles de grado 1.

	Alta	Media	Baja
Terrorismo		Suele centrase en media, aunque existan ejemplos de personal, cuya valoración debería ser superior	
Espionaje	Dirección de la vivienda obtenida en fuentes abiertas		
Sabotaje	Familiares	Amigos	
Subversión		Media de los sujetos	
Crimen organizado		Media de los sujetos	
Víctima de ciberataque		Observado personal que comunica el tipo de plataforma que usa	Principalmente no observado

Tabla 4-6 Distintos sujetos vistos.

Fundamentos: Los distintos sujetos identificados del entorno del sujeto inicial suelen encontrarse situados en una valoración media en lo que a TESSCO se refiere, aunque se ha visto el caso de un ex comandante de un buque de la Armada cuya valoración de terrorismo debería ser superior por ser comandante de una unidad y de que la dirección de la vivienda del mismo se encuentre subida a la red junto con una foto de la familia. Esto hace que la valoración de espionaje sea superior a la media, así como la de posible sabotaje de la unidad a través de los familiares de este. En cuanto a subversión y crimen organizado, la valoración se encuentra centrada en media, ya que son los empleos los que juegan un papel en contra. Es decir, a mayor nivel de empleo, más posibilidad existe de que aumente el grado en estos. Entre la valoración de estos de sufrir un ciberataque, se encuentra no observada, salvo en aquellos cuyas plataformas que se obtienen a través de Twitter, o cuyos comentarios en plataformas de compra en línea presuponen el uso de un terminal. En estos casos la valoración es media.

4.3.6 Sujeto 69

El modo de acceder a dicho sujeto es mediante el análisis de la red a través de la herramienta OSINT de Maltego.

En principio, un controlador de una red no tiene por qué aparecer reseñado en la red, e incluso puede que el nombre que a parezca no sea real. Como resultado del mismo, no es necesario que aparezca como uno de los dos controladores de la red.

En cuanto a las redes sociales, presenta un grado 3 de protección en Facebook.

En LinkedIn el grado de protección es 5 ya que cualquiera puede ver su currículum e interactuar con él (Tabla 4-7).

Cabe destacar que la información vertida en LinkedIn, corrobora que se trata de un Teniente Coronel de Ingenieros, encargado del nodo INET[57] y de las comunicaciones del Ministerio de Defensa. Se sabe por Facebook que tiene familia y la ciudad donde vive.

	Alta	Media	Baja
Terrorismo	X		
Espionaje	X		
Sabotaje	X		
Subversión		X	
Crimen organizado		X	
Víctima de ciberataque	X		

Tabla 4-7 Sujeto 69.

Fundamentos: El sujeto 69 presenta una valoración alta en lo que a terrorismo se refiere. Se debe a que el sujeto es una parte fundamental en las comunicaciones del Ministerio de Defensa. Cualquier acto sobre dicho sujeto puede causar graves consecuencias tanto en el sujeto como en la defensa de España como nación.

Este sujeto presenta también una valoración alta en espionaje, ya que como dice en su propio perfil trabaja como coordinador del nodo INET. Esto puede causar que si se accediese a los permisos que este tiene pudiese causar graves problemas de espionaje y dejaría al sistema expuesto.

Unido al factor anterior, hace que la valoración de sabotaje sobre el mismo sea elevada. Todo ello es debido al volumen de información que el sujeto puede manejar o haya manejado, de forma que se le pueda sabotear mediante la familia o similares, dejando de nuevo expuesto al sistema.

Presenta una valoración media en subversión, destacando que cualquier filtrado de información de dicho sujeto puede hacer que las comunicaciones de Defensa corran peligro. Igual ocurre con el crimen organizado. Sin embargo, no es un sujeto que se presente como vulnerable en dichos valores.

En cuanto al valor de ciberataque, es de carácter alto, ya que cualquier ciberataque, hasta el más sencillo que anule las capacidades de dicho nodo, puede anular las comunicaciones del Ministerio de Defensa.

4.4 Justificación del malware

Durante el desarrollo práctico de la memoria, se observó que la mejor forma de llegar al objetivo mediante un ciberataque era la utilización de un malware. En este caso, de todas las posibilidades se eligió un *backdoor*.

Su funcionamiento está basado en el modo caballo de Troya. Es decir, se envía un archivo con apariencia legítima pero que a su vez me facilita realizar un ataque sobre el objetivo.

Durante la realización del mismo se puede ver que son múltiples los modos de actuación de estos. Esto quiere decir que un mismo *backdoor*, puede realizarse de diversas formas y puede tener diferentes funciones.

[57] Instituto Nacional de Educación Tecnológica.

En este caso se trató de omitir las memorias USB, que solo aumentan el grado de dificultad y son más fáciles de detectar. Esto se debe a que muchos de los antivirus modernos vuelcan sus esfuerzos en el análisis de memorias extraíbles.

Por este motivo y la facilidad de uso se eligió la red. Así, el archivo infectado fue puesto en común a través de Dropbox. Se eligió esta plataforma debido a que la mayoría de los correos actuales utilizan antivirus dentro de la aplicación.

Para la realización del ataque también se llevó a cabo un mapeo de los puertos de la red a utilizar. Esto es esencial a la hora de efectuar un ataque, ya que es necesario saber qué puertos se encuentran abiertos.

Llegados a este punto, cobra especial importancia la información adquirida a través de fuentes abiertas.

Una vez creado el archivo ejecutable, se eligieron los *payloads* y *exploits*, por ser los más eficaces. También se eligió la comunicación reversa, ya que al ser un ataque en tiempo real era la que más convenía al proceso.

La justificación del mismo en su elección es para que permita camuflar el archivo en tiempo real, haciendo mudar el proceso dentro de otro proceso o incluso acabar con el antivirus de la plataforma enemiga.

A modo de conclusión, estas son las principales razones por las cuales se defiende el *backdoor* como ciberataque dirigido hacia un miembro de las FAS: rapidez, versatilidad, eficacia y capacidad de que se pueda hacer el archivo indetectable.

4.5 Análisis del personal de las FAS en redes sociales

Durante el presente trabajo, se observó que el personal de las FAS analizado, carece en la mayoría de los casos de seguridad óptima en sus diversos perfiles. Es importante destacar que el personal de las FAS, por su condición de militar debe tomar precauciones a la hora de subir material a la red.

Además, durante el presente análisis se vio que no existe ninguna clase de filtro a la hora de volcar información a las redes sociales. Así, en la mayoría de los casos el material es asequible para la mayoría de usuarios.

Se observó también que durante la realización del estudio las redes sociales de los integrantes de las FAS dependen de su empleo y se encuentran en la mayoría de los casos relacionadas con la edad de los integrantes.

La Tabla 4-8 muestra las principales redes sociales utilizadas dentro de las FAS.

	Edad	**Facebook**	**Instagram**	**Twitter**	**LinkedIn**	**Grupo**
Alumnos, tropa y marinería	18-30	X	X		-	1
Oficiales y suboficiales	30-45	X	X	-	-	2
Comandantes y Suboficiales antiguos	45-59	-		X	X	3
Oficiales generales	60 en adelante			-	-	4

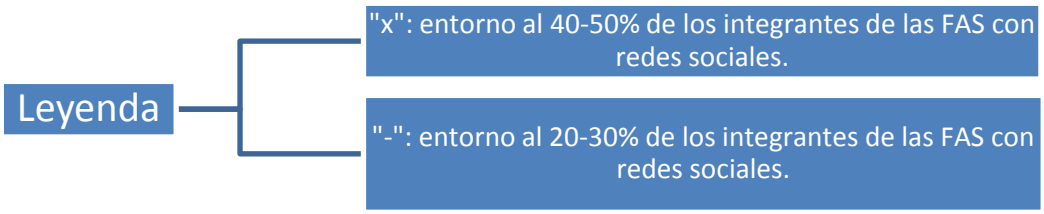


Tabla 4-8 Análisis de las redes sociales en las FAS.

Fundamentos: Como reflexión general, destacar que las redes sociales se encuentran presentes en las FAS. Son las nuevas generaciones las que más uso le dan. El tipo de uso suele ser para subir fotografías y realizar comentarios. Durante el estudio puedo verificar la enorme cantidad de fotografías que no pasan ningún tipo de filtro disponibles en las redes sociales. Como curiosidad, destaca de este primer grupo que casi en su totalidad se identificaran como militares y que los comentarios públicos del sistema o de lo relacionado con el sistema es bastante común. Esto ocurre tanto en Instagram como en Facebook. Resalta curioso destacar el uso de la red social LinkedIn cuya finalidad es la búsqueda de trabajo y contactar con profesionales del sector.

En cuanto a los integrantes del grupo 2 interactúan principalmente mediante Facebook en el ámbito familiar y amistades. Es en el grupo 2 donde se asienta la red social LinkedIn. Tiene en este grupo menor uso la red social Instagram, aunque tiene adeptos igual que Twitter.

Los integrantes del grupo 3 se alejan del uso de la red social Facebook aunque existan integrantes en ella. El uso de las redes sociales se encuentra en Twitter pero, sobre todo, en LinkedIn (con más afinidad que en Facebook).

Por último, los integrantes del grupo 4 siguen los mismos patrones que los anteriores, pero con menor participación que el resto del personal de las FAS.

5 CONCLUSIONES Y LÍNEAS FUTURAS

5.1 Conclusiones generales

El presente trabajo se ha realizado tomado como muestra el personal de FAS como institución nunca como individuo, empleándose exclusivamente la información vertida en la red por los mismos de carácter completamente pública y a la que podría tener acceso cualquier usuario.

A lo largo del mismo, se ha podido constatar la gran cantidad de información vertida en el ciberespacio por personal perteneciente a las FAS. Con ello se ha podido descubrir que la mayor parte de la misma se la puede catalogar como "personal". Debidamente empleada, puede servir de base para la realización de ataques que podrían tener un doble objetivo: la institución y la persona.

Por otro lado, es muy complicado modificar las configuraciones y los protocolos asociados a las redes sociales. Es por ello, por lo que el principal objetivo de este trabajo es el de concienciar y sensibilizar a los componentes de las FAS de la gran vulnerabilidad que representa para ellos mismos y sus familias divulgar de manera descontrolada informaciones asociadas a la persona.

Sorpresivamente, también se ha descubierto en la elaboración de este trabajo que es el propio Estado, a través de cualquiera de sus boletines (BOE, BOD), el primero que "etiqueta" a parte del personal perteneciente a FAS, allanando el trabajo preliminar para todo aquel que quisiera atacar a la institución o sus componentes.

A modo de resumen, a continuación, se exponen una serie de medidas que, tras la elaboración de este trabajo, se considera interesante hacerlas llegar a todos los componentes de FAS:

- Desconfiar de cualquier usuario de la red, siendo esta la principal máxima a la que debe ceñirse el personal de las FAS. Esta medida es necesaria, ya que se desconoce el individuo que se puede encontrar tras un usuario cibernético.
- Aumentar el grado de privacidad y seguridad personal en las distintas redes sociales. Mentalizar en el empleo de alias, nombre falsos o abreviaturas
- Reducir la interacción en la red. Lo deseable es que la misma quedase reducida a nombre y apellidos, a ser posible falsos. Por ejemplo: comentarios en páginas de compras en línea, páginas de eventos, etc. De esta forma se dificultaría notablemente la obtención de los perfiles personales del personal de FAS.
- Desconfiar de perfiles no conocidos y que traten de interactuar con el personal de las FAS.
- Desconfiar de cualquier medio de interacción que haga dar más datos de los necesarios ya que, por norma general, se desconoce el lugar donde se van a almacenar o el fin de los mismos.

- Leer los términos y políticas de privacidad de las aplicaciones (redes sociales, correos, etc.) utilizadas en las distintas plataformas.
- Desconfiar de aplicaciones o programas cuyo origen sea desconocido, aunque sean recomendados por un allegado.
- Restringir el uso de las redes sociales al personal de las FAS, realizando una auditoria sobre los perfiles del personal integrante de las FAS. Dicha restricción podría llegar a ser prohibición, si de zona de operaciones se tratase.
- Restringir el uso de redes sociales a partir de ciertos empleos, o en personal que ocupe determinados puestos/destinos.
- Evitar el uso de páginas destinadas a confeccionar una "bolsa de trabajo" teniendo en cuenta del gran volumen de datos que se han de dar.
- Prohibir el uso de empleos militares y destinos en cualquier fuente abierta.
- Endurecer las medidas disciplinarias asociadas al mal uso de las redes sociales, llegándose las mismas a contemplarse de manera explícita en el actual "Régimen disciplinario de las Fuerzas Armadas".
- Prohibirse, de manera general y conjunta, el uso de páginas como LinkedIn o similares. Dicha plataforma tiene como objeto la búsqueda de empleo o la creación de bolsas de trabajo. De todos es conocido que el personal en situación de activo en FAS está sujeto a la Ley de Incompatibilidades.
- Prohibir la "existencia" en la red de determinadas personas de las FAS en virtud de su cargo, grado militar o destino.

Todas estas medidas podrían reducirse en una: ***Reducir de manera drástica el volumen de información que los miembros de las FAS divulgan, de manera consciente o inconsciente, en la red.***

5.2 Líneas futuras

Como líneas de actuación futura se destacan las que siguientes:

- Creación de herramientas que permitan controlar la cantidad de información que el personal de las FAS vierte a las redes sociales. Lo ideal es que la misma pudiera identificar quiénes son los usuarios y analizar el tipo de información con el objeto de buscar soluciones.
- Desarrollar unos patrones o perfiles de conducta que permitan conocer cuál es el tipo de "persona" que vierte más información en la red, así como el tipo de la misma. Conocer qué es lo que le lleva a esta persona al mal empleo de la red.
- Elaborar un documento marco que sirva para realizar futuras auditorias en cada uno de los Ejércitos, marcándose en el mismo la dirección estratégica a seguir.
- Elaborar, de manera conjunta, programas destinados a la mentalización y concienciación del personal de FAS sobre las consecuencias del mal uso de la red.

6 BIBLIOGRAFÍA

[1] P. F. Iglesias, «pabloyglesias» [En línea]. Disponible: https://www.pabloyglesias.com/mundohacker-ingenieria-social/. [Último acceso: 24 enero 2017].

[2] A. Ramos Varón, Hacking con Ingeniería Social Técnicas para hackear humanos, Madrid: Ra-Ma, 2015.

[3] K. Mitnick, Interviewee, *Ingeniería Social.* [Entrevista]. 27 mayo 2005.

[4] Instituto Nacional de Ciberseguridad (INCIBE); Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), «Oficina de Seguridad del Internauta» [En línea]. Disponible: https://www.osi.es/es/actualidad/blog/2015/02/13/moviles-y-fotos-intimas-que-nos-arriesgamos. [Último acceso: 27 enero 2017].

[5] Laboratorio Hispasec, «Hispasec» 18 febrero 2013. [En línea]. Disponible: http://unaaldia.hispasec.com/2013/02/el-66-de-los-phishings-se-cuelgan-en.html. [Último acceso: 27 enero 2017].

[6] R. Moya, «elhacker,» [En línea]. Disponible: http://blog.elhacker.net/2014/01/phishing-en-2014-ejemplo-practico-facebook.html. [Último acceso: 21 enero 2017].

[7] Agencia EFE, «El Mundo» [En línea]. Disponible: http://www.elmundo.es/espana/2016/03/12/56e3f990ca47414f2c8b4666.html. [Último acceso: 25 enero 2017].

[8] S. d. l. Santos, «Hispasec» 22 marzo 2013. [En línea]. Disponible: http://unaaldia.hispasec.com/2013/03/historia-del-malware-en-cajeros_22.html. [Último acceso: 27 enero 2017].

[9] B. Quintero, «HISPASEC» 27 enero 2002. [En línea]. Disponible: http://unaaldia.hispasec.com/2002/01/gusano-producto-de-ingenieria-social.html. [Último acceso: 28 enero 2017].

[10] S. d. l. Santos, «Hispasec» 11 enero 2012. [En línea]. Disponible: http://unaaldia.hispasec.com/2012/01/curiosidades-sobre-el-pharming-i.html. [Último acceso:

26 enero 2017].

[11] A. Ropero, «Hispasec» 19 marzo 2016. [En línea]. Disponible: http://unaaldia.hispasec.com/2016/03/nuevo-malware-para-ios-puede-infectar.html. [Último acceso: 27 enero 2017].

[12] CERTSI, «CERTSI» 7 diciembre 2016. [En línea]. Disponible: https://www.certsi.es/alerta-temprana/avisos-sci/puertas-traseras-camaras-ip-ipela-engine-sony. [Último acceso: 25 enero 2017].

[13] anónimo, «Hack players» [En línea]. Disponible: http://www.hackplayers.com/2012/10/social-engineering-toolkit-set.html. [Último acceso: 22 enero 2017].

[14] A. Lamouroux, «Segu.Info» [En línea]. Disponible: http://blog.segu-info.com.ar/2015/10/manual-de-la-pina-wifi-wifi-pineapple.html. [Último acceso: 22 enero 2017].

[15] NATO, APP-6, Publicaciones OTAN, 2006.

[16] M. d. A. y. Doctrina, Manual de Inteligencia Táctica, Granada: MADOC-ET.

[17] TheGuardian, «The Guardian» 6 julio 2016. [En línea]. Disponible: http://www.eldiario.es/theguardian/invasion-Irak-desvela-informe-Chilcot_0_534396996.html. [Último acceso: 29 enero 2017].

[18] E.P.M, *Mando Conjunto de Ciberdefensa*, Madrid, 2017.

[19] F. E. Matamala, «Sistemas de ciberinteligencia» de *Obtención en el ciberespacio*, Madrid, 2015.

[20] I. Perez, «We live security» 19 febrero 2014. [En línea]. Disponible: http://www.welivesecurity.com/la-es/2014/02/19/maltego-herramienta-muestra-tan-expuesto-estas-internet/. [Último acceso: 11 diciembre 2016].

[21] Paterva, «Maltego,» Paterva CE, 2016.

[22] Eleven Paths, «Eleven Paths» 22 mayo 2015. [En línea]. Disponible: https://www.elevenpaths.com/es/labstools/foca-2/index.html. [Último acceso: 12 diciembre 2016].

[23] C. Alonso, «El lado del mal» 5 agosto 2010. [En línea]. Disponible: http://www.elladodelmal.com/2010/08/hacking-foca-1-de-3.html. [Último acceso: 12 diciembre 2016].

[24] Congreso de los diputados, «Agencia Estatal Boletín Oficial del Estado» 5 julio 2011. [En línea]. Disponible: http://www.boe.es/buscar/doc.php?id=BOE-A-2011-11605. [Último acceso: 22 enero 2017].

[25] E. A, «Open we binairs» 27 julio 2015. [En línea]. Disponible: https://openwebinars.net/blog/hacking-tutorial-busquedas-con-google-dorks/. [Último acceso: 19 enero 2017].

[26] C. Alonso, «El lado del Mal» 30 abril 2010. [En línea]. Disponible: http://www.elladodelmal.com/2011/04/creepy-data.html. [Último acceso: 21 enero 2017].

[27] I. Perez, «We live security» 8 abril 2015. [En línea]. Disponible:

http://www.welivesecurity.com/la-es/2015/04/08/the-harvester-riesgo-nformacion-publica/. [Último acceso: 11 enero 2017].

[28] RIPE, «RIPE.NET» [En línea]. Disponible: https://www.ripe.net/. [Último acceso: 4 diciembre 2016].

[29] J. Ramos, «Rootear» 16 abril 2014. [En línea]. Disponible: https://rootear.com/seguridad/shodan. [Último acceso: 29 enero 2017].

[30] M. Bazzell, «Intel Techniques Search Tool» 2009. [En línea]. Disponible: https://inteltechniques.com/menu.html. [Último acceso: 29 enero 2017].

[31] J. Nordine, «Osint Framework» [En línea]. Disponible: http://osintframework.com/. [Último acceso: 29 diciembre 2016].

[32] Asociación de academias de la lengua española, «Real Academia Española» [En línea]. Disponible: http://dle.rae.es/?id=VXs6SD8. [Último acceso: 24 enero 2017].

[33] CERTSI (CERT de Seguridad e Industria), «CERTSI» [En línea]. Disponible: https://www.certsi.es/blog/frente-abierto-entre-las-redes-sociales-y-los-ciberdelincuentes. [Último acceso: 25 enero 2017].

[34] Infobae, «Infobae América» 29 marzo 2014. [En línea]. Disponible: http://www.infobae.com/2014/03/29/1553717-estos-son-los-paises-que-bloquean-facebook-twitter-y-youtube/. [Último acceso: 16 enero 2017].

[35] El profe Morales, «El profe Morales» 18 agosto 2015. [En línea]. Disponible: http://www.profemorales.com/?p=16993. [Último acceso: 18 agosto 2017].

[36] Mesa Editorial Merca2.0, «Merca2.0» 31 julio 2015. [En línea]. Disponible: http://www.merca20.com/cual-es-la-edad-que-predomina-en-las-principales-redes-sociales/. [Último acceso: 26 enero 2017].

[37] Portal TIC, «20 Minutos» 28 mayo 2013. [En línea]. Disponible: http://www.20minutos.es/noticia/1858474/0/filtracion-facebook/mas-grave/brecha-seguridad/. [Último acceso: 26 enero 2017].

[38] Redacción de El Mundo, «El Mundo» 11 julio 2016. [En línea]. Disponible: http://www.elmundo.com/portal/vida/tecnologia/amigos_y_familiares_son_ahora__la_prioridad_en_facebook.php#.WI4QX1PhCUk. [Último acceso: 26 enero 2017].

[39] C. D. v. Eitzen, «Blog de Christian» 14 julio 2013. [En línea]. Disponible: http://www.christiandve.com/2013/07/atencion-que-redes-sociales-borran-los-datos-personales-de-mis-fotos-cuando-las-publico/. [Último acceso: 25 enero 2017].

[40] S. Barrera, «TECNOXPLORA» 22 marzo 2016. [En línea]. Disponible: http://www.tecnoxplora.com/internet/ciudad-con-ley/que-facebook-sugiere-amigos-que-daba-olvidados_2016032257fd32760cf2fd8cc6b1f97e.html. [Último acceso: 24 enero 2017].

[41] M. Varela, «Marketing 4 Ecomerce» 11 agosto 2016. [En línea]. Disponible: http://marketing4ecommerce.net/historia-de-twitter/. [Último acceso: 27 enero 2017].

[42] M. R. Rangel, «Universidad Cooperativa de Colombia» [En línea]. Disponible: http://www.ucc.edu.co/institucion/paginas/rectoria.aspx. [Último acceso: 24 enero 2017].

[43] M. Ramirez, «El Mundo» 27 enero 2014. [En línea]. Disponible:

http://www.elmundo.es/internacional/2014/01/27/52e6b11d22601d843c8b457a.html. [Último acceso: 24 enero 2017].

[44] Á. Borroy, «Ángel Borroy Wordpress» 4 febrero 2013. [En línea]. Disponible: https://angelborroy.wordpress.com/2013/02/04/medios-de-identificacion-delegada-oauth-y-openid/. [Último acceso: 23 enero 2017].

[45] E. Schmitt, «New York Times» 27 julio 2016. [En línea]. Disponible: https://www.nytimes.com/2016/07/28/world/middleeast/us-intelligence-isis.html?_r=0. [Último acceso: 29 enero 2017].

[46] Agencia EFE, «Primerahora» 21 mayo 2016. [En línea]. Disponible: http://www.primerahora.com/tecnologia/nota/cuantosusuariostieneinstagram-1160278/. [Último acceso: 27 enero 2017].

[47] Ediciones, «Reportaje de lo Bueno» 22 noviembre 2016. [En línea]. Disponible: http://reportajede.news/?p=8404. [Último acceso: 28 enero 2017].

[48] Happy Fm, «El Mundo» 3 agosto 2016. [En línea]. Disponible: http://www.elmundo.es/happy-fm/2016/08/03/57a1bfd7e2704e7d2a8b45da.html. [Último acceso: 29 enero 2017].

[49] F. Fernandez, «En Bytes» 26 diciembre 2012. [En línea]. Disponible: http://enbytes.com/site/2012/12/26/instagram-da-marcha-atras-a-nuevas-politicas-ante-protesta-de-sus-usuarios/. [Último acceso: 27 enero 2017].

[50] F. Ruiz, «Educadictos» 8 mayo 2013. [En línea]. Disponible: http://www.educadictos.com/como-crear-un-perfil-de-empresa-en-linkedin/. [Último acceso: 28 enero 2017].

[51] Á. Campos, «The Motley Fool» 19 julio 2014. [En línea]. Disponible: http://www.fool.com/investing/general/2014/07/19/heres-how-linkedin-is-targeting-future-growth.aspx. [Último acceso: 29 enero 2017].

[52] A. A.Llorca, «Genbeta» 5 agosto 2016. [En línea]. Disponible: https://www.genbeta.com/redes-sociales-y-comunidades/linkedin-cuenta-con-mas-de-450-millones-de-usuarios-pero-solo-el-25-la-visita-todos-los-meses. [Último acceso: 29 enero 2017].

[53] Agencia EFE, «ABC» 18 marzo 2016. [En línea]. Disponible: http://www.abc.es/tecnologia/redes/abci-linkedin-supera-8-millones-usuarios-espana-2015-201603161153_noticia.html. [Último acceso: 28 enero 2017].

[54] M. Gonzalez, «Genbeta» 6 junio 2012. [En línea]. Disponible: https://www.genbeta.com/redes-sociales-y-comunidades/el-dia-negro-de-linkedin-se-filtra-una-lista-con-supuestas-contrasenas-y-se-desvelan-problemas-de-privacidad-en-ios. [Último acceso: 28 enero 2017].

[55] J. Domingo, «Seguridad en redes,» 18 abril 2013. [En línea]. Disponible: https://statusexcessu.wordpress.com/2013/04/18/sha-1/. [Último acceso: 29 enero 2017].

[56] P.R., «El Español» 18 mayo 2016. [En línea]. Disponible: http://www.elespanol.com/ciencia/tecnologia/20160518/125737475_0.html. [Último acceso: 29 enero 2017].

[57] UAB, «Blogs UAB,» 2 marzo 2015. [En línea]. Disponible:

http://blogs.uab.cat/todowhatsapp/2015/03/02/whatsapp-que-es-y-para-que-sirve/. [Último acceso: 24 enero 2017].

[58] V. Rodríguez, «Movil Zona» 21 marzo 2013. [En línea]. Disponible: https://www.movilzona.es/2013/03/21/como-instalar-whatsapp-en-una-tableta/. [Último acceso: 29 enero 2017].

[59] J. C. Baños, «Frikipandi» 29 mayo 2016. [En línea]. Disponible: http://www.frikipandi.com/public/post/historia-whatsapp/. [Último acceso: 24 enero 2017].

[60] D. G.Aparicio, «20 Minutos» 3 mayo 2016. [En línea]. Disponible: http://www.20minutos.es/noticia/2762095/0/whatsapp-telegram-comparativa-mensajeria-instantanea/. [Último acceso: 24 enero 2017].

[61] J. M. Zurriarain, «El País» 9 Abril 2016. [En línea]. Disponible: http://tecnologia.elpais.com/tecnologia/2016/04/06/actualidad/1459942001_217614.html. [Último acceso: 25 enero 2017].

[62] Á. d. l. Rios, «El Correo» 28 enero 2017. [En línea]. Disponible: http://www.elcorreo.com/bizkaia/tecnologia/gadgets/201701/27/whatsapp-permitira-grupos-saber-20170127170042.html. [Último acceso: 29 enero 2017].

[63] C. Triebert, «bellingcat» 24 julio 2016. [En línea]. Disponible: https://www.bellingcat.com/news/mena/2016/07/24/the-turkey-coup-through-the-eyes-of-its-plotters/. [Último acceso: 22 enero 2017].

[64] A. Salas, Los hombres que susurruban a las máquinas, Barcelona: Espasa, 2015.

[65] A. Salas, «El Mundo» 24 noviembre 2015. [En línea]. Disponible: http://www.elmundo.es/cronica/2015/11/24/56503c47268e3ecf218b4577.html. [Último acceso: 30 enero 2017].

[66] C. Zahumenszky, «GIZMODO» 1 diciembre 2015. [En línea]. Disponible: http://es.gizmodo.com/isis-asegura-haber-vulnerado-la-cuenta-de-twitter-del-p-1679009683. [Último acceso: 1 febrero 2017].

[67] I. Oroz, «Pepeles de inteligencia» 19 diciembre 2013. [En línea]. Disponible: http://papelesdeinteligencia.com/que-es-la-infoxicacion/. [Último acceso: 29 enero 2017].

[68] Enforex, «Enfolang» [En línea]. Disponible: http://www.enfolang.com/internacional/redes-sociales/privacidad-redes-sociales.html. [Último acceso: 28 enero 2017].

[69] J.A.Dominguez, «Sobre privacidad» CIFAS, Madrid, 2017.

[70] Instituto Español de Estudios de la Defensa, IEEE, «IEEE» Diciembre 2010. [En línea]. Disponible: http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf. [Último acceso: 15 febrero 2017].

[71] U. d. Vigo, «Faitic» 2012. [En línea]. Disponible: http://www.faitic.uvigo.es/index.php/es/. [Último acceso: 25 febrero 2017].

[72] A. "forocule", «forocule» 5 marzo 2015. [En línea]. Disponible: http://www.forocule.net/t5635-nos-espian. [Último acceso: 5 marzo 2017].

[73] S. EMERGUI, «El Mundo» 12 enero 2017. [En línea]. Disponible:

http://www.elmundo.es/internacional/2017/01/11/5876662fe2704ed2618b4617.html. [Último acceso: 28 enero 2017].

[74] UP! Psicología & Coaching, «UP! Psicología & Coaching» 16 diciembre 2013. [En línea]. Disponible: http://up-psicologia.com/blog/2013/varios/mi-ego-en-la-red-trastorno-narcisista-de-la-personalidad/. [Último acceso: 14 febrero 2017].

[75] E. C. Calpe, «Psicología y Mente» [En línea]. Disponible: https://psicologiaymente.net/social/psicologia-redes-sociales-codigo#!. [Último acceso: 14 febrero 2017].

[76] Bellingcat, «bellincat» 20 enero 2017. [En línea]. Disponible: https://www.bellingcat.com/news/mena/2017/01/20/new-satellite-imagery-shows-russian-su-24-jets-hmeimim-air-base/. [Último acceso: 22 enero 2017].

[77] V. total, «Virustotal» [En línea]. Disponible: https://www.virustotal.com/es/. [Último acceso: 2 febrero 2017].

ANEXO I: GLOSARIO DE TÉRMINOS

- **Algoritmo SHA-1:** Algoritmo de autenticación.
- **Anonymus:** Conjunto de personas con conexión a internet, cuyo común ideal, por encima de cualquier otro, es la defensa de la libertad de expresión.
- **Autorun:** Capacidad de un sistema/programa/archivo de ejecutarse sin la necesidad de interactuar con él.
- **Bajas cero:** Término que hacer referencia a no sufrir ninguna baja durante el desarrollo de una contienda.
- **Briefing:** Reunión/exposición.
- **Caché:** Área de almacenamiento dedicada a la recuperación a gran velocidad de los datos usados o solicitados con más frecuencia.
- **Ciberarma:** Neologismo que hace referencia a las armas utilizadas en el ámbito ciber.
- **Ciberataque:** Neologismo que hace referencia a los ataques sufridos a través de una plataforma cibernética.
- **Ciberdelito:** Neologismo que hace referencia a los delitos cometidos a través de la red.
- **Ciberguerra:** Neologismo que hace referencia a la guerra llevada a cabo a través de la red.
- **CIFAS:** Centro de Inteligencia de las Fuerzas Armadas.
- **CNI:** Centro Nacional de Inteligencia.
- **Códigos QR:** Módulo que permite almacenar información en una matriz de puntos.
- **Deep Web:** También conocida como Web Oscura, es la parte de la red que carece de regulación jurídica, y cuenta como máxima fundamental con el anonimato de sus integrantes.
- **Dispositivo Teensy:** Pequeño microcontrolador HID programable con interfaz USB que permite emular un teclado y mouse para enviar comandos a cualquier sistema operativo.
- **DNS Spoofing:** Método para alterar las direcciones de los servidores DNS que utiliza la potencial víctima y de esta forma poder tener control sobre las consultas que se realizan.
- **Encoder:** Programa utilizado para convertir una información de un formato a otro.
- **Exploit:** Programa o código que se aprovecha de un agujero de seguridad (vulnerabilidad) en una aplicación o sistema.
- **Factor humano:** Término que hace referencia al humano como herramienta en sí misma.
- **Fake AP:** Punto de acceso Wi-Fi falso.
- **FAS:** Fuerzas Armadas.
- **FCSE:** Fuerzas y Cuerpos de Seguridad del Estado.
- **Grupo terrorista HAMAS:** Grupo terrorista que lucha por la imposición de un estado islámico en palestina.
- **Hacktivista:** Individuo que lleva a cabo acciones de activismo a través de la red.
- **Hashtag:** Del inglés etiqueta. Se refiere a la palabra o la serie de palabras o caracteres alfanuméricos precedidos por el símbolo de la almohadilla.
- **Hispasec:** Organización informática dedicada a la seguridad informática.
- **HUMINT (HUman INTelligence):** Procedimiento de obtención de inteligencia a través de humanos.
- **IMINT (IMage INTelligence):** Procedimiento de obtención de inteligencia a través de imágenes.
- **INET:** Instituto Nacional de Educación Tecnológica.
- **ISIS:** Islamic State of Iraq and Syria-Estado Islámico de Irak y Síria.
- **Kali Linux:** Sistema operativo utilizado para realizar pruebas de seguridad, así como auditorias de seguridad.

- **Malware:** Abreviatura de "software malicioso", se define como un software destinado a acceder a un dispositivo de forma inadvertida.
- **MASINT (Measurement and Signature INTelligence):** Procedimiento de obtención de inteligencia a través de mediciones y firmas electrónicas.
- **Metadatos:** Conjunto de datos contenido dentro de un archivo.
- **Metasploit:** Es un proyecto de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad.
- **Microblogging:** Servicio que permite a sus usuarios enviar y publicar mensajes breves, generalmente solo de texto.
- **MITM:** (Man in the Middle) ataque consistente en situarse entre usuario y sistema.
- **NSA (National Security Agency -Agencia de Seguridad Nacional):** Es una agencia de inteligencia del Gobierno de los Estados Unidos que se encarga de todo lo relacionado con la seguridad de la información.
- **OSINT (Open Source Intellingence):** Procedimiento de obtención de inteligencia a través de fuentes abiertas.
- **OTAN:** Organización del Tratado del Atlántico Norte.
- **Payload:** Parte del malware que realiza la acción maliciosa.
- **Powershell:** Terminal de un sistema operativo.
- **Puerta trasera/backdoor:** Malware que tiene como finalidad adquirir permisos de usuario, pudiendo llegar a realizar cualquier tipo de modificación sobre la plataforma objetivo.
- **Punto de acceso Wi-Fi:** Área física en la cual se puede conectar un equipo con capacidades Wi-Fi.
- **Red de Defensa:** Es la red utilizada por los integrantes de las FAS, asequible a través de ordenadores corporativos que puedan acceder a dicha VPN.
- **Ripe.net:** Página dedicada a dar información sobre IP/usuarios, así como controladores de redes.
- **Servidor DNS (Domain Name System - Sistema de nombres de dominio):** es un servidor que traduce nombres de dominio a IPs y viceversa. En las redes TCP/IP, cada PC dispone de una dirección IP para poder comunicarse con el resto de PCs.
- **SIGINT (SIGnal INTelligence):** Procedimiento de obtención de inteligencia a través de señales(electromagnéticas).
- **Sniffing:** Efecto de capturar los paquetes que viajan dentro de una red.
- **Software:** Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en un ordenador.
- **Spam:** Correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales.
- **Spear phising:** Consiste en crear un correo electrónico que aparenta ser de una persona o empresa conocida, con el fin de introducir un malware en la plataforma objetivo.
- **Valoraciones de amenaza TESSCO:** Valoraciones que hacen referencia a las posibles amenazas surgidas del terrorismo, espionaje, subversión, sabotaje y crimen organizado.
- **VoIP:** Voz sobre IP, es decir llamadas a través de Internet.
- **WikiLeaks:** Es una organización mediática internacional sin ánimo de lucro, que publica a través de su sitio web informes anónimos y documentos filtrados con contenido sensible en materia de interés público, preservando el anonimato de sus fuentes.

ANEXO II: EJEMPLOS REALES

Personal de la EZAPAC:

Se trata de personal de la EZAPAC (Escuadrón de Zapadores paracaidistas), se mantienen activos a la hora de comentar en páginas relacionadas con las Fuerzas Armadas. Se puede ver los lugares donde han estado desplegados, e incluso elaboran etiquetas para dicho fin y muestran armas relacionadas con unidades de operaciones especiales (Figura A2-3).

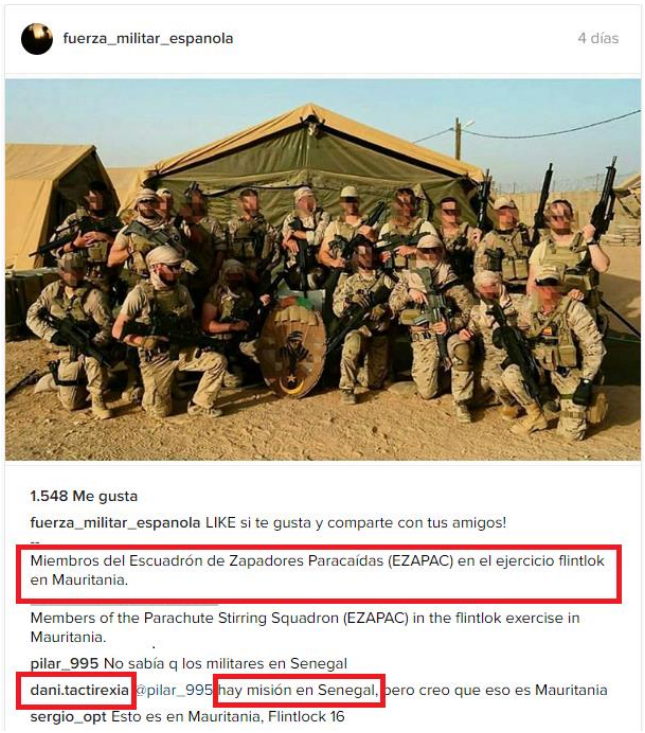


Figura A2-1 Integrantes EZAPAC.

Misión Mauritania de la EZAPAC (Figura A2-1).

Figura A2-2 Misión en Senegal 2016.

Misión Senegal de la EZAPAC (Figura A2-2).

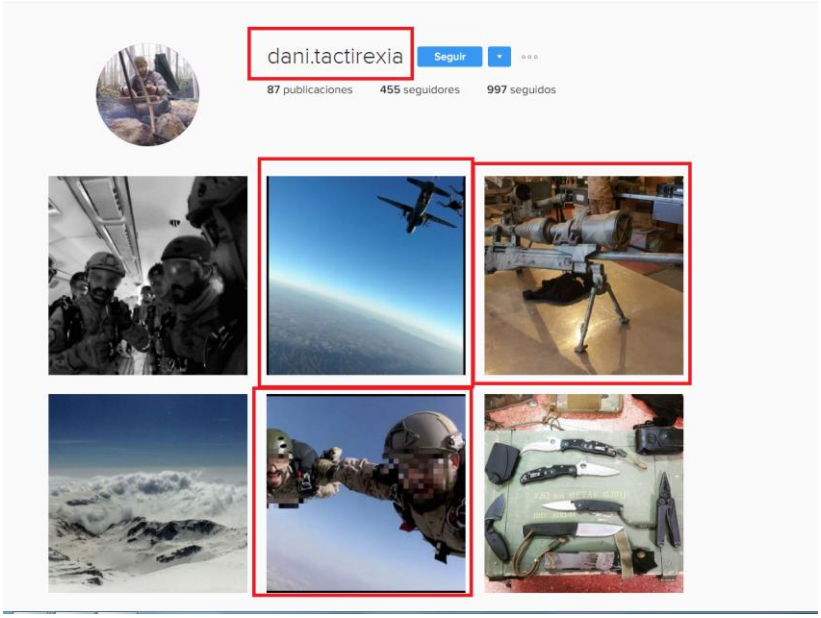


Figura A2-3 Fotografías personales de miembros EZAPAC.

Personal de misión:

Se trata de un soldado de la Legión que sube fotos estando de misión y también de carácter personal, por lo que puede ser un objetivo de ataque, siendo su familia un objetivo rentable.

Figura A2-4 Miembro de la legión en Afganistán.

Añade etiquetas no relacionadas con el propósito de la fotografía y que puedan tener mucha más audiencia que una etiqueta relacionada con la misma (Figura A2-4).

Figura A2-5 Imágenes personales.

Además, aunque no identifique la cuenta con nombre y apellidos, en varias fotografías aparece con la identificación de pecho (Figura A2-5).

Otras fotografías de redes sociales:

Ejemplos de acciones que se deben suprimir del uso de las redes sociales (Figura A2-6).

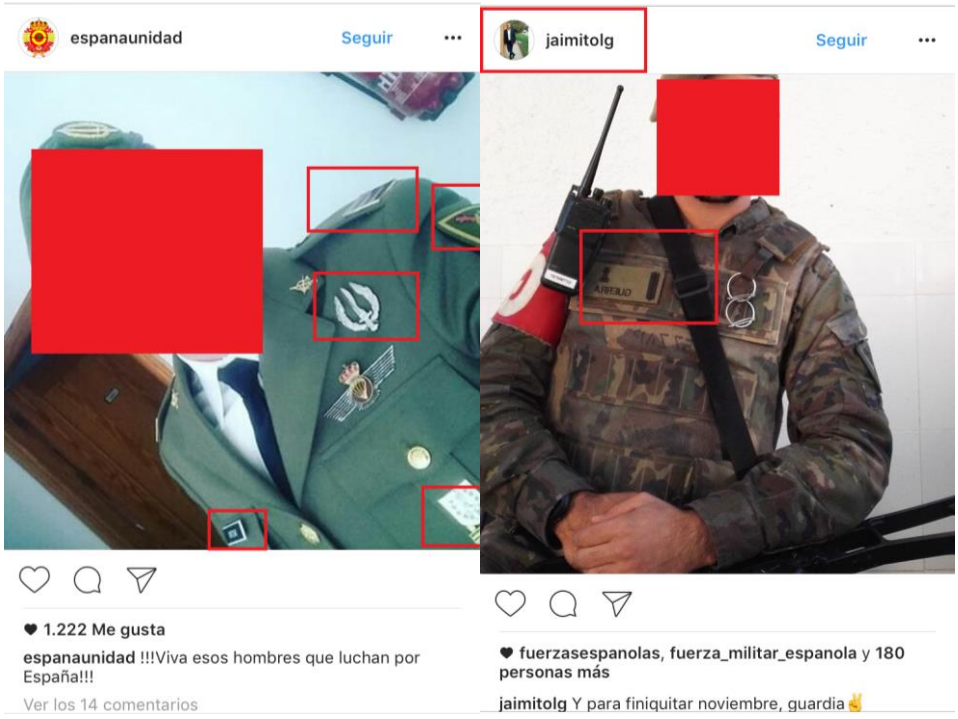


Figura A2-6 Imágenes obtenidas de redes sociales.

Ejemplo de Creepy en Escuela Naval Militar:

Durante este ejemplo se llevó a cabo el uso de la herramienta Creepy sobre Marín, se detectó el uso de Twitter por parte de un alumno (Figura A2-7,Figura A2-8, Figura A2-9 y Figura A2-10).

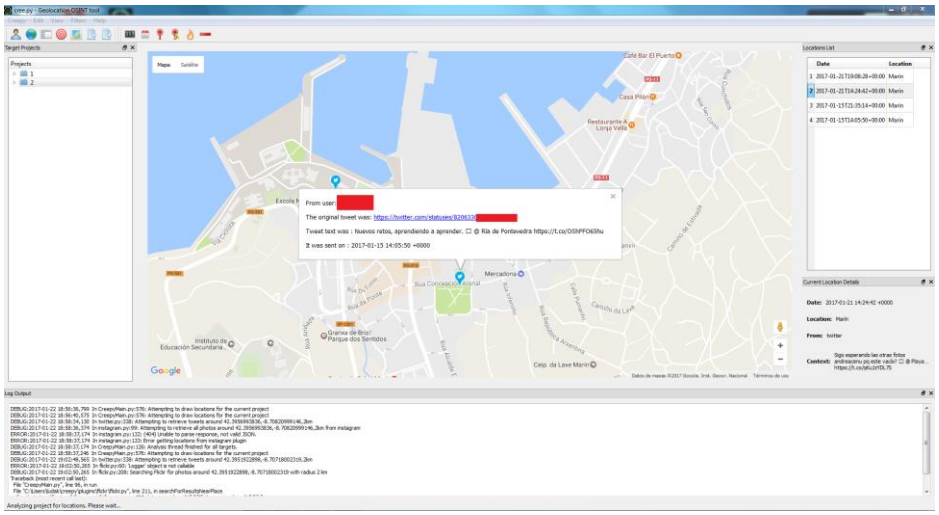


Figura A2-7 Localización en Creepy de alumno de la E.N.M.

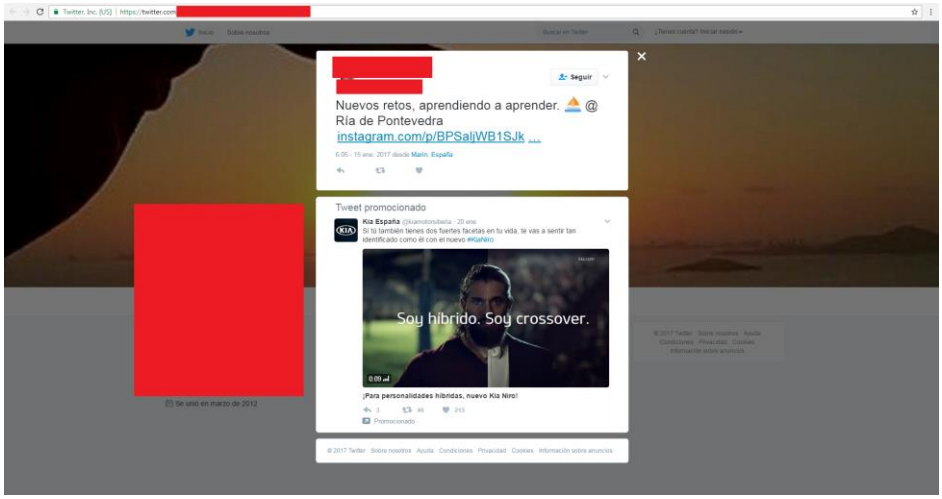


Figura A2-8 Mensaje obtenido a través de Creepy.

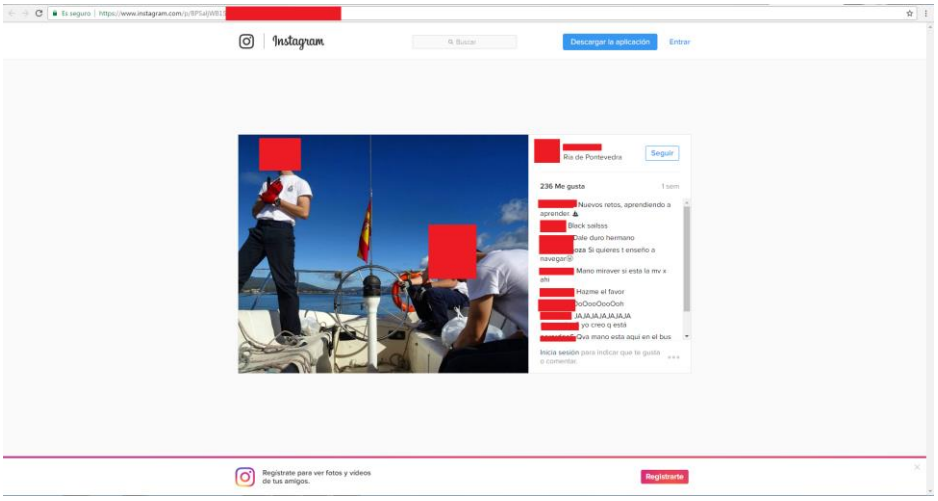


Figura A2-9 Imagen compartida en redes sociales.

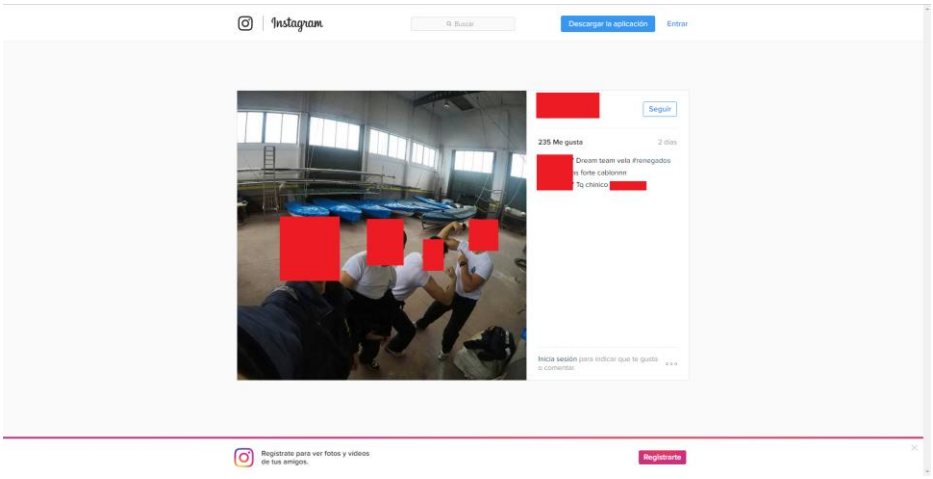


Figura A2-10 Muestra de imagen compartida en redes sociales.

Como se puede ver, nada en la red queda exente de poder ser utilizado en contra de los usuarios que lo hayan publicado, en este caso se trata de una práctica normal entre los nuevos integrantes de las FAS.

Información vertida por las propias FAS:

En este caso son las propias fuentes oficiales las que vierten información innecesaria a la red (Figura A2-11).

Figura A2-11 Imagen compartida por Ministerio de Defensa.

Ejemplo de perfiles en LinkedIn:

Dentro de este ejemplo se puede ver verdaderos currículums de personal de las FAS, llama la atención currículum de personal que acaba de salir de una academia militar.

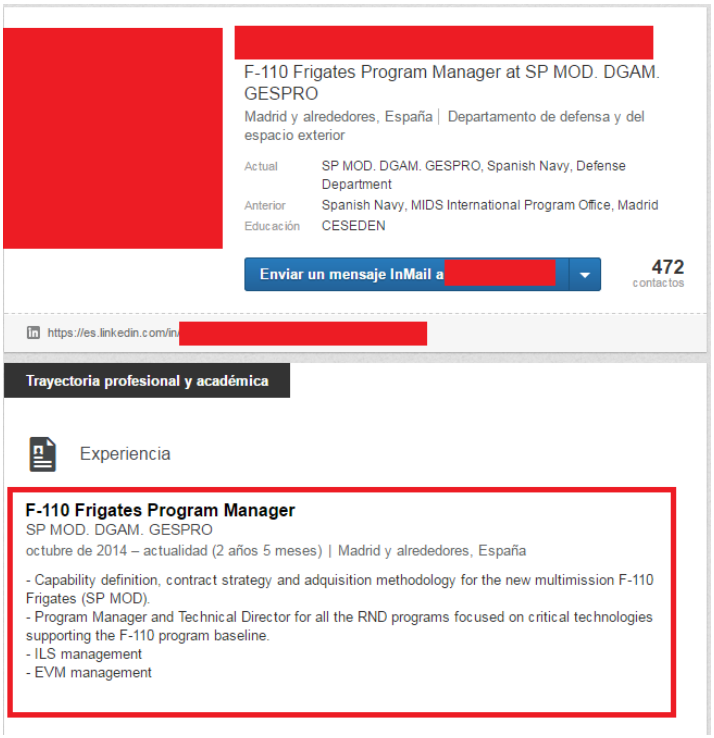


Figura A2-12 Director del programa de fragatas F-110.

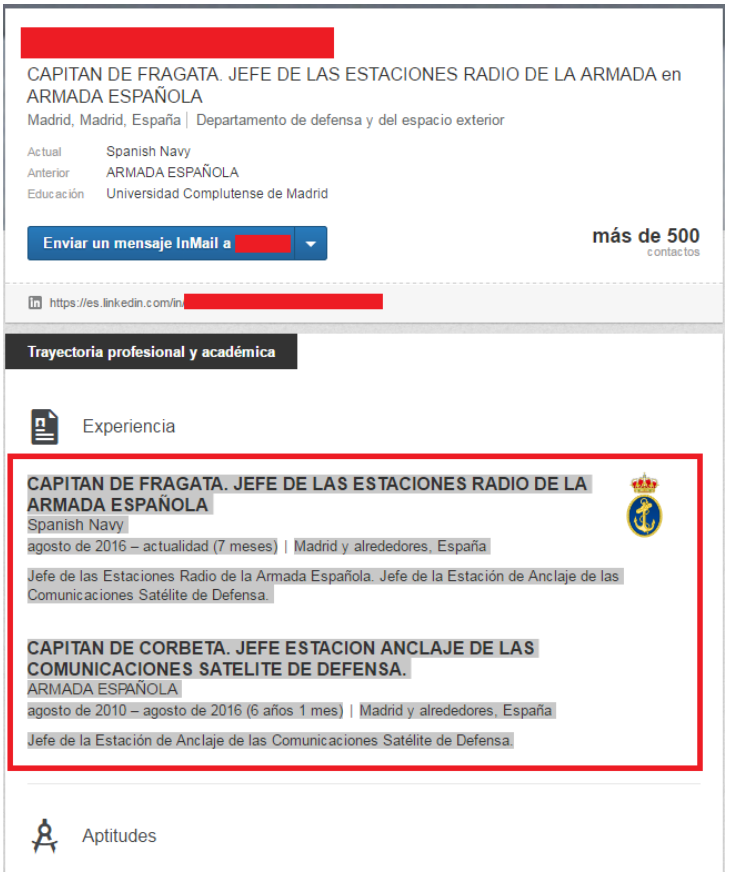


Figura A2-13 Jefe de estaciones radio de la Armada.

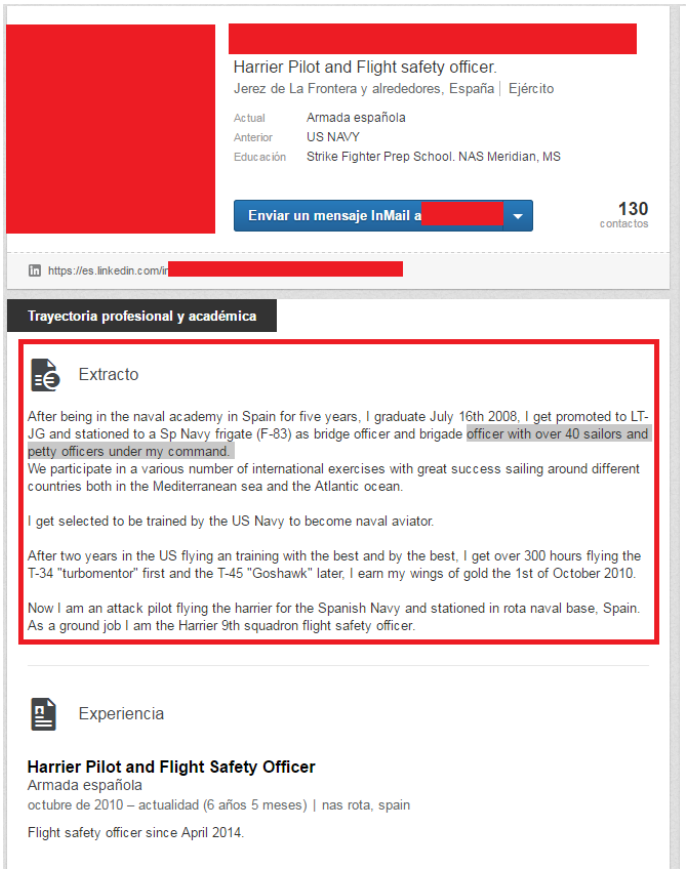


Figura A2-14 Perfil piloto de la Armada.

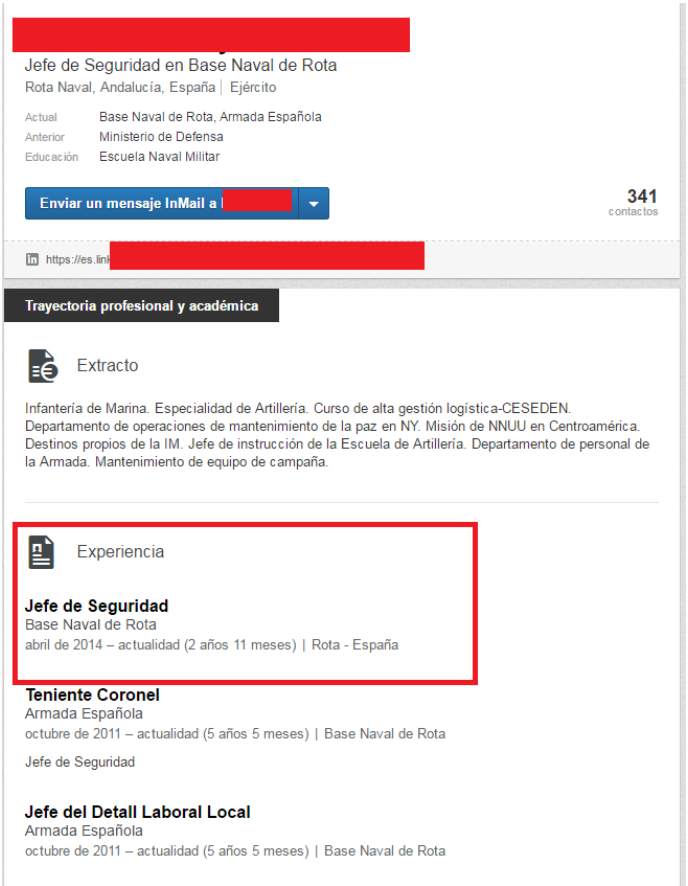


Figura A2-15 Jefe de seguridad en Base Naval de Rota.

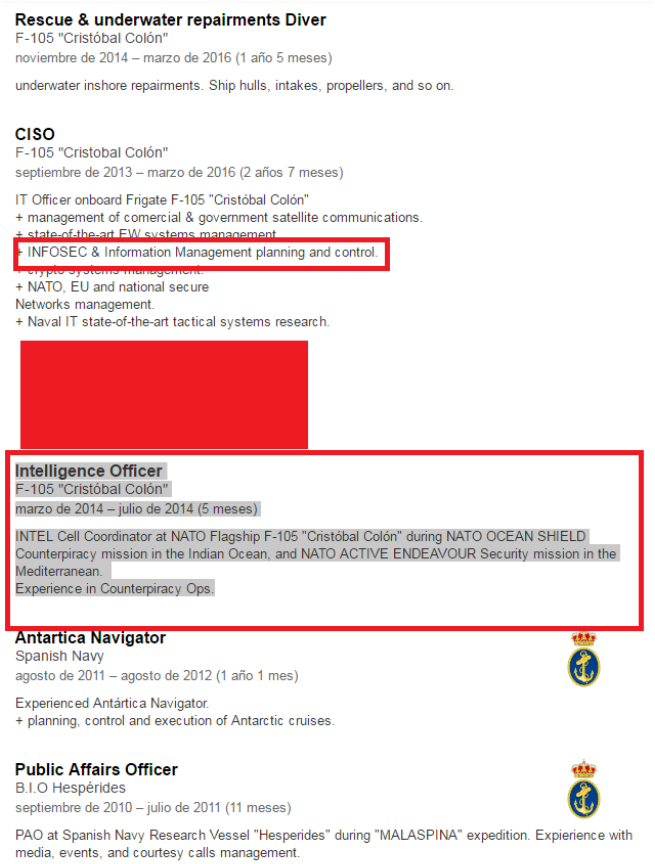


Figura A2-16 Oficial de inteligencia de la F-105.

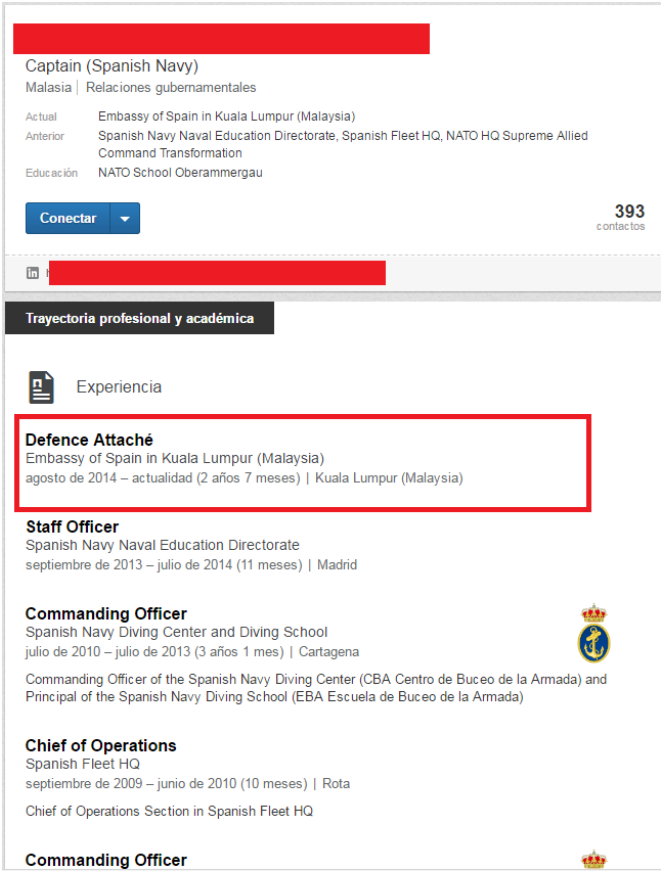


Figura A2-17 Capitán en embajada de Kuala Lumpur.

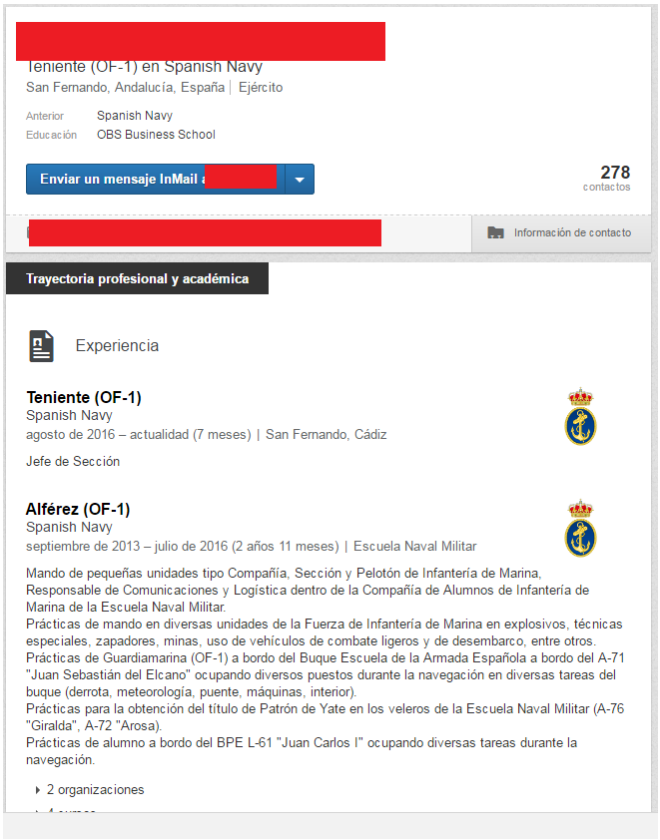


Figura A2-18 Teniente moderno de Infantería de Marina.

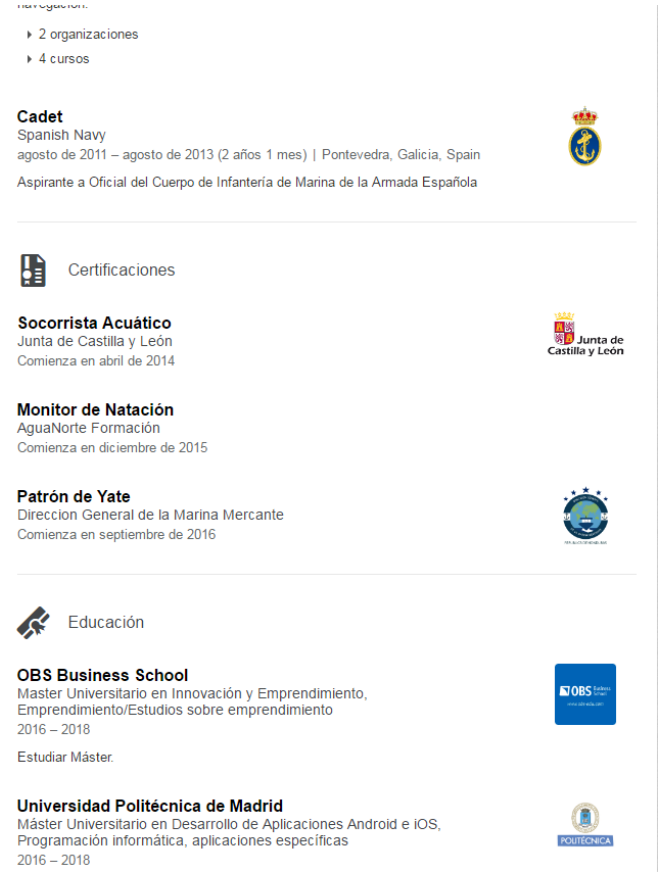


Figura A2-19 Teniente moderno de Infantería de Marina (estudios).

Como se puede ver, son numerosos los perfiles (Figura A2-12,Figura A2-13,Figura A2-14,Figura A2-15,Figura A2-16,Figura A2-17,Figura A2-18 y Figura A2-19) a los que se puede acceder a través de la red, información que en la mayoría de los casos la red no es su ubicación más idónea.

Ejemplo de obtención de información de fuentes abiertas sobre Donald Trump:

Figura A2-20 Oficial con maletín del Presidente Trump.

En la Figura A2-20 se puede ver como se filtra la identidad del oficial que lleva el maletín que autoriza al presidente estadounidense a efectuar un ataque nuclear.