Universidad
Carlos III de Madrid
www.uc3m.es

Grado en Ingeniería Informática

Especialidad: Sistemas de la Información

Trabajo Fin de Grado

Fraude Digital: Prevención, Detección, Análisis y Eliminación.

Autor: Manuel Hernández Fernández.

Tutor: Miguel Ángel Ramos.

Madrid, 9 de Marzo de 2015.

Agradecimientos

Vislumbrando el final de mi etapa universitaria y con poco que demostrar ya académicamente, es el momento de recordar a toda esa gente que me ha llevado en el día a día en lo que será, probablemente, la etapa más importante de mi vida y una de las más bonitas sin duda.

Atrás quedan ya los momentos de exámenes, prácticas, las tensiones y preocupaciones propias de la actividad universitaria y me veo en la obligación de mencionar, en primer lugar, a todas aquellas personas que han vivido esos momentos conmigo con la misma intensidad. Gente sin la que, estoy convencido, esto hubiera sido completamente diferente y no tan satisfactorio. Personas que considero mucho más que compañeros, verdaderos amigos que espero conservar para toda la vida. No tengo palabras para agradecer a Fernando García, José Luis Garrido, Ignacio García, Jesús Alberto Llorente y Daniel López por su impagable apoyo y amistad.

En segundo lugar me gustaría acordarme, como no podía ser de otra manera de mis padres y mi hermana, ellos han sido el apoyo más fuerte sin duda que he tenido y merecen mención especial. Sus ánimos, indispensables y siempre presentes cuando hacían falta, han sido los que me han hecho continuar hacia adelante y no desfallecer en este largo tramo que llega a su fin, en parte, gracias a ellos. También quiero acordarme de mis amigos de toda la vida, sin cuya ayuda esto habría sido mucho más difícil y que desde luego siempre han estado ahí cuando más lo necesitaba.

Además me gustaría agradecer particularmente a Miguel Ángel Ramos, por su profesionalidad y tiempo dedicados a que este documento gozase de la máxima calidad, así como a todos los profesores y docentes con los que me he encontrado a lo largo de estos años y me han ayudado a ser mejor.

En este punto me encuentro dando el paso más importante de mi vida, el del mundo estudiantil al laboral, el cual afronto con ganas y espero sea, por lo menos, tan satisfactorio como la etapa que dejo atrás.

1. Resumen

El delito digital es una realidad que no se puede pasar por alto. Cada día son más y más los delincuentes que deciden cambiar la calle por el ordenador debido a todas las ventajas que ello conlleva, pues se trata de un mundo que a día de hoy permanece casi virgen en lo que a seguridad se refiere y les permite actuar a voluntad con mucho menos riesgo del que tendrían en el mundo real. Por ello se ha ideado este documento, cuyo objetivo es orientar en la lucha contra uno de los delitos más comunes, el *Fraude Online*.

La gestión de un caso de *Fraude Online* como pudiese ser un *Phishing* se estructurará en 3 momentos claves para su tratamiento: Detección, Análisis y Eliminación. Se añadirá un apartado extra, el de Prevención, que son unas pautas más orientadas al usuario medio en un ámbito doméstico que al analista del ámbito profesional.

Aunque se ha intentado crear una guía lo más sencilla posible para el lector, la naturaleza de la temática que se va a tratar hace que sea fácil perderse en algunos puntos, es por ello que a continuación, se explicarán los pasos básicos a realizar para solventar con éxito un caso reportado:

- ***Detección:*** La motivación de este módulo es conseguir verificar que se está ante un caso de fraude fidedigno. Para ello se harán uso de diferentes herramientas (ya sean privadas o públicas) que permitirán al analista comprobar la actividad y evaluar la gravedad del caso. Con esto ya se podrá informar al cliente de su apertura y del tratamiento del mismo. Éste, probablemente, sea el momento que más experiencia requiere por parte del analista, pues la información obtenida por las herramientas debe ser interpretada por él para sacar las conclusiones adecuadas y proceder en consecuencia declarando como fraude un caso.
- ***Análisis*****:** Llegado este punto, es el momento de recabar toda la información posible para poder acelerar el cierre del caso. Para ello y de nuevo, se deberán utilizar diversas herramientas que mostrarán toda la información relacionada con el *Dominio* afectado. Con esta información se elaborará un plan de actuación con el que empezar a contactar en el siguiente apartado con los contactos que puedan tener algún tipo de influencia en el caso. Como se indicará es recomendable revisar casos ya cerrados en el pasado para comprobar si existe algún patrón de actuación ya utilizado que pueda ser de ayuda o si hay algún tipo de información que sea común a ambos, con el consiguiente ahorro de tiempo y medios.
- ***Eliminación*****:** En este momento de la vida del caso, se van a realizar las acciones oportunas para solicitar que aquellas personas o empresas que tengan algún tipo de poder administrativo sobre el *Dominio* empiecen a gestionar el cierre del mismo o, en su defecto, colaboren con el analista para conseguirlo. Una vez obtenido el cierre y verificado el mismo, se informará al cliente de la conclusión satisfactoria del caso y se procederá a monitorizar la/s *Uri/*s afectada/s.

Con esto se tendría el plan de ruta básico y elemental para hacer frente al *Fraude Digital*, no obstante, la experiencia del analista es la que va a determinar el éxito en la gestión de un caso, por lo que independientemente de esta guía, es primordial contar con una formación especializada sólida.

2. Abstract

The digital crime is a reality that cannot be overlooked. Every day there are more and more criminals who decide to change the streets for the computer, due to all the advantages that it carries, because it is a question that today still remains almost virgin in what to safety refers and allows them to operate to will with much fewer risk of which they would have in the real world. That is the reason why this document has been designed, and which aim is to orientate in the fight against one of the most common crimes, the Fraud Online.

The management of a case of Fraud Online like Phishing, for example, will be structured in 3 key moments for his treatment: Detection, Analysis and Elimination. It will be added an extra paragraph, the Prevention one, which is a few guidelines more orientated to the average user in a domestic area that to the analyst of the professional area.

Though an as simple as possible guide has tried to be created for the reader, the nature of the subject matter that is going to treat does that it is easy to get lost in some points, is for it that later, the basic steps which must be done will be explained to solve successfully a brought case:

- ***Detection:*** The motivation of this module is to manage to check that one is in front of a case of trustworthy fraud. For that, it will be used different tools (private or public ones) that will allow to the analyst to verify the activity and to evaluate the gravity of the case. With this, it will already be possible to inform to the client of his opening and how to treat it. This one, will probably be the moment that more experience needs on the part of the analyst, since the information obtained by the tools must be interpreted by him to extract the suitable conclusions and to proceed in consequence declaring as fraud a case.
- ***Analysis:*** Come this point, it is the moment to obtain all the possible information to be able to accelerate the closing of the case. For it and again, there must be used diverse tools that will show all the information related with affected Domain. With this information there will be elaborated a plan of action with which to start contacting in the following paragraph with the contacts that could have some type of influence in the case. As it will be indicated it is advisable to check other cases already closed, to verify if there is some boss of action already used, that could help or if there is some type of information that is common to both, with the consequent saving of time and a half.
- ***Elimination:*** At this moment of case's life, the opportune actions are going to start in order to request that those persons or companies that have some type of administrative power on the Domain start managing the closing of it or, in his fault, collaborate with the analyst to obtain it. Once obtained the closing and assured it, the client will be informed of the satisfactory conclusion of the case and we will proceed to monitor the *Uri's* afected.

With this we have the basic and elementary plan of route to face the Digital Fraud, nevertheless, the experience of the analyst it is what is going to determine the success in the management of a case, for what independently of this guide, it is basic to possess a specialized solid formation.

3. Índice

4. Índice Ilustraciones

5. Prólogo: Ciberdelito ¿Por qué Internet?

Todo el mundo ha oído hablar alguna de vez de los delitos que se realizan en Internet. Cada cierto tiempo suele aparecer alguna noticia que apunta a algún golpe de gran magnitud con fines lucrativos y desarrollado desde la red, pero, ¿Por qué?, ¿Por qué en Internet y no en la vida real como ha venido ocurriendo hasta ahora?

Internet es una red donde todas las ventajas pueden tornarse inconvenientes desde el punto de mira que se use. Por ejemplo, la búsqueda de privacidad siempre ha estado bien vista desde la perspectiva de un usuario medio, pues a nadie le gusta que vigilen por donde navega, ni a con qué frecuencia o a qué horas lo hace, sin embargo, si se mira desde la perspectiva de un delincuente, el prisma cambia por completo y empiezan a saltar todas las alarmas.

Esta bipolaridad latente en todo lo que rodea Internet es la que fomenta su uso de manera ilegal o con fines lucrativos. Cualquier aspecto que beneficie a un usuario común, también beneficia al criminal y si se une a unos conocimientos del sector avanzados (como suele ser en la mayoría de los casos de delito Online) el resultado puede llegar a ser abusivo.

Pero concretamente ¿Qué lleva al criminal a involucrarse en el delito Online y no al de la vida real? Aunque complicada, esta pregunta tiene respuesta y para ayudar a encontrarla, los siguientes factores pueden ser determinantes:

- ***Privacidad***: Aunque siempre habrá organismos públicos que intentarán tranquilizar respecto a la privacidad Online, la realidad es otra muy distinta. La realidad es que el escenario actual en la red de redes, por la manera en la que los organismos lo están gestionando, pone más énfasis en vigilar al usuario común que al criminal. Vigilar los pasos que cualquier persona da por internet es relativamente sencillo si se tienen ciertos conocimientos y, de hecho, hay multitud de herramientas corporativas que ayudan a las empresas a ello. Sin embargo, no se pone el mismo énfasis en el delincuente y esto viene determinado por dos factores:
    - El primero, es difícil hallar un equilibrio en la privatización del usuario que permita tanto salvaguardar la información del usuario común, como de perseguir los pasos del que delinque. No existe la paridad, lo que beneficia a unos perjudica a otros y, obviamente siempre hay que actuar en consecuencia al comportamiento de una mayoría, en este caso, los usuarios comunes.
    - El segundo, el delito digital requiere unos conocimientos técnicos, los cuales en muchos casos permiten al delincuente pasar por encima de la mayoría de técnicas empleadas en el rastreo de un usuario (Un buen ejemplo son los *Proxies* que se explicarán en este documento).

  Por otro lado suponiendo ambos escenarios, el real y el digital, la diferencia en el tiempo de respuesta tras dar con el delincuente puede llegar a ser abismal. El riesgo de captura un ladrón convencional respecto al de un ladrón digital es totalmente

desproporcionado en favor del segundo. En la calle hay infinidad de factores que puedan dar al traste con los planes del delincuente en minutos, sin embargo en Internet, suponiendo una formación informática apropiada, el éxito o el fracaso lo dicta el propio delincuente y suponiendo un fracaso en sus planes, el tiempo de espera hasta que es identificado suele ser bastante amplio llegando a ser de meses o incluso años.

En definitiva, en la calle no se puede cambiar de cara mientras que Internet ofrece infinidad de mecanismos, a cuál más sofisticado, para impedir que gente indeseable la vea, además siempre es más fácil apagar un ordenador que huir de la policía.

- ***Accesibilidad***: Hoy en día prácticamente cualquiera tiene acceso a un ordenador con conexión a Internet y por lo tanto, a todo el contenido de este. Atrás quedan las metodologías de hurto empleadas por los delincuentes en el mundo real, ahora, lo único que necesitan son conocimientos (lo más complicado de obtener del proceso) y un ordenador personal.

  Además, los límites geográficos desaparecen, lo cual permite a un ladrón actuar en casi cualquier parte del mundo con una infraestructura tecnológica relativamente moderna, esto combinado con el punto anterior, complica extremadamente el proceso de búsqueda e identificación de los responsables, pues estos pueden estar a miles de kilómetros de distancia.

  Por otro lado, el costo de realizar una operación digital a gran escala es mínimo en comparación a lo que una operación equivalente en el mundo real podría suponer. De hecho, no son pocos los casos en los que el origen del delito se ha llevado a cabo desde lugares públicos como cibercafés, cuyo coste es mínimo.

  En resumen, moverse por Internet resulta más barato y cómodo que moverse por el mundo real y cuando se trata de delinquir, estos dos aspectos son tenidos muy en cuenta.

- ***Posibilidades***: En un mundo donde prácticamente todo está tecnológicamente conectado a Internet, desde una simple nevera hasta una central nuclear, es evidente que las posibilidades que ofrece el manejo de dichas conexiones es prácticamente infinito. Esto supone que cualquier dispositivo, en teoría, podría comunicarse con cualquier otro del planeta si se sabe cómo.

  Lo que a priori parece una ventaja y, de hecho, nació con la intención de ser tal, si se emplea con aviesas intenciones se pueden obtener resultados realmente desproporcionadas tanto del lado que se beneficia de ello como del lado que se perjudica.

  Entre todas las posibilidades que brinda Internet, una de las que más valoradas están entre los *Piratas Informáticos,* es la capacidad de disfrazar el rastro de las comunicaciones con infinidad de mecanismos de lo más variopintos llegando, en algunos casos, a imposibilitar su rastreo.

Además, la diversidad de ataques existentes, el impacto generado, el acceso a todos los recursos necesarios sin necesidad de salir de casa, así como un sinfín más de facilidades, generan una abrumadora cantidad de combinaciones y posibilidades que dejan al libre albedrío de los *Piratas* el *Modus Operandi* a utilizar, tanto, que en ocasiones se llegan a ver auténticas obras maestras del delito online.

- ***Coordinación:*** Simplemente revisando algunos de los casos más sonados en la historia del *Ciberdelito*, no es difícil percatarse de que la mayoría tienen un factor común, son ataques perpetrados por más de un individuo, en algunos casos tantos, que se ha llegado a paralizar el tráfico de todo Internet durante horas (Se hablará más adelante de algunos de estos casos). Esto se debe a que Internet nació con el objetivo de comunicar dispositivos entre sí, por lo que esta comunicación puede ser utilizada para coordinar acciones de una forma mucho más rápida y barata de lo que implicaría dicha coordinación en el mundo real.

  Por otro lado, este punto es muy valorado por algo obvio, a más individuos implicados, mayor dimensión puede llegar a tomar el ataque y en consecuencia los beneficios. Además esto no implica un mayor reparto del beneficio, algo que en el mundo real si sería lógico, puesto que en muchas ocasiones los implicados en los ataques ni siquiera son conscientes de estar involucrados en algo ilegal como es el caso de las *BotNets*.

  En resumen, la facilidad para escalar un ataque a niveles a todas luces inviable en la vida real, hace muy atractivo el delito digital.

- ***Reconocimiento***: Aunque parezca contradictorio, se puede conseguir fama con el delito digital. De hecho los ataques más importantes casi siempre han sacado a la luz al protagonista o protagonistas de los mismos. Además, si se observa el desarrollo de los acontecimientos, es fácil caer en la cuenta de que todos ellos tuvieron, paradójicamente, un gran desenlace para los implicados.

  Un ejemplo de esto es el caso de Kevin Mitnick (del que se hablará un poco más adelante), considerado “el criminal informático más buscado de la historia”, fue un joven estadounidense que consiguió penetrar en la seguridad de corporaciones como Nokia y Motorola, además de robar multitud de información privada. La fama cosechada por su proceso legal y la importancia de sus ataques, le proporcionaron la oportunidad de trabajar como consultor en materia de seguridad y cosecharse un prestigio que a día de hoy, le posiciona como una leyenda de la *Seguridad Informática*.

  La explicación de esto es sencilla, aquel que es capaz de romper los mecanismos de seguridad es porque conoce las vulnerabilidades de los mismos. Evidentemente esta información es muy valiosa para las empresas de cara a reforzar sus sistemas informáticos, por lo que no es difícil entender que se lancen a la caza de estos *Piratas Informáticos* algunas de las mejores entidades informáticas del mundo en busca de sus servicios. La competencia entre dichas organizaciones hace que el protagonista tenga la posibilidad de venderse al mejor postor, a menudo, consiguiendo puestos de alta remuneración y prestigio en las empresas punteras del sector.

- ***Objetivos de alto valor:*** Atacar una entidad bancaria, tumbar alguna infraestructura altamente protegida o intentar acceder de manera ilegal a cantidades masivas de datos, son objetivos que solo puede plantearse, partiendo de una mínima probabilidad de éxito, un *Cibercriminal*.

  La lógica de esto es simple, las infraestructuras críticas de alto valor que emplean las empresas para gestionar el núcleo de su actividad, son componentes prácticamente imposibles de acceder de forma física. Por ejemplo, parece impensable que alguien, evidentemente sin consentimiento, pueda acceder in situ a los servidores de cualquier organismo gubernamental, sin embargo, no parece tan descabellado pensar en un ataque digital masivo mediante *BotNets* con el objetivo de tumbar dicho servidor.

  Es por ello que, cuanto más valioso es el objetivo, más fuerza toma la posibilidad de realizar un ataque digital frente al ataque físico.

Aunque ya se han visto los puntos principales que decantan a un criminal por optar por el *Ciberdelito*, es necesario ser conscientes de la magnitud que pueden llegar a tener estas acciones y la complejidad que alcanzan, para ello es interesante repasar los ataques con ánimo de lucro más famosos.

Algunos de los *Hackers* autores de los siguientes hechos son considerados, a día de hoy, auténticas leyendas de la *Seguridad Informática*.

5.1 Vladimir Levin, el hacker que robó 10.000.000 $

En 1994 el bioquímico y matemático ruso Vladimir Levin consideró que atacar entidades financieras podría reportarle muchos más beneficios de los que obtendría con una vida normal como científico o matemático. Esta decisión, le llevó a optar por atacar, en colaboración con *Hackers* amigos suyos, la red de Citibank, una famosa entidad financiera.

Tras acceder a claves y cuentas de miles de usuarios llegó a transferir hasta 3,7 millones de dólares en menos de una semana a las cuentas del grupo, repartidas en varios países como Argentina, EEUU, Finlandia, Holanda, Alemania o Israel.

El ataque se prolongó durante casi un año hasta que la *Interpol*[1] dio con él en el aeropuerto de Heathrow, en Londres, tras seguir el rastro de su ataque alertados por la propia entidad bancaria tras percatarse de lo extraño de las transferencias que realizaba.

Aunque llegó a demostrarse que había llegado a robar más de 10 millones de dólares (casi 11 apuntan algunas fuentes) y tras declararse culpable por todas las evidencias que apuntaban a ello, fue condenado únicamente a 3 años de prisión y una indemnización de 240.015 dólares.

[1] Organización Internacional de Policía Criminal (http://www.interpol.int/es).

5.2 El ataque a Sony y el robo masivo de cuentas

Entre el 16 y 19 de Abril de 2013, se produjo uno de los ataques más mediáticos de la historia. Un grupo de *Piratas informáticos* perpetraron un ataque contra una de las empresas del ámbito digital y electrónico más conocidas, Sony. Concretamente, los objetivos fueron el servicio PSN[1] y SOE[2].

La idea del ataque era penetrar en estos sistemas con el fin de obtener información confidencial de los usuarios que hacían uso de tales servicios y, lo más reseñable, conseguir las tarjetas de crédito y cuentas bancarias asociadas a los mismos.

En el caso de Playstation Network, se calcula que se vieron afectados unos 75 millones de usuarios de todo el mundo. En cuanto a Sony Online Entertainment, la cifra alcanzó casi los 25 millones.

Todos estos usuarios vieron comprometidos datos como nombre, dirección, email, fechas de nacimiento…etc. y, lo que es peor, sus cuentas y tarjetas de crédito. Esta operación alcanzó tal magnitud, que Sony se vio obligada a cerrar ambos servicios de forma preventiva durante varias semanas.

Tras poner el ataque en manos de la justicia, el propio FBI se encargó de investigar el caso, en lo que se consideró uno de los mayores ataques informáticos de la historia.

La propia multinacional relacionó el ataque a grupos *Hacktivistas* como Annonymous que, aunque rápidamente desmintieron su vinculación, no descartaron que alguno de sus miembros pudiese estar detrás del incidente.

Tras el ataque, la seguridad de Sony quedó en entredicho, así como la confianza de los usuarios en sus servicios, suponiendo un duro golpe en la imagen mundial de la empresa.

A día de hoy, todavía se desconocen a ciencia cierta quienes fueron los responsables del ataque, que se saldó con 100 millones de usuarios afectados y, según algunas fuentes, pérdidas para Sony estimadas en 1.500 millones de dólares aproximadamente.

5.3 Albert González: Operación "Hazte Rico o Muere en el Intento"

En 2008 el *Pirata Informático* Albert González y dos colaboradores suyos efectuaron uno de los mayores robos de datos bancarios de la historia, en la que ellos mismos llamaron la operación "Get Rich or Die Trying" (Hazte Rico o Muere en el Intento).

[1] *Playstation Network.*
[2] *Sony Online Entertainment.*

Los protagonistas, tras realizar un minucioso estudio de vulnerabilidades de las 500 principales empresas aparecidas en la revista "Fortune"[1], decidieron atacar el sistema de pago con tarjeta Heartland Payment Systems y los comercios 7-Eleven Inc. y Hannaford Brothers Co.

El *Modus Operandi* consistía en realizar ataques de tipo *SQL Injection* con el objetivo de penetrar en dichos sistemas y robar datos bancarios que posteriormente serían enviados a servidores de California, Illinois, Letonia, Holanda y Ucrania.

Su intención era vender dichos datos robados a terceros con el fin de que los utilizasen en la realización de compras fraudulentas.

Albert González fue detenido en Mayo de 2008 y condenado a 20 años de cárcel. Hasta su captura llevaba recaudados más de 130 millones de números de tarjeta de crédito y débito.

5.4 Adobe y la divergencia de víctimas

En Octubre de 2013 la empresa de Software Adobe System vio comprometida su seguridad en lo que, a priori parecía un ataque informático más.

En un primer momento la compañía aseguraba que el número de víctimas ascendía a, "solo", 3 millones de usuarios, por lo que el ataque no podía considerarse demasiado relevante en lo que a la historia del *Ciberdelito* se refiere.

Varias semanas después de hacer pública dicha cifra, Adobe salía a la palestra de nuevo para reconocer haber visto incrementada dicha cifra hasta los 38 millones de afectados, 35 más de los estimados en principio. Aunque alarmante la gran diferencia de resultados en apenas unas semanas, el ataque, considerable en cuanto a víctimas, seguía sin destacarse como un gran golpe.

Pero fue en Noviembre de 2013 cuando la empresa de seguridad LastPass, llegó a afirmar que la cifra de víctimas que Adobe exponía estaba irrisoriamente por debajo de la real, que ellos habían estimado en aproximadamente 4 veces más de la asegurada por la multinacional.

Si bien Adobe llegó a reconocer la cifra hecha pública por LastPass, intentó suavizar el problema asegurando que, de esa cifra desorbitada de cuentas robadas, una gran parte pertenecía a *Cuentas Fantasma*. Estas cuentas, siempre según Adobe, estarían en un proceso de eliminación y no supondrían poner en compromiso ningún tipo de información susceptible de ser robada.

No obstante, las explicaciones dadas por Adobe parecieron no convencer a la corporación *PRC*[2]*,* que aseguró que dichas *Cuentas Fantasma* podrían usarse para fraudes de tipo *Phishing* (el cual tratará este documento).

Tras todo el revuelo causado y los problemas acaecidos para Adobe Systems, 152 millones de víctimas vieron comprometidas sus cuentas, donde aparecían contraseñas, direcciones de

[1] Revista Fortune: http://fortune.com/
[2] *Privacy Rights Clearinghouse.*

correo electrónico y cuentas cifradas en lo que, a día de hoy, sigue siendo el tercer mayor ataque *Hacker* de la historia.

5.5 El gran Hack a EE.UU

Sin un nombre oficial debido a la multitud de empresas afectadas, el ataque se prolongó nada menos que 7 años, desde 2005 a 2012, con el objetivo de robar la mayor cantidad de datos bancarios posible de entidades bursátiles, entre ellas NASDAQ, 7-Eleven, JC. Penney, JetBlue, Dow Jones o Global Payment.

Curiosamente, no hay mucha información al respecto pero se sabe que, en total, 160 millones de usuarios vieron como sus datos bancarios pasaban a manos de delincuentes.

Aunque se desconoce quiénes fueron los protagonistas, se detuvieron y condenaron a cinco personas de origen Ruso en lo que fue, hasta 2014, el mayor ataque *Hacker* de la historia.

5.6 Carbanak, ataque financiero mundial

El 15 de febrero de 2015 (en plena elaboración de este documento) salió a la luz lo que parecía un nuevo ataque hacker a entidades financieras internacionales.

La famosa empresa de seguridad rusa *Kaspersky* hizo público un informe donde indicaba que un grupo de *Piratas Informáticos* repartidos por todo el mundo, a los que la empresa denominó *Carbanak*, habían llevado a cabo un ataque a gran escala sin precedentes.

En teoría los atacantes habían accedido a ordenadores de más de 100 bancos repartidos en 30 países, infectándolos con un software proveniente de un *Phishing* que les permitía grabar todo lo que sucedía en los mismos. De esta manera observando como trabajaban los empleados, eran capaces de realizar transferencias de dinero a cuentas falsas sin levantar sospechas, imitando sus actividades diarias. Este ataque fue perpetrado mediante el denominado *Spear Phishing*, una variante que consiste en realizar un *Phishing* de manera personalizada para un pequeño grupo u organización.

Los bancos afectados estaban repartidos entre Europa Oriental y Rusia aunque según afirma *Kaspersky* también intentaron acceder a bancos estadounidenses, asiáticos y del resto de Europa.

En un principio se calcularon pérdidas por más de 300 millones de dólares en un ataque que tuvo su comienzo a finales de 2013, sin embargo, más tarde se confirmó que la cifra alcanzaba los 1000 millones de dólares. Una cifra desorbitada que convertía el ataque más sofisticado realizado hasta la fecha en el mayor robo informático de la historia.

Al cierre de este documento los delincuentes no fueron detenidos y, debido a la reticencia de los bancos por reconocer el ataque y colaborar con las fuerzas legales, el ataque continúa a día de hoy.

Estos cinco ejemplos son solo una pequeña muestra de lo que la delincuencia organizada puede conseguir con un ordenador y una conexión a Internet.

Llegado este punto, ya se puede tener un concepto general de lo que es el *Ciberdelito* y lo que puede llegar a suponer.

Dentro del *Ciberdelito,* una de las ramas que más están proliferando en la última década es la del *Fraude Digital*, en torno al cual gira este documento.

6. Introducción

"El único sistema seguro es aquél que está apagado en el interior de un bloque de hormigón, protegido en una habitación sellada y rodeada por guardias armados".

Gene Spafford (Experto en seguridad).

Así de rotundo se expresaba Gene Spafford, uno de los expertos en *Seguridad Informática* más prestigiosos del mundo cuando se le cuestionaba acerca de cómo conseguir sistemas totalmente seguros.

Aunque en una primera interpretación pudiese parecer que exageraba, no es menos cierto que, a día de hoy, pocos pueden dar una descripción realista de lo que es (o podría ser) un sistema verdaderamente seguro. El porqué, como bien explicaba Gene Spafford (no sin cierta ironía), se debe a que simplemente no existen dichos sistemas, al menos no como se suele entender un sistema seguro en su totalidad.

Y es que con todo el camino andado en el aspecto de la seguridad digital, todavía no se ha dado con la tecla que permita al usuario permanecer totalmente seguros y resguardados de actividades malintencionadas. El principal factor que alimenta esta incapacidad, es el hecho de que el delito digital evoluciona y se modifica tan rápido como las mentes que lo idean aprenden nuevas maneras de atravesar nuestras defensas.

Por ello la única solución viable, al menos actualmente, consiste en mitigar en la medida de lo posible los efectos y las consecuencias producidas por una amenaza vigente. Detectar, identificar, saber analizar y tratar dichas amenazas es de vital importancia a la hora de obtener éxito en esta particular batalla contra el delito informático y es aquí donde este TFG pretende ahondar y arrojar algo de luz en la lucha contra el delito digital, más concretamente en el ámbito del fraude electrónico.

El objetivo principal de este documento es servir como guía o al menos como una referencia sólida para el ámbito empresarial de la S*eguridad Informática* en el campo del *Fraude Digital*.

Con ello se pretende dar una visión clara y actualizada de la situación contemporánea del *Fraude Digital*, así como su evolución y características más reconocibles para facilitar su neutralización.

Dicho fraude se verá reflejado principalmente en la amenaza denominada como *Phishing,* alrededor de la cual gira este trabajo, así como otras amenazas estrechamente relacionadas con este y que en conjunto suponen un peligro mayor, como son los *Troyanos Bancarios*, *Redirectores* y *Scam*.

Una vez trabajado este documento en su completitud se debería obtener una idea completa de los protocolos de actuación ante las amenazas citadas.

Como primer punto se explicarán que medidas preventivas aplicar para evitar ser víctima del *Fraude Digital*, así como los aspectos que se deben tener en cuenta para ello y que precauciones hay que tomar.

En segundo lugar se trabajará profundamente en el aspecto de la detección del fraude (el más importante de los cuatro). Se explicará que se debe saber para poder identificar las distintas amenazas existentes y diferenciarlas. Tras esto se desglosarán las pautas de actuación tras realizar la identificación.

En tercer lugar se detallará el proceso de análisis de la amenaza. En este apartado se hará una breve introducción a las empresas de seguridad, se mostrarán las herramientas que permitirán obtener información de utilidad, se explicará su uso y finalmente se darán consejos para la correcta interpretación de la información obtenida.

En cuarto lugar se mostrará cómo proceder a la eliminación de la amenaza. Se detallará que uso hacer de la información obtenida en el punto anterior, quien o quienes son posibles contactos de ayuda para el caso y como constatar que se ha eliminado satisfactoriamente la amenaza. Como apartado extra y debido a que la experiencia demuestra que no siempre se obtienen los resultados deseados por el camino habitual, se indicará que procedimiento/s alternativo/s tener en cuenta en caso de que la situación se complique más de lo esperado.

Finalmente y a modo de repaso se cerrará el documento con un resumen de todo lo tratado así como una conclusión personal y líneas futuras.

Una vez aclarada la estructura del trabajo a continuación se realizará una introducción sobre el *Fraude Digital* y su evolución que permitirá sentar antecedentes y obtener una base sólida en cuanto a conocimientos a partir de los que trabajar en los puntos a tratar.

6.1 *Fraude Digital* (*Phishing*)

Cuando se habla de *Fraude Digital* se habla de todas aquellas actividades cuyo objetivo es la obtención de datos personales de manera fraudulenta con el fin de conseguir beneficios (principalmente dinero) explotando la información obtenida de manera ilegítima.

La amenaza más visible en este campo es la denominada *Phishing*, un tipo de ataque cuyo objetivo es, como ya se ha comentado, obtener información de los usuarios de manera ilegal a partir de una suplantación de identidad de una empresa conocida por el objetivo.

El patrón de conducta más habitual de este tipo de ataques, consiste en el envío masivo de correos electrónicos hacia víctimas de cualquier localización geográfica, incitando a las mismas a entrar en un enlace incluido en el correo, que redirige hacia una página fraudulenta cuya estética es idéntica a la de la identidad a suplantar. Una vez ahí, se intenta convencer en el cuerpo del correo de que la víctima facilite sus datos personales en dicha web con algún motivo (falso por supuesto) que incite a ello y así obtener las credenciales de la víctima y poder hacer un uso ilegítimo de las mismas por parte de los atacantes (*Phishers*).

Otra variante de conducta consiste en la utilización de *malware* (principalmente *Troyanos*) que permitan el robo directo de credenciales tras infectar el ordenador objetivo.

Como última variante, el *Phishing* se vuelve más difícil de detectar cuando se combina con *Redirectores* que generan flujos de navegación alternativos, dificultando en extremo la identificación y localización del fraude.

En cuanto a su origen, los primeros ataques mediante este tipo de amenaza datan aproximadamente de los años 90, si bien se extendieron e hicieron bastante más famosos algunos años más tarde. En España no se tuvieron noticias de estos tipos de ataque hasta el 2004, cuando empezó a proliferar el *Ciberdelito* relacionado con el fraude.

A día de hoy el *Phishing* está plenamente extendido a lo largo de todo el mundo y es una de las principales amenazas a erradicar sobre todo por entidades bancarias, que son las que se ven más afectadas por dicha actividad delictiva.

El fenómeno del *Phishing* ha evolucionado tanto tras todo este tiempo, que no sería correcto hablar únicamente de *Phishing*. El fraude on-line actual ya no utiliza únicamente el correo electrónico o los mensajes de tipo *spam* como método de difusión. De hecho los detectores de *spam* en muchos casos ya son incapaces de detectar este tipo de actividades. Además ya no se basan únicamente en la relación de confianza empresa-usuario explotada hasta ahora y desde hace tiempo dejaron de utilizar el correo electrónico como medio de transmisión para dar paso a mecanismos mucho más complejos.

Las constantes mejoras y evoluciones tecnológicas hacen que estas amenazas se modernicen en consonancia, aprovechando todas las facilidades de las que hoy en día disponen para intensificar su capacidad de actuación e incrementar su alcance en gran medida.

Además aparecen nuevas amenazas que, en colaboración con el *Phishing*, hacen de este un arma muy poderosa y realmente difícil de combatir. Estas amenazas son, por ejemplo, *Troyanos Bancarios*, *Redirectores* y, en menor medida, el *Scam* (o abuso de marca). Todas estas variantes que por separado son peligrosas pero que en conjunto, lo son mucho más, impiden la detección temprana del fraude y provocan que la educación sobre este sea cada vez menos efectiva.

Por todo ello es estrictamente necesario que los mecanismo de detección de estas amenazas estén actualizadas, adaptándose a las nuevas generaciones y con ello actualizándose en la misma medida que lo hacen las estafas.

Actualmente la lucha contra el fraude digital no se centra únicamente en la detección del mismo, sino en prestar atención y saber reaccionar a los cambios que este sufre en el proceso de tratamiento mientras permanecen activos. Hace tiempo, el fraude aparecía, se propagaba, se detectaba, se eliminaba y desaparecía. Las diferentes técnicas de evolución contemporáneas hacen que esto ya no sea posible y que se deba de utilizar otra metodología de actuación.

Un fraude moderno es capaz de utilizar docenas de *IP* cambiantes en poco tiempo, reenviando la información robada a diferentes localizaciones geográficas de manera prácticamente simultánea. Por ello es estrictamente necesario prestar atención a cualquier modificación o alteración en el comportamiento de la amenaza, para poder actuar a tiempo y ser capaces de contrarrestarla obviando las medidas obsoletas y generando o aprovechando nuevas medidas que, para resultar efectivas, también deben cambiar con rapidez en consonancia a la amenaza.

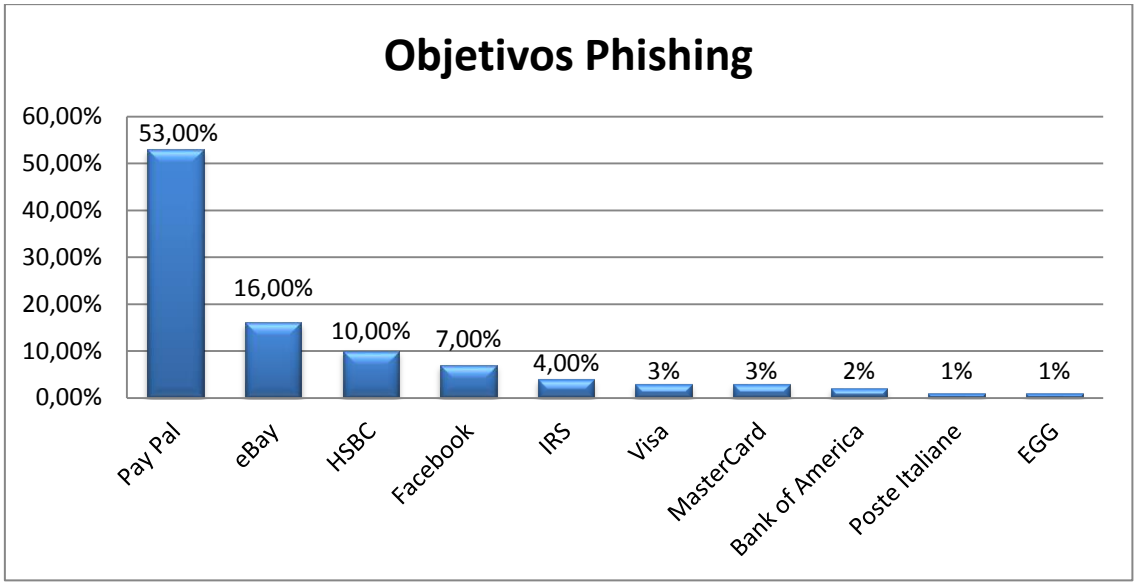


Ilustración 1: Gráfica de objetivos de Phishing (Datos de 2014)[1].

En cuanto a los objetivos de este tipo de *Ciberdelito*, hace tiempo se podría decir que solo grandes empresas solían ser principales objetivos de estos ataques. Sin embargo, en los últimos años estos ataques han ido dirigidos a diversas entidades de modo paralelo, avisando de que nadie está libre de riesgo. Donde hace unos años, el principal objetivo era el sector financiero, ahora se sabe que, prácticamente cualquier empresa que realice transacciones por Internet, se convierte en posible presa de estos ataques, incluso ONGs pueden ser víctimas del *Phishing* en procesos de recaudación de gran magnitud. No obstante las entidades financieras y los bancos siguen siendo, por mucho, la lista de objetivos más rentables del *Fraude Online*, mientras que las plataformas de pago suelen ser los objetivos más comunes.

Geográficamente hablando, estos objetivos se localizan principalmente en Rusia, seguido por Estados Unidos e India, posicionándose los mismos muy arriba en el ránking de víctimas, muy por encima por ejemplo, de España.

[1] Fuente: S21Sec. Elaboración Propia.

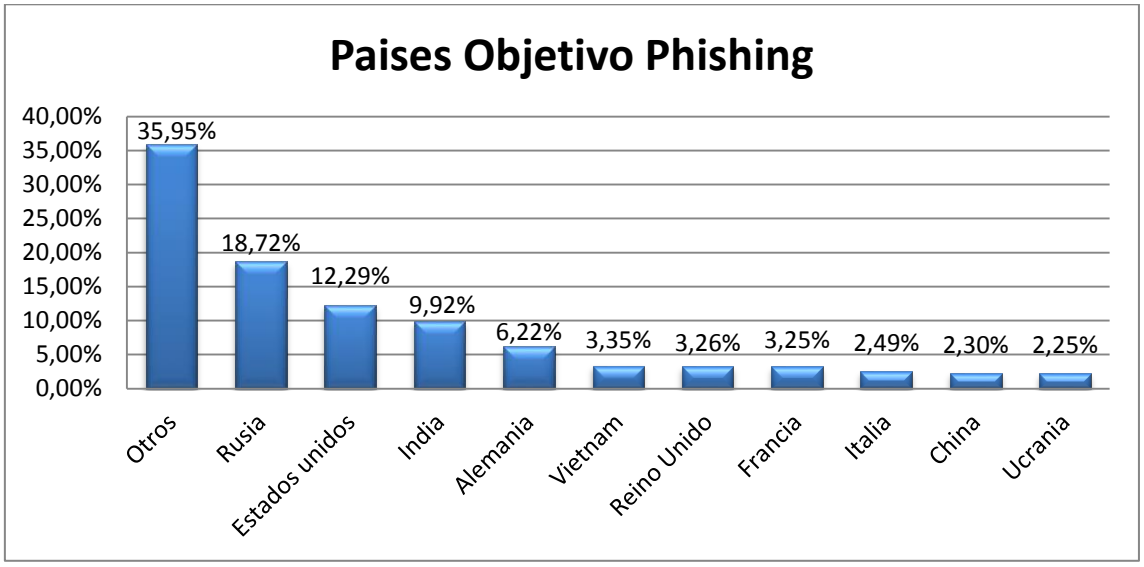


Ilustración 2: Grafica países objetivo Phishing (Datos de 2013[1]).

Por otro lado el país que más *Fraude Online* produce es, con diferencia, Estados unidos. Esto se debe a que América contiene la mayor parte de *ISP* (Internet Service Provider) del mundo y esto favorece el alojamiento de páginas web fraudulentas.

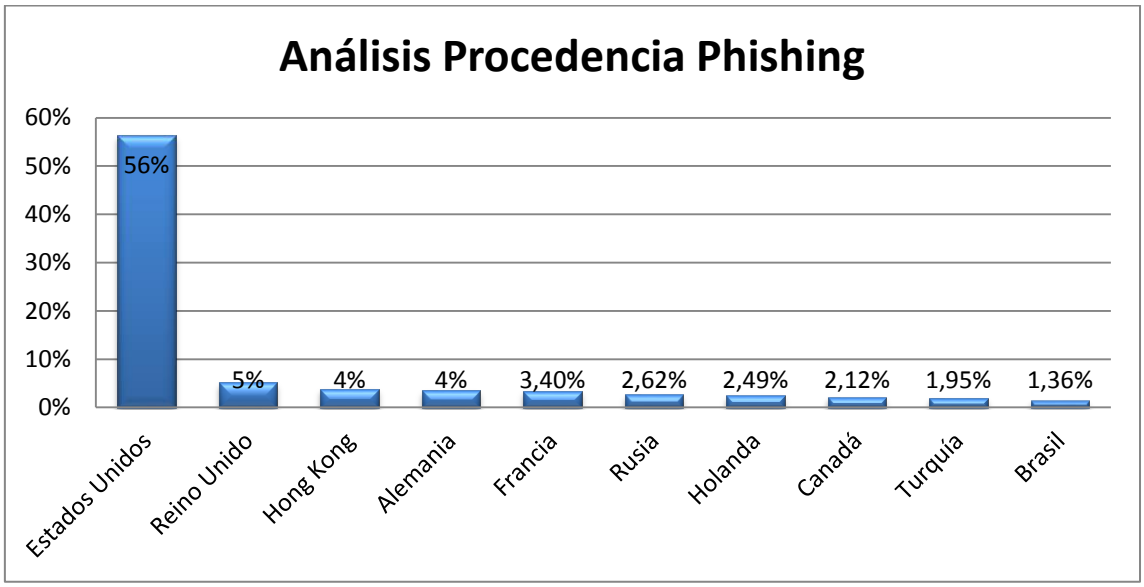


Ilustración 3: Gráfica de procedencia de Phishing (Datos de 2014[1]).

[1] Fuente: S21Sec. Elaboración Propia.

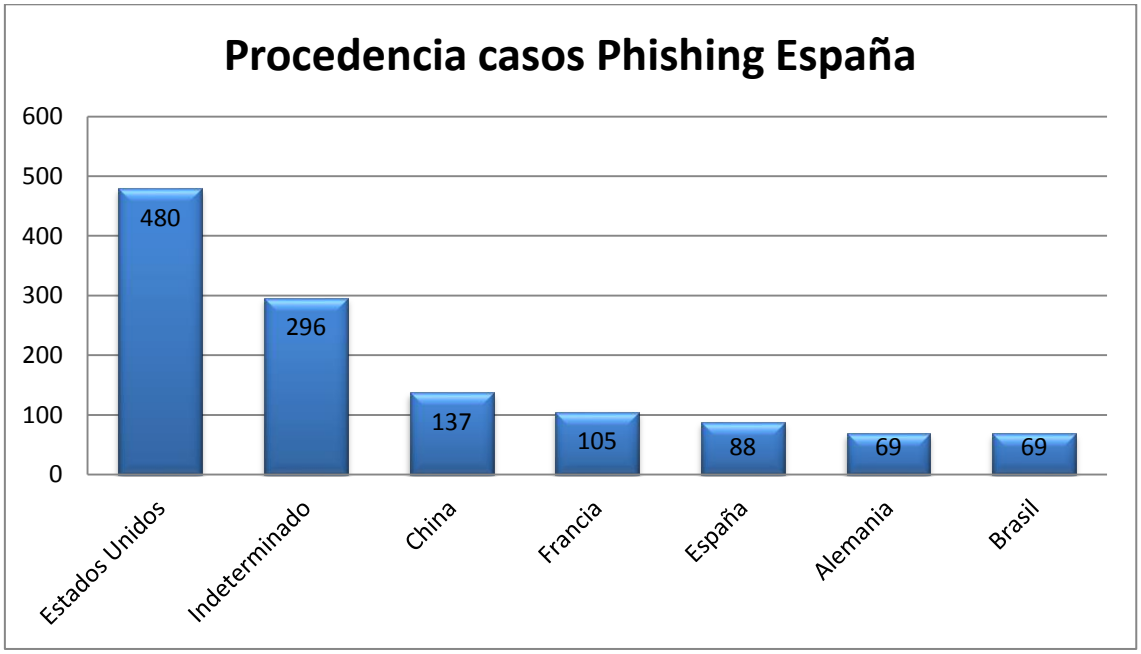


Ilustración 4: Gráfica de procedencia de casos españoles Phishing (Datos de 2010[1]).

Como sus principales benefactores, se habla de que prácticamente un 36% de los casos de fraude (datos de 2011) provenían de mafias rusas, las cuales, obtuvieron ganancias por valor de 4500 millones de dólares. En 2014, Rusia sigue liderando este particular ránking, con la creciente presencia en los últimos tiempos de Nigeria, un país que, debido a sus débiles leyes contra los delitos informáticos y la falta de departamentos gubernamentales (CERTs) que sean capaces de preservar la seguridad de los usuarios, cada vez está obteniendo más relevancia en este campo del *Ciberdelito*.

En definitiva el *Fraude Digital* (o *Phishing*) es un problema que se acrecienta según pasa el tiempo y que cada vez mantiene en jaque a más entidades (principalmente financieras), así como a los organismos encargados de contrarrestarlo.

6.2 *Dominios* afectados

En cuanto a los dominios, evidentemente, no todos se ven afectados por igual. Se puede ver una dependencia muy grande del *Phishing* en función de si dispone de un *gTLD*[2] o de un *ccLTD*[3]. Los dominios poseedores de un *gTLD*, en concreto los dominios *.com*, *.net* y *.org*, abarcaron más del 60% de los casos en 2014[4]. El resto de *Phishings* se concentraron en unos pocos *ccTLD* como los dominios procedentes de Brasil, Nueva Zelanda y Palau que abarcaron un 7% de los casos.

[1] Fuente: S21Sec. Elaboración Propia.
[2] *Generic Top Level Domain* o *Dominio de nivel superior genérico.*
[3] *Country code Top Level Domain* o *Dominio de nivel superior geográfico.*
[4] Fuente: APWG (Anti Phishing Working Group).

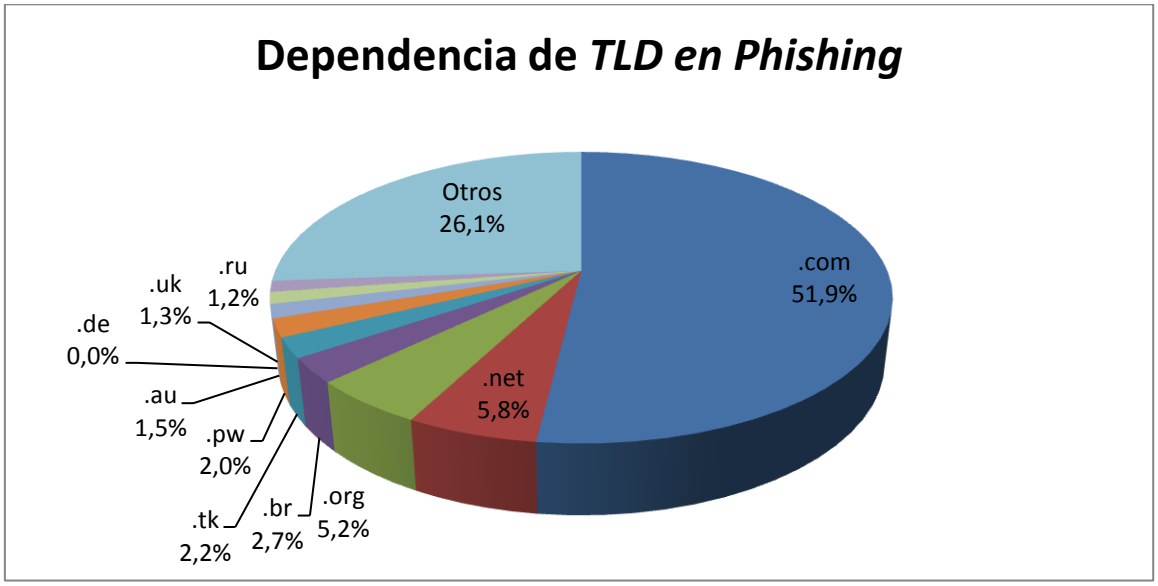


Ilustración 5: Gráfica de dependencia de *TLD* en los *Phishing* (Datos de 2014)[1].

6.3 Evolución del *Fraude Digital*

En los últimos años los ataques mediante *Phishing* han crecido de manera alarmante, aumentando en los últimos años hasta 87%, esto se traduce en que aproximadamente unos 37 millones de víctimas a lo largo de todo el mundo fueron afectadas por esta amenaza entre 2012 y 2013.

Gran parte de la culpa de este aumento la tienen el paso del *Phishing* tradicional al *Phishing* moderno.

Mientras que al principio y durante algún tiempo, los ataques consistían en una página web fraudulenta con contenido suplantado fácilmente detectable por su *Uri*[2] (se hablará de ellas en la sección dedicada a la *Plataforma de Seguimiento*) ilegítima, de un tiempo a esta parte se ha convertido en una amalgama de mecanismos y combinaciones de ataques que impiden, cada día más, su detección y eliminación.

De todas esas evoluciones, sin duda, la más dañina y famosa son los llamados *Troyanos Bancarios*.

Estos *Troyanos*, en contra de lo que se pueda pensar, no disponen de mecanismos de ataque complejos sino todo lo contrario. Al principio basaban su eficacia en la técnica denominada como *Keylogger*, que permitía al *Troyano* capturar las claves que el usuario iba introduciendo por teclado al conectarse a algún tipo de entidad que requiriese de credenciales.

No obstante la proliferación de teclados virtuales, tanto en los propios ordenadores personales, como en las mismas webs, anuló por completo la efectividad de dicha técnica y los

[1] Fuente: APWG (Anti Phishing Working Group). Elaboración Propia.
[2] Uniform Resource Identifier.

Troyanos se vieron en la obligación de evolucionar, de tal manera que, hoy en día, los *Troyanos* siguen siendo capaces de capturar las contraseñas que el cliente introduce, independientemente de si usa un teclado virtual o no.

Las técnicas que permiten esto son tan variadas y cambiantes que se calcula que aparece un nuevo tipo de *Troyano Bancario* cada semana aproximadamente.

Con todo esto, no es difícil dilucidar que las empresas de seguridad, así como las propias entidades víctima de estas amenazas, no dan abasto para gestionar tal cantidad de *Troyanos Bancarios* consiguiéndose tratar, solamente, una ínfima parte de todo el flujo de ataques generado.

Además y por si fuera poco, debido a la poca información obtenida y la gran variedad de tipos que existen, no se ha conseguido realizar un protocolo de actuación eficaz contra estas amenazas. Al ser tan difícil averiguar los mecanismos que emplean en su labor de ataque, las entidades se ven limitadas en cuanto a su capacidad para inmunizarse al respecto. Esto unido a que la amenaza evoluciona constantemente, hace que cada vez, las distancias entre lo analizado y lo existente sean mayores.

En cuanto a los casos denunciados a las empresas por ataques de este tipo desde 2005 hasta nuestros días, se habla aproximadamente de más de 30 millones de reportes en total[1], lo cual posiciona al *Phishing* como uno de los agentes de ataque informático más activos, más populares y más a tener en cuenta en los últimos 10 años.

Más específicamente, el *Phishing* tuvo una clara progresión ascendente hasta tocar techo en 2009 (año en el que se detectaron más de 400.000 casos[1]), momento en el cuál la tasa de casos reportados empezó a bajar y a mantenerse estable durante el siguiente trienio hasta llegar a 2013, cuando se registró el pico de casos denunciados más alto hasta la fecha (aproximadamente unos 450.000 casos[1]) incluido el récord de casos reportados en un mes (aproximadamente unos 50.000 casos en Julio de 2013[1]).

Ilustración 6: Evolución casos de Phishing reportados 2005-2014 (Datos anuales[1]).

[1] Fuente: APWG (Anti Phishing Working Group).

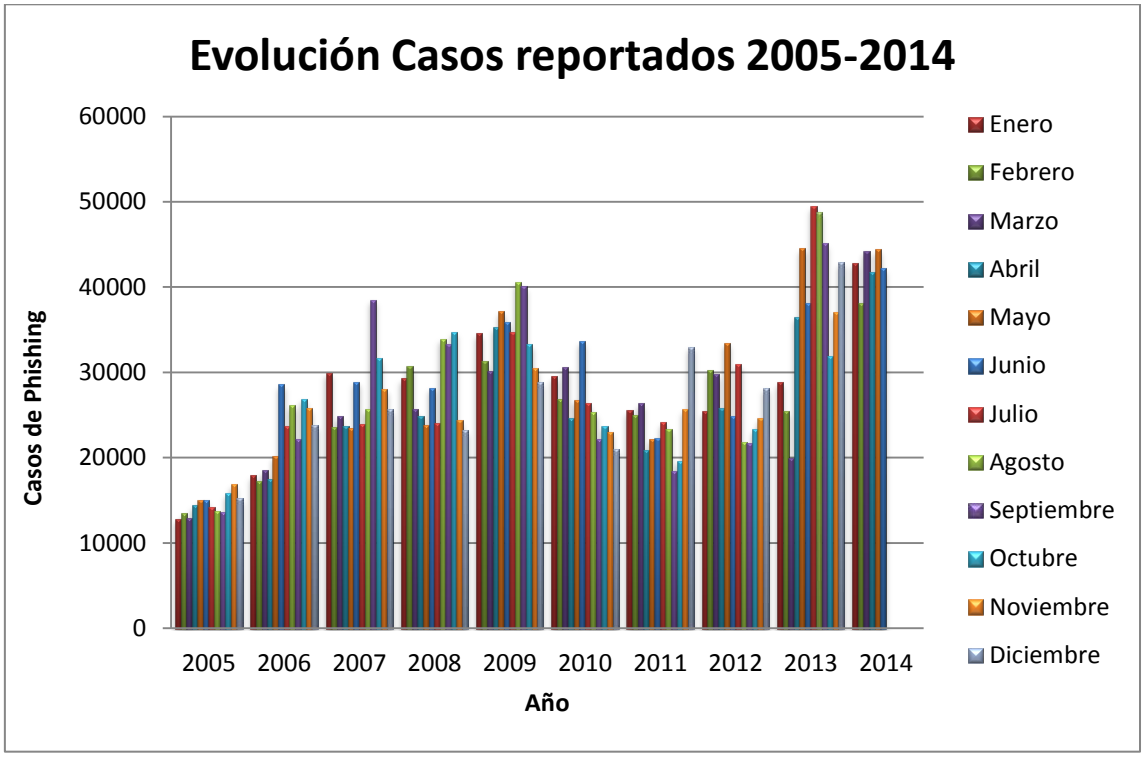


Ilustración 7: Evolución casos de Phishing reportados 2005-2014 (Datos mensuales[1]).

Como conclusión, se puede afirmar que el *Phishing* se encuentra actualmente en su punto de máxima expansión desde que se conoce su existencia y además, muestra indicios de que esto se verá acentuado cada vez más.

[1] Fuente: APWG (Anti Phishing Working Group). Elaboración Propia.

7. Prevención

Una vez entrados en materia, se pasarán a explicar los aspectos más importantes a la hora de evitar ser víctimas de estos fraudes o *Phishing*.

Para empezar cabe indicar que, prevención como tal, no existe, es más bien una manera de salvaguardarse ante un intento de estafa y evitar caer en las trampas de los *Ciberdelincuentes* ya que no hay manera real de evitar que nos lleguen los "cebos" en forma de, por ejemplo, los famosos correos ya citados.

En este apartado se dará información relevante y consejos sobre la manera de proceder en entornos digitales susceptibles de ser suplantados como por ejemplo bancos o plataformas de pago online.

A continuación se tratarán los aspectos a tener en cuenta para evitar ser estafados.

7.1 Información básica para la prevención

Hay que recalcar que, la mayoría de víctimas del *Phishing* son estafadas debido a una falta de información grande en cuanto a su entorno digital y el de la empresa suplantada, independientemente de lo bien elaborado que esté el fraude.

Con unos mínimos conocimientos sobre los protocolos de actuación online de las empresas y del propio fraude en sí, se evitarían gran parte de los casos reportados.

Por ello se van a mostrar algunos datos interesantes de los *Phishing*, así como medidas generalmente comunes a las empresas a la hora de prevenir una estafa. Lógicamente cada empresa tiene unas metodologías propias, por lo que los siguientes puntos se centrarán en aspectos generales que todas suelen emplear.

- En primer lugar hay que tener en cuenta que ninguna entidad financiera (las más suplantadas) pide las credenciales a sus clientes bajo ningún motivo y menos en un entorno tan inseguro como podría serlo un correo electrónico. En un hipotético caso de que fuera necesario algo así, la entidad se pondría en contacto personalmente con el cliente y siempre salvaguardando su privacidad.
- Cualquier empresa con *Dominio* web es susceptible de ser suplantada, no existen las web infranqueables, por lo tanto es necesario estar alerta siempre. Aunque es cierto que las empresas más importantes toman precauciones para evitar esto en la mayor medida de lo posible, no es menos cierto que esto no es fiable por completo y que la única manera de navegar seguro es ser desconfiado.
- Hechos como teclear directamente desde el navegador la *Uri* de una empresa suele dar la falsa confianza al usuario de que está entrando a un *Dominio* legítimo cuando no tiene por qué ser necesariamente así. Existen mecanismos de ataque como por ejemplo el *Pharming* (ver Anexo) que se encargan de redireccionar las direcciones web

que el usuario introduce a otras que el *Pirata Informático* haya establecido, llevando a cabo igualmente su estafa.

- Un *Phishing* no es un virus, al menos no en su forma más básica (más adelante se tratarán las variantes con *Troyanos* que si actúan como tal), por lo tanto el hecho de tener un *AntiVirus* actualizado y un ordenador protegido no implica en absoluto estar exento de estafas. El *Phishing* se denomina *Ingeniería Social* (Hack Story, 2013) debido a que su poder reside en la redifusión y en la capacidad de engañar al usuario, no en la infección de equipos.
- Como ya se ha dicho en la introducción el *Phishing* no tiene una tipología de objetivos fijo, la creencia de que una empresa, por pequeña que sea, está excluida de este tipo de ataques, es falsa y sumamente peligrosa. Cualquiera puede ser suplantado.
- En el punto opuesto al anterior, las webs más populares o visitadas (redes sociales) y las entidades que manejen caudal monetario procedente de sus clientes son siempre puntos calientes de este tipo de estafas, por lo que hay que maximizar las precauciones y ser sumamente cuidadoso con el trato que se les da.
- Es recomendable estar al día en la medida de lo posible de las amenazas que van surgiendo principalmente en aquellos entornos en los que el usuario se mueva habitualmente. Gran cantidad de empresas de seguridad utilizan blogs para dar a conocer al público nuevas formas de estafa en estos ámbitos, alertando a los usuarios y explicando las medidas que llevar a cabo para evitarlos. Cuanta más información se obtenga en este campo, más rápidamente se podrá identificar y evitar cualquiera de estos fraudes.
- Es vital conocer y saber interpretar lo que dice el navegador de las páginas que se visitan, a menudo las señales para detectar un fraude las da el propio navegador y por falta de entendimiento o desconocimiento al interpretarlas son ignoradas.

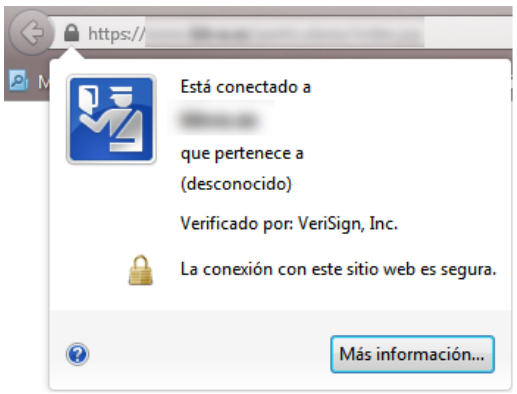


Ilustración 8: Acceso a información de certificado de una página web.

- En el supuesto caso de detectar un fraude y ser un particular sin conocimiento en la materia, es recomendable alertar a la empresa suplantada para que traten el problema (Ver Detección – Como actuar). La mayoría de las veces reportan el caso a empresas de seguridad especializadas que darán de baja dichos fraudes en pocas horas/días. Con esto a parte de sacar de la red el fraude, se estará evitando que otras personas caigan engañadas por él.

La mayoría de empresas (y absolutamente todos los bancos) cuentan con un apartado de contacto al que se pueden denunciar estos casos, dichos contactos suelen estar vinculados a un departamento de abuso (se hablará de ellos en el apartado Eliminación) que suele ser el que da nombre al correo y que se encarga de la gestión de fraudes. En caso de no existir tal departamento se puede dar uso de alguna herramienta de tipo *WhoIs* (se hablará de ella en el apartado de Análisis) para obtener otras vías de comunicación. Si aun así no se encuentran contactos especializados, el contacto habitual debería bastar.

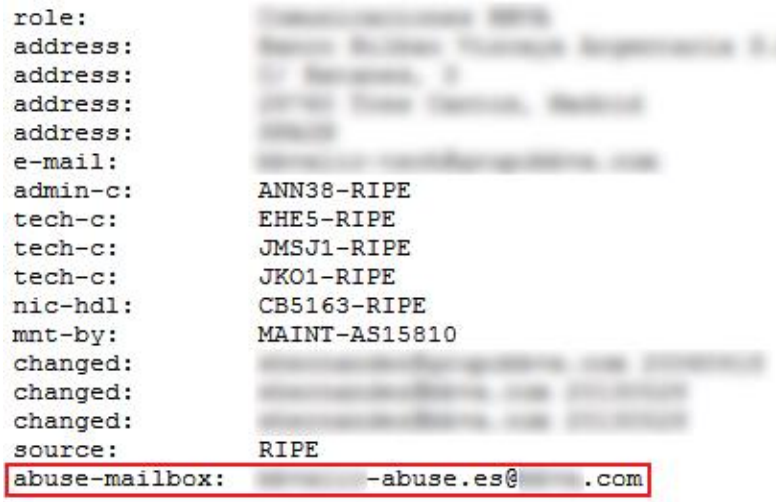


Ilustración 9: Correo de abuso obtenido mediante Whois.

Para concluir este apartado, decir que, simplemente, trabajar con aplicaciones que se conozcan, saber interpretar la información que se muestra y ser cautos en todos los movimientos que se realicen, minimizan en gran medida las probabilidades de caer en una de estas trampas.

En contra de lo que se suele pensar, evitar ser estafados en el mundo digital, no implica unos conocimientos exhaustivos sobre informática ni es algo solo al alcance de unos pocos especializados en la materia. La educación en la seguridad online es un aspecto al alcance de cualquiera y que el usuario medio suele infravalorar, lo cual favorece la proliferación de estos engaños.

7.2 Precauciones a tomar

Ya se ha visto lo que se debe saber a la hora de trabajar en entornos potencialmente inseguros, ahora se van a mostrar algunos consejos útiles para evitar ser estafados.

No hay que olvidar que ser víctimas de un *Phishing* no es sino la consecuencia de las malas decisiones del usuario. Un usuario informado, consciente de los peligros y que siga los siguientes consejos, en principio, no debería ser víctima de ningún tipo de *Fraude Online*.

Por otro lado cabe recalcar que estos consejos son útiles actualmente, pero en un futuro no muy lejano, probablemente algunos de ellos queden obsoletos debido a que el *Phishing* trabaja con mecanismos de engaño que se adecúan a los tiempos y se modifican en función de las precauciones que toman los usuarios.

- Como punto de partida, el consejo más importante que se puede dar es que ser desconfiado es una virtud en lo que a seguridad online se refiere. Nunca hay que bajar la guardia simplemente porque se navegue en un entorno que, a priori, se muestra como seguro. Al fin y al cabo, el usuario no sabe que vulnerabilidades caracterizan las páginas por las que navega, por lo tanto, aplicar una confianza ciega es un grave error. Generalmente los casos de *Phishing* en las entidades bancarias internacionales suelen ser de un gran nivel, siendo a simple vista, imposible de diferenciar de la web legítima, por ello fiarse de lo que se ve es un fallo muy habitual a la vez que grave.
- Es recomendable verificar las fuentes de origen de todas las informaciones que lleguen al usuario relativas a cuentas personales bancarias en forma de correo electrónico. El email es un medio muy poco habitual (por no decir obsoleto) para la notificación personal por parte de un banco. El correo físico o el contacto telefónico suele ser lo más utilizado en esos casos, por lo tanto lo mejor es desconfiar del correo electrónico y si es posible, buscar información al respecto por Internet, a menudo se encuentran casos similares de otras personas que ayudan a decidir si el mensaje es un cebo de *Phishing* o no.
- Mantener un control estricto de todos los movimientos de las cuentas bancarias es una buena forma de identificar si ha habido movimientos sospechosos para evitar futuros fraudes.
- En caso de haber detectado un intento de *Phishing,* es recomendable que el usuario guarde el correo o alguna captura de pantalla en alguna carpeta dedicada para ello, así en caso de volver a recibir cebos de la misma entidad puede comparar con casos que ya haya recibido e identificar el fraude más rápidamente.
- Aunque no es completamente seguro, es recomendable ingresar a las web de entidades financieras desde el propio navegador e ignorar cualquier enlace que se obtenga por otros medios. Aunque como ya se ha explicado este método no es del todo fiable debido al *Pharming*, es bastante menos habitual ser estafados por este método por su complejidad.
- Si algo no resulta familiar o es incoherente es preferible no arriesgarse y contactar directamente con la empresa en cuestión.
- Evitar en la medida de lo posible cualquier dirección web que no se corresponda a un protocolo de navegación segura como pueda ser el *HTTPS*, todas las plataformas de pago online y entidades financieras utilizan dicho protocolo en sus webs y el propio navegador muestra información al respecto.

Ilustración 10: Página web con protocolo *HTTPS*.

- Desconfiar especialmente de la información que llegue masificada y que no se dirija al usuario en particular.
- El *Phishing* no solo actúa online, los teléfonos asociados a un correo también pueden ser una trampa.
- Siempre que se pueda, utilizar teclados virtuales para introducir credenciales en las webs seguras. Aunque este método es inútil en caso de estar en una web suplantada, si es eficaz en caso de ser víctimas de virus (*Troyanos Bancarios*) que utilizan *keyloggers* para capturar las claves personales.

Ilustración 11: Teclado virtual de una famosa marca de *AntiVirus*.

- Mantener el *AntiVirus* actualizado y realizar análisis del equipo cada cierto tiempo, no previene el *Phishing* en su forma más básica, pero si mantendrá el ordenador libre de virus o *Troyanos* derivados del mismo.

En definitiva y a modo de resumen, ser precavidos, actuar solo cuando se tenga plena seguridad de lo que se hace y ser cuidadosos es la mejor manera de evitar ser estafados.

8. Detección

A continuación se van a mostrar las claves que permitirán identificar un *Phishing*.

Estas claves se centrarán en características comunes, comportamientos, medios de contacto con el usuario, incoherencias con la política de la empresa suplantada…etc.

Hay que decir que todo lo que se va a mostrar son elementos característicos de cualquier *Phishing*, lo cual no quiere decir que sean las únicas características que poseen, ya se ha explicado que el carácter cambiante de este tipo de fraude hace que las técnicas evolucionen y sea posible encontrarse con casos en los que se hayan aplicado técnicas más sofisticadas. No obstante, con lo aquí mostrado se podrán identificar casi la totalidad de los fraudes que circulan a día de hoy por Internet.

Tras mostrar las características básicas de un *Phishing* se indicará como se debe proceder en caso de ser un usuario medio ya que el resto del documento estará enfocado a los profesionales del sector debido a la complejidad en el manejo y entendimiento de las herramientas que se van a utilizar tanto en el análisis como en la eliminación.

8.1 Características del *Phishing*

Los parámetros que se van mostrar a continuación son los más comunes en estos casos y además no requieren de especialización por parte del usuario, no es necesaria (a priori) ninguna herramienta sofisticada ni unos conocimientos avanzados para poder detectarlas. Es por eso que la detección de un *Phishing* es, en principio, una labor al alcance de cualquiera y no únicamente de personal especializado.

Como el correo electrónico sigue siendo uno de los medios favoritos para captar víctimas se va a mostrar el perfil que suele tener un correo fraudulento con enlace a un *Phishing* bancario.

En primer lugar hay que decir que suelen ser correos con un encabezado en el que destaca el logo de la empresa y que intentan alarmar de alguna manera al usuario con falsas justificaciones, como por ejemplo, una actualización en la base de datos de la empresa que puede dejarle fuera en caso de no notificar sus credenciales, la pérdida de algún beneficio del que estuviese gozando o del que pudiese empezar a gozar…etc.

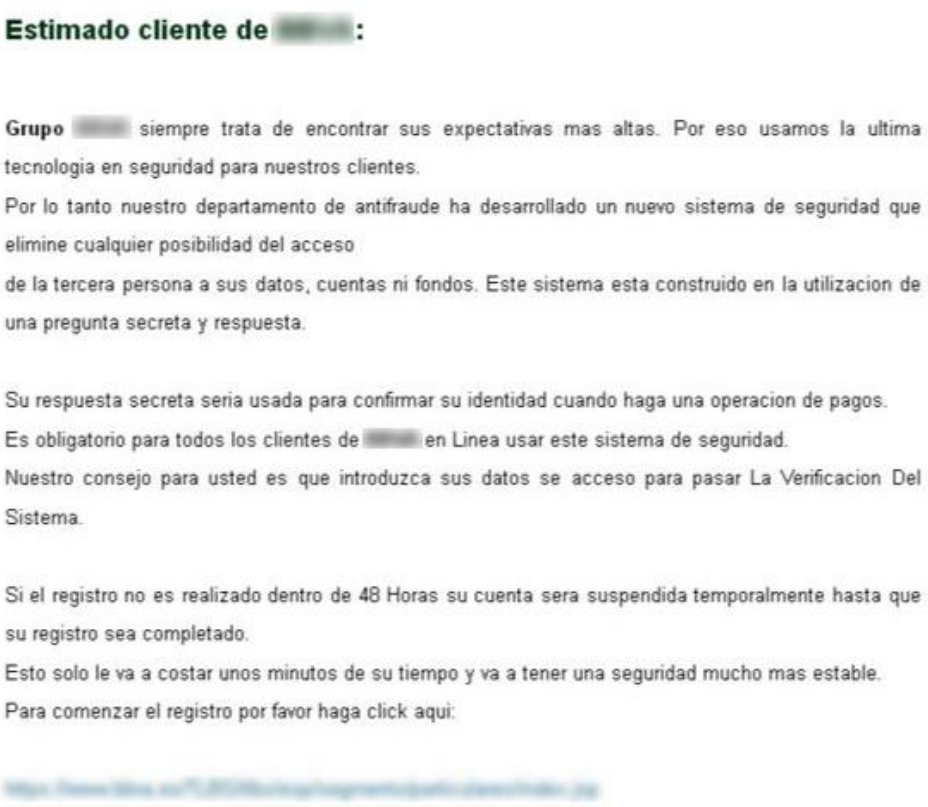
Esto que a priori no parece demasiado importante, es la clave para hacer que un usuario sea víctima de la estafa, pues con esto se consigue presionar al usuario y evitar que piense con claridad, precipitándose, probablemente, a una decisión prematura y errónea como es la de facilitar los datos personales. Además algunas veces dan poco margen de tiempo a la víctima para poder enviar su información de cuenta, por lo que esto acentúa más el nerviosismo y la presión.

Hay que recordar que ninguna entidad bancaria se pone en contacto por correo electrónico para algo tan importante como una obtención de credenciales, básicamente porque ningún

banco le pide las contraseñas a sus clientes y menos en un entorno tan inseguro. No obstante ante la duda, lo mejor es contactar directamente con la empresa.

De hecho es poco probable que le lleguen correos a un usuario de su entidad bancaria, a menos que se haya suscrito, previa autorización, a un plan de notificaciones de la misma.

A continuación un ejemplo:



Estimado cliente de [redacted]:

Grupo [redacted] siempre trata de encontrar sus expectativas mas altas. Por eso usamos la ultima tecnologia en seguridad para nuestros clientes.
Por lo tanto nuestro departamento de antifraude ha desarrollado un nuevo sistema de seguridad que elimine cualquier posibilidad del acceso
de la tercera persona a sus datos, cuentas ni fondos. Este sistema esta construido en la utilizacion de una pregunta secreta y respuesta.

Su respuesta secreta seria usada para confirmar su identidad cuando haga una operacion de pagos.
Es obligatorio para todos los clientes de [redacted] en Linea usar este sistema de seguridad.
Nuestro consejo para usted es que introduzca sus datos se acceso para pasar La Verificacion Del Sistema.

Si el registro no es realizado dentro de 48 Horas su cuenta sera suspendida temporalmente hasta que su registro sea completado.
Esto solo le va a costar unos minutos de su tiempo y va a tener una seguridad mucho mas estable.
Para comenzar el registro por favor haga click aqui:

[redacted]

Ilustración 12: Ejemplo de email fraudulento asociado a un *Phishing*.

Como se puede observar el mensaje comienza intentado tranquilizar al usuario con la premisa de que se está intentado preservar su seguridad. Obviamente esto es falso, pero consigue generar un estado de confianza en el mismo de cara a la segunda parte del mensaje donde se procede al engaño.

Además en este caso en particular al usuario se le da muy poco margen de tiempo, solo 48 horas para proceder, lo que probablemente sea suficiente para provocar que un usuario ajeno a este tipo de fraudes se precipite y caiga en la trampa.

Además, el mensaje también suele contener palabras técnicas que confundan a la víctima de tal manera que, en muchas ocasiones, el usuario es estafado sin siquiera saber el verdadero motivo del mensaje.

Por otro lado otro punto a tener muy en cuenta es el remitente del mensaje. Normalmente estos mensajes son enviados desde cuentas falsas que intentan emular al remitente legítimo o

simplemente son correos normales y confían en que el usuario no se moleste en comprobarlo. Este es el indicativo más claro de que se está ante un caso de email fraudulento, si el remitente no cuadra con ningún correo oficial de la empresa legítima ya se puede afirmar que es un caso de *Phishing*.

El problema reside en que, obviamente, es complicado conocer todos los correos oficiales de un banco o entidad por lo que no se puede estar seguro de si el remitente es legítimo o no. Para ello lo mejor es, de nuevo, contactar con la empresa directamente para verificar si existe algún departamento con ese correo.

Lógicamente y como primer paso antes de contactar con la empresa, si el *Dominio* del correo es desconocido o no está relacionado con el nombre de la empresa, se puede calificar el mensaje como ilegítimo y proceder a su reportación o eliminación.

Hay que destacar que los casos de *Phishing* actuales suelen enmascarar el remitente de tal manera que simulan un correo legítimo de la empresa, por lo tanto a simple vista no se podría declarar como fraudulento y habría que tener en cuenta el resto de puntos.

Ilustración 13: Remitente falso en un correo fraudulento de BBVA.

Otro aspecto importante a tener en cuenta, es la redacción del mensaje. Es frecuente encontrar erratas o faltas de ortografía que alerten al usuario de que no se encuentra ante un mensaje legítimo, pues resta profesionalidad y credibilidad al mismo, incluso la manera de expresar puede dar pistas de ello. Además, el idioma también puede ser una pista, cualquier mensaje que llegue en un idioma diferente al habitual, también es un indicio de que se está ante un cebo *Phishing*.

También es común recibir mensajes donde el texto este embebido en una imagen. Esto es frecuente debido a que si el texto fuera real, el propio gestor de correo probablemente desechase el correo a la carpeta de no deseados, por lo tanto es recomendable desconfiar de las imágenes en correos corporativos.

Para finalizar el análisis del contenido del mensaje, es importante fijarse en la firma del mismo. Si el mensaje no ha sido firmado por algún departamento perteneciente a la empresa legítima, el correo no es de carácter corporativo, por lo que debería ser desestimado.

Independientemente del mensaje es importante comprobar si el correo dispone de archivos adjuntos. Es poco probable que una entidad importante asocie archivos a sus correos, por lo que, en la medida de lo posible, es recomendable intentar analizar con alguna herramienta dichos archivos en busca de virus o malware que pueda infectar el equipo (*Troyanos Bancarios*).

Por otro lado es importante analizar también que tipo de enlace contiene el correo suponiendo que no se haya podido dilucidar si es un email fraudulento, por las características anteriores.

Hay que decir que la información mostrada a continuación es vital en caso de haber llegado a una página potencialmente fraudulenta por medios propios y no a través de un correo o cualquier otro tipo de ingeniería social. Esto se debe a que al no tener un referente previo como es el cuerpo del mensaje en el caso anterior, no se pueden sentar antecedentes que pongan sobre aviso al usuario de que lo que va a visitar puede ser una web ilegítima.

Además las características que se van a exponer son las que realmente van a delatar un caso como fraudulento, pues, hasta ahora, lo único que se han obtenido son indicios y sospechas que, obviamente, hay que ratificar, sobre todo, en caso de querer reportar el caso, ya que por sí solas no son un argumento válido para poder dar de baja una *Uri*.

Para empezar y como ya se ha indicado, en los casos de las entidades más famosas, una página que suplante su identidad es, a la vista, imposible de diferenciar de la legítima. Es por ello que se deben buscar indicios en otros lugares.

El principal y más importante es la *Uri*, en un caso de *Phishing,* ésta siempre tiene un *Dominio* diferente al de la web legítima. Esto, que parece obvio, es algo que el usuario medio suele desconocer y que es un indicativo claro de si la web es fiable.

Debido a que el *Dominio* no puede ser el mismo, los *Piratas Informáticos* suelen utilizar trucos para intentar enmascarar de alguna manera el *Dominio* y que pueda pasar por legítimo. Por ejemplo un truco muy frecuente es imitar el *Dominio* de la empresa legítima añadiéndole pequeñas variaciones que de un vistazo sean imperceptibles. Estos cambios pueden ir desde cambiar letras por números, añadir letras de más, utilizar palabras con ortografía similar… etc. Las posibilidades son infinitas, pero si el usuario presta atención a lo que lee, no es difícil, en la mayoría de los casos, encontrar alguno de estos elementos llamativos que delatan el fraude.

Otro truco, menos habitual por lo llamativo, pero también utilizado, es el de cambiar la extensión del *Dominio* y alojarlo en una web extranjera. Si la empresa legítima es, por ejemplo, española la extensión debería ser .ES, por lo tanto cualquier *Uri* procedente supuestamente de esa empresa debería tener un *Dominio* con dicha extensión.

Es cierto que muchas entidades bancarias internacionales disponen de varios dominios, pero lo lógico es que el usuario sea contactado desde la de su propio país, por lo tanto no debería ser necesario conocer todo el abanico de dominios controlados por la entidad, para poder declarar como fraudulenta una web en este punto.

Como punto de interés y que puede aportar información relevante para decidir la legitimidad del caso, la información que muestra el navegador en la web legítima respecto al protocolo de seguridad usado o certificado de la misma, siempre difiere con la información mostrada en la web suplantada, debido a que los *Piratas Informáticos* no pueden, lógicamente, conseguir certificados para sus páginas web fraudulentas.

Ilustración 14: En rojo, ejemplo de *Uri* ilegítima, en azul, la web legítima suplantada.

Para puntualizar, es importante indicar que siempre se debe comprobar la *Uri* directamente desde el navegador y no en el propio correo. Esto es debido a que existen enlaces denominados *Redirectores* (ver Anexo), cuya función se centra en redireccionar hacia otra *Uri* sin que el usuario sea alertado de ello. Un *Redirector* combinado con la posibilidad de poner un enlace en cualquier texto hace que, a priori, el enlace pueda parecer legítimo. Esta circunstancia y el hecho de no comprobar la *Uri* en el navegador crea la combinación perfecta para que el usuario caiga en la trampa.

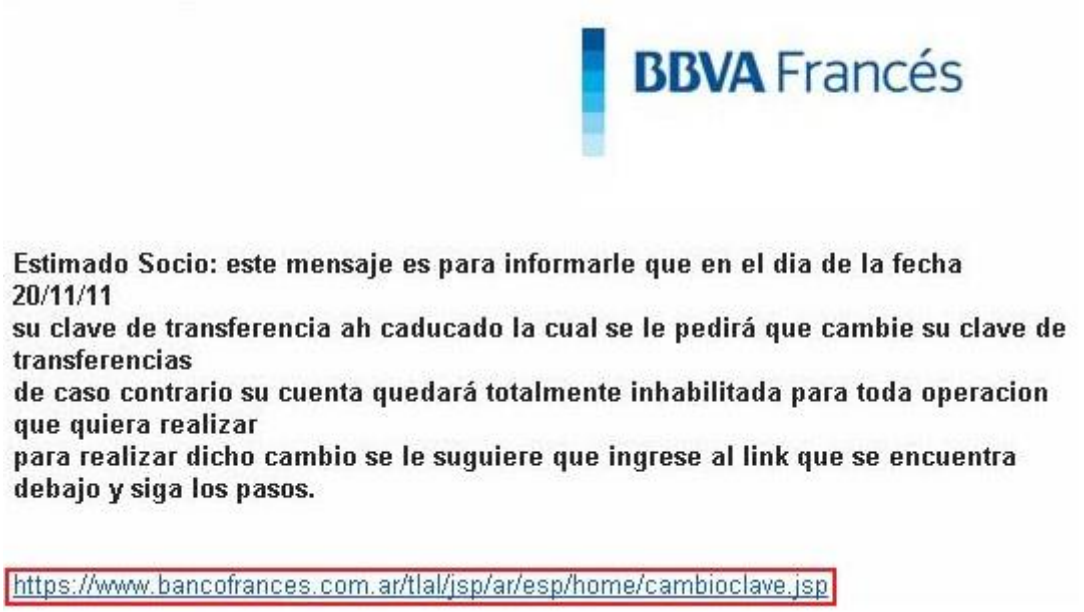


Ilustración 15: Ejemplo de *Redirector* que aparenta ser un enlace legítimo.

En caso de no ser posible reconocer el *Dominio* o no poder asegurar que es ilegítimo, el resto de la *Uri* puede ser de gran utilidad.

Normalmente las empresas asignan un nombre a cada página encargada de mostrar cada departamento de la propia web (Estas son vistas como carpetas en el propio servidor web), sin embargo, en los *Phishing,* es muy común encontrarse con nombres aleatorios e incluso totalmente incoherentes, formados por letras y números. Este aspecto es a la vista el más llamativo de las *Uri* fraudulentas y que más rápidamente pueden llevar a definir la autenticidad de la web.

También es frecuente ver en casos menos profesionales que en vez de *Dominio* aparezca directamente la *IP* asociada. Esto no es frecuente verlo en el caso de grandes entidades debido a que es un indicio muy claro de que es una web suplantada y, además, de cara al análisis por parte de un profesional, le facilita la labor al ya tener la *IP* asociada de antemano para poder solicitar su cierre (ver apartado Eliminación).

Ilustración 16: En rojo ejemplo de *IP* en vez de *Dominio,* en azul, subcarpeta fraudulenta.

En cuanto al contenido en sí de la página, es posible que al pasar el ratón por los botones de la misma se detecte que no son botones en sí sino enlaces en imágenes. Esto es un recurso de los *Piratas Informáticos* que, para imitar el estilismo de los botones de la web legítima, crean capturas de los botones y las asocian al enlace del mismo en la web suplantada para hacer lo más real posible la suplantación. Obviamente este es un recurso bastante pobre y que delata claramente como ilegítima a la web.

8.2 Como actuar

Es evidente que no todo el mundo que se pueda topar con un caso de *Phishing* va a saber a lo que se enfrenta, por lo tanto se van a dar unas pautas, recomendables de llevar a cabo, en caso de querer reportar algún caso de este tipo.

En primer lugar se va a explicar que hacer en caso de haber detectado el fraude a tiempo y no haber caído en la trampa.

En esta circunstancia lo ideal es contactar con la empresa afectada y reportar el caso. Para ello se puede enviar un email al departamento de atención al cliente indicándoles las circunstancias en que se ha recibido el caso, la *Uri* afectada y opcionalmente algún tipo de información personal por si fuese necesario ponerse en contacto con el usuario. Por lo general el protocolo de actuación de la empresa será redirigir el correo a su departamento de abuso (con el que se puede contactar directamente si se sabe cómo, ver apartado Eliminación), estos a su vez analizarán el caso y tras corroborar que, efectivamente, es un caso de *Fraude Online*, reportarán a su vez la *Uri* con la información que se haya facilitado a alguna empresa de seguridad especializada que se encargará de dar de baja el *Phishing* y cualquier página relacionada con él.

Con esto se conseguirá dar de baja el caso evitando futuras víctimas. Además las empresas de seguridad que se especializan en este tipo de fraudes, suelen monitorizar periódicamente las *Uri/IP* que hayan sido reportadas y dadas de baja para comprobar que no se hayan reabierto (ver apartado Análisis), por lo que, reportando el caso, se estará dificultando que los *Piratas Informáticos* puedan actuar de nuevo sobre los mismos dominios o IP.

En caso de caer en la trampa y haber revelado las credenciales en una de estas páginas, además de lo anterior, es vital cambiar cuanto antes todas las claves que hayan sido reveladas. Con esto se evitará que hagan movimientos en las cuentas bancarias en caso de que no las hayan hecho ya y en caso contrario, se evitará que puedan seguir haciéndolos.

Además es preciso avisar de lo sucedido a la entidad para que estén informados del caso y den de baja tarjetas, cuentas corrientes, o lo que fuese en caso de ser necesario.

Obviamente esta última circunstancia es un caso extremo, por lo que, más que en prevenir, las pautas a seguir, lo que buscan, es intentar minimizar daños.

Con esto se concluye el apartado de detección de fraude. Hasta el momento solamente se han detallado a las características de *Phishing* por ser el método más utilizado y más común de encontrar, no obstante, existen mecanismos como ya se ha indicado en otros apartados, que colaboran conjuntamente con el *Phishing* y cuya función consiste en potenciarlo desde otros medios menos habituales haciéndolo aún más imprevisible.

Como estos mecanismos se salen del foco de atención de este documento, centrado principalmente en el *Phishing*, para más información sobre los mismos deberá consultarse el Anexo disponible al final del documento donde se detallarán sus principales características.

Cabe indicar que en el siguiente apartado de Análisis se hará mención a algunos de estos mecanismos, por lo que es recomendable ampliar la información puntualizada en dicho apartado con lo mostrado en el Anexo.

9. Análisis

Este apartado va a dedicarse única y exclusivamente a mostrar los pasos y conocimientos necesarios para el análisis y tratamiento del *Phishing*, así como de *Redirectores*, *Troyanos Bancarios* y *Scam* en menor medida.

Por ello es necesario indicar que este apartado va orientado al trabajo profesional y no del usuario medio, pues las herramientas a utilizar, sin tener una complejidad excesiva, sí requieren de conocimientos avanzados para poder interpretar la información mostrada.

Con esta guía se explicará cómo conseguir toda la información posible de un caso para su posterior eliminación (ver apartado Eliminación) y también como conseguir desactivar los variados mecanismos de camuflaje que se emplean para evitar la extracción de información.

Finalmente y antes de empezar, aclarar que todo lo aquí mostrado es trabajo para un departamento cualificado y especializado como pudiese ser un Centro de Operaciones de Seguridad (SOC) de una empresa de seguridad, por lo que es inviable llevar a cabo dicha guía sin los recursos y las plataformas de control requeridas para ello.

9.1 ¿Por qué analizar?

Para poder trabajar con casos de *Fraude Online* como el *Phishing*, es vital saber con qué se está tratando. Toda la información obtenida del caso, será la que permitirá, cuando llegue el momento, solicitar el cierre del mismo y dar de baja las páginas implicadas.

En función de lo que se sepa de un *Phishing* el camino a tomar será diferente o, en todo caso, más recomendable o fructífero que otros. No hay que olvidar que toda la información que se vaya a obtener es precisamente la que va a manejar las personas u organismos encargados de inhabilitar el *Phishing*, por ello es fundamental hacer hincapié en cualquier detalle que se presente en el proceso de análisis.

Por otro lado y como es obvio, a la hora de pedir cerrar un caso, es necesario justificar el por qué, al fin y al cabo, en esencia, se estaría mandando dar de baja una simple página web, sin ningún peligro aparente, lo cual no es posible.

Además el proceso de eliminación es un proceso incierto, pues no es el analista el que se encarga directamente de ello, sino las personas o entidades que tengan algún tipo de relación o potestad sobre las *Uri* denunciadas. Por ello, ya no solo la información en sí, sino como se exponga y muestre a la hora de pedir el cierre, es vital para acelerar el proceso y evitar los, más que comunes, tropiezos e interrupciones por información incompleta o mal expresada.

Sabiendo esto no es difícil dilucidar que es una labor que requiere de cierta experiencia y capacidades para poder obtener óptimos resultados. Es por circunstancias como esta por lo que nacen las empresas de seguridad.

9.2 Empresas de Seguridad

En muchos casos las empresas de seguridad no realizan una labor que, en lo práctico, difiera demasiado de lo que podría hacer un particular con conocimientos desde su hogar con un ordenador. Es la experiencia, la capacidad de reacción y la visión del problema la que justifica y hace necesaria la presencia de empresas de seguridad y sus empleados.

Por otro lado el mundo del delito online requiere de reacciones rápidas y de adecuarse a lo que sucede en el menor tiempo posible para mitigar daños. Es ahí donde reside el verdadero potencial de las empresas de seguridad, que garantizan solvencia y resultados en márgenes de tiempo muy escasos al alcance solo de personal especializado y fruto de su labor.

Independientemente de lo anterior, el delito online evoluciona constantemente como ya se ha citado en algún punto del documento. Es por esto que ya no solo la labor y los conocimientos se presentan suficientes en la lucha contra el delito digital, ahora además, se hacen indispensables mecanismos de monitorización o seguimiento que permitan prever nuevos casos o que controlen la evolución de casos ya tratados. Esto no solo es útil de cara a combatir el propio delito en sí, pues permite elaborar estadísticas y documentar comportamientos que sean los que definan el perfil público de estos delitos, ya sea para la docencia del usuario común o para la elaboración de protocolos de actuación (como este documento). Estos mecanismos, obviamente, no están al alcance de un usuario medio. Su complejidad, su diseño, su uso y sobre todo, su costo, hace que estos mecanismos estén solo al alcance de corporaciones especializadas en seguridad digital y además, en muchos casos, son un elemento clave a la hora de desmarcar a unas empresas de otras.

¿Son necesarias las empresas de seguridad digital? ¿Qué labor realizan? ¿Por qué no se tiene constancia de ellas? ¿A quién realizan el soporte? ¿Qué garantizan?... estas son algunas de las preguntas más frecuentes a plantearse cuando se quiere conocer más acerca del mundo de la seguridad digital privada y las cuáles van a responderse en las siguientes líneas.

Para empezar se responderá a la primera pregunta, ¿Son necesarias las empresas de seguridad digital?, por supuesto que sí. Ya se han dado motivos más que suficientes para justificar su existencia pero hay aún más motivos para ello.

El delito online es un tipo de delito que, por su naturaleza, no destaca en los medios públicos al mismo nivel que el resto. Esto es debido a que parece algo vinculado a un mundo oscuro donde no todos pueden entrar. Telediarios, periódicos, revistas… prácticamente ningún medio de comunicación le da la importancia que requiere, si bien es verdad que cada vez se presta más atención como consecuencia de la creciente repercusión que empieza a tener el *Ciberdelito* en el usuario común. Es por ello que la información que obtiene el usuario, sin necesidad de investigar por su cuenta, es mínima, de ahí la sensación aparente de no existencia de este tipo de delito, o aún peor, la banalización del mismo.

Sabiendo esto, puede parecer lógico, desde el punto de vista del usuario, preguntarse si este tipo de empresas justifican su existencia, no obstante, los motivos que se presentan para ello

son más que convincentes. Sin empresas de seguridad no existiría la banca online. Más en concreto, no existiría la banca online ni ningún tipo de gestión online usuario-empresa.

Es necesario pensar en estas empresas como una base o soporte para las entidades que más suenan en el día a día. De esta manera se entiende su existencia y su función, pues realizan una labor poco reconocida pero clave en el funcionamiento de las mismas.

En cuanto a su cometido, resulta imposible de explicar todos y cada uno de los cometidos que estas empresas llevan a cabo, gestión de *Ciberdelito*, monitorización, análisis de tráfico, mantenimiento de servidores…etc., en definitiva, un sinfín de competencias, todas ellas igual de necesarias y de importantes.

En cuanto a la relación con las empresas cliente suelen funcionar de manera bastante sencilla, el cliente nutre a la empresa de seguridad de un flujo intermitente de casos que sus respectivos departamentos de informática califican como sospechosos o delictivos. Dicha empresa se encarga de realizar el tratamiento para comprobar de qué se trata y en caso necesario, llevar a cabo su eliminación.

Por otro lado, en cuanto a personal se refiere, las empresas de seguridad suelen ser bastante exigentes con sus empleados en lo que a atribuciones se refiere. Esto quiere decir que exigen una evolución constante en los conocimientos del trabajador. Para llevar a cabo este proceso de aprendizaje continuo los empleados suelen estudiar para conseguir los denominados *Certificados profesionales de seguridad*, que son los que modelan el perfil del trabajador, definen su labor y son relevantes en este sector.

9.2.1 Certificados profesionales de seguridad

Los certificados son documentos que cualifican a un trabajador en un campo específico o especialidad de su sector laboral. Dichos certificados permiten desmarcar a un trabajador del grueso de empleados, haciéndole más valioso y permitiéndole acceder a puestos de trabajo más especializados con sus correspondientes ventajas (mayor sueldo) e inconvenientes (mayor responsabilidad).

Los certificados son expedidos por el *SPEE*[1] y por la Administración Laboral de las Comunidades Autónomas.

Para obtener certificados es necesario realizar los cursos formativos que los componen, siendo estos en número y dificultad variable. No obstante la experiencia laboral también es considerada válida para poder optar a uno de estos certificados.

Los certificados informáticos de seguridad son algunos de los más complejos y valiosos que se pueden encontrar, es por ello que gozan de gran popularidad entre las empresas del sector. Su demanda es grande, pero su dificultad, en la mayoría de los casos, también.

[1] Servicio Público de Empleo Estatal.

Un trabajador certificado es sinónimo de un trabajador competente, además ciertos certificados son muy poco habituales de ver en empleados ya sea por la dificultad elevada del mismo, por su duración (en algunos casos bastante larga) o por su precio, no hay que olvidar que, habitualmente, los cursos formativos son cursados paralelamente al trabajo del empleado, por lo que en muchos casos requieren de un gran sacrificio en tiempo, esfuerzo y dinero por parte del aspirante.

Por todo esto es que el mundo de la *Seguridad Informática* es una de las ramas más especializadas y con mayor capacidad y necesidad de formación, de ahí su fama en el sector Informático.

Ilustración 17: Diploma de certificado de profesionalidad Español.

En cuanto a los certificados más valiosos o interesantes, habría que destacar por encima de todos los CSIM[1], los cuales están destinados a administradores de seguridad de la información muy reconocidos y valiosos. El objeto de su fama reside en los requisitos necesarios para poder conseguirlos, requiriéndose 5 años de experiencia en el sector, y en la dificultad para aprobar el examen de adquisición, en el cuál se exige una puntuación mínima del 75%.

Expedido por la ISACA[2], el examen es común en todo el mundo y exige que, una vez obtenido, se realicen cursos anuales con la intención de mantener actualizados en dicho campo a aquellos que lo posean.

[1] *Certified Information Security Management.*
[2] *Information Systems Audit and Control Association.*

9.2.2 Servicios

Los servicios que ofrecen las empresas de seguridad suelen depender en gran medida del enfoque que esta quiera tener, no obstante, se puede realizar un resumen global de los servicios más habituales que se pueden encontrar.

Cabe indicar que, los siguientes servicios, habitualmente tienen una nomenclatura propia en cada empresa. Con esto se consigue personalizar los departamentos relacionados y vender una imagen más independiente de la empresa.

- ***Cumplimiento de estándares y normativas:*** Este servicio proporciona ayuda al cliente para asegurar que los estándares, normativas y legislaciones son implementados y llevados a cabo con suma rigurosidad en todos y cada uno de los aspectos de la empresa cliente. Por ejemplo, en la protección de infraestructuras críticas[1].
- ***Consultoría:*** Asesora al cliente con el objetivo de garantizar la integridad de sus plataformas de información, con el fin de preservar la privacidad y seguridad de todos los datos susceptibles de ser robados.
- ***Delito digital:*** Permite dar soporte al cliente en cuestiones de *Ciberdelito*. La labor principal se centra en el tratamiento de los casos reportados por el cliente y en la generación de un *feedback* que permita mantenerle informado sobre los mismos. Este servicio es el eje principal de este documento y sobre el que se profundizará a lo largo del mismo.
- ***Inteligencia:*** Este servicio no tiene un enfoque de seguridad propiamente dicho, es más un departamento de soporte al cliente que le ayuda en la evolución de su empresa en aspectos de competitividad y progreso frente a sus rivales de sector.
- ***CERT[2]:*** Departamento generalmente *24x7*, cuya labor se detallará en profundidad en su apartado correspondiente en el proceso de Eliminación, debido a la implicación y relevancias directas con este documento.
- ***Formación:*** Servicio cuya función es asesorar al cliente en cuanto a los nuevos cambios que sufre el mundo digital, de tal manera que pueda adaptarse a los mismos estableciendo ventajas estratégicas. Suelen proporcionar cursos docentes que forman al cliente en aspectos de auditoría, análisis forense, talleres de seguridad…etc.
- ***Investigación:*** Proporciona avances, soluciones y metodologías para responder a las necesidades actuales y futuras del sector empresarial e institucional de la seguridad.

Vistos los servicios se puede decir que ya se tiene una idea general de la actividad desempeñada por las empresas de seguridad, a continuación se procederá a explicar el proceso de análisis que suelen llevar a cabo en casos de *Fraude Online*. En primer lugar se mostrará el proceso para casos de *Phishing*, pues es el caso que ocupa el grueso del documento, en siguiente lugar se mostrará el proceso para *Redirectores*, *Troyanos Bancarios* y finalmente para *Scam*.

[1] Ley 8/2011 de Protección de Infraestructuras Críticas.
[2] *Computer Emergency Response Team.*

9.3 Proceso analítico de un caso (*Phishing*)

Como punto de partida tras haber recibido un caso presuntamente fraudulento por una empresa cliente, el analista debe comprobar, sin excepciones, la actividad que desarrolla el supuesto *Phishing*. El principal objetivo es comprobar si el caso continúa actuando operativo (en cuyo caso habría que proceder a su tratamiento) o, por el contrario, se trata de un caso inactivo o cerrado.

Aunque pueda parecer una obviedad, no son pocos, de hecho, los casos en los que una empresa cliente (de aquí en adelante se supondrá un banco o entidad financiera) reporta casos que, contra toda lógica, han sido cerrados o no están en activo. Esto se explica fácilmente por el hecho de que los departamentos informáticos encargados de reportar casos, no suelen tener tanta capacidad de comprobar la actividad maliciosa de los enlaces que reciben. Pues a diferencia de las empresas de seguridad, sus conocimientos de la materia son más limitados y muchas veces su juicio se basa en la apariencia de lo que ven, sin profundizar en los detalles o informaciones que, a alguien experimentado, le permiten dilucidar rápidamente la actividad que desarrollo el supuesto fraude.

No obstante hay que tener en cuenta que un caso puede ser reportado, principalmente por otras empresas o por usuarios anónimos, a otras empresas de seguridad. Esto quiere decir que en el lapso de tiempo entre que el banco cliente recibe la denuncia y lo reporta a la empresa de seguridad (lo cual no siempre ocurre de inmediato), es posible que el caso haya sido tratado y dado de baja por otra empresa y se esté ante un caso totalmente inofensivo.

Aclarado el motivo de este chequeo se procederán a explicar los pasos para llevarlo a cabo.

9.3.1 Análisis de actividad

Lo primero que se debe hacer es abrir con un navegador la dirección reportada por el cliente y observar lo que aparece en pantalla. Si lo observado cumple las características de un *Phishing* se procederá a comprobar su actividad.

Para ello se procederá a realizar un chequeo con un analizador de código *HTML*[1]. Hay que indicar (para esta y todas las herramientas expuestas en adelante), que muchas veces las empresas prefieren tener su propia colección de herramientas privadas, no obstante, debido a la imposibilidad de acceso a las mismas y a que generalmente tienen un equivalente en herramientas públicas, son esta últimas las que se mostrarán.

En el caso que ocupa se va a comprobar la información mostrada por el *HTML* de la página mediante la aplicación online *Wannabrowser*[2]. Existen alternativas interesantes y algo más complejas como *Rex Swain*[3], no obstante, debido a la información que compete al caso (la cual es solo una pequeña parte de la que muestra esta herramienta) simplemente se mostrarán algunas capturas en el apartado Herramientas del Anexo.

[1] *Hyper Text Markup Language.*
[2] http://www.wannabrowser.com/
[3] http://www.rexswain.com/httpview.html

El objetivo de analizar el código es comprobar que mensaje de actividad[1] se muestra en la aplicación. Si los mensajes de actividad corresponden a códigos de inactividad temporal o permanente, es posible que se esté ante un caso cerrado de los anteriormente comentados.

Los códigos de actividad que pueden ser mostrados son los siguientes:

- ***Códigos 1XX:*** Son aquellos pertenecientes a mensajes sus valores son:
  - ***100-111:*** Mensajes de conexión rechazada, la *Uri* no presenta peligro pero sería recomendable analizarla a través de *Proxies* o herramientas que camuflen el origen de la conexión para asegurarse
- ***Códigos 2XX:*** Pertenece a las conexiones realizadas con éxito e indican que el caso está activo, son:
  - ***200:*** Conexión realizada sin mensajes adicionales.
  - ***201-203:*** Mensaje de información no oficial.
  - ***204:*** Sin contenido.
  - ***205:*** Contenido que es necesario recargar.
  - ***206:*** Contenido parcial.
- ***Códigos 3XX:*** Implican una redirección, si el destino lleva a un caso de *Phishing*, se considera activa, las variantes son:
  - ***301:*** Mudado permanentemente.
  - ***302:*** Encontrado.
  - ***303:*** Ver otras *Uri* relacionadas.
  - ***304:*** No ha sido modificada la web.
  - ***305:*** Necesario conectarse a *Proxy.*
  - ***307:*** Redirección temporal.
- ***Códigos 4XX:*** Muestran mensajes de error en el cliente y son:
  - ***400:*** Solicitud incorrecta, el caso no está activo.
  - ***402:*** Pago requerido, en principio el caso estaría inactivo, pero se recomienda seguir investigando.
  - ***403:*** Prohibido, el caso no está activo.
  - ***404:*** No encontrado, es el mensaje más común cuando se cierra un caso y no da lugar a dudas de que está inactivo.
  - ***409:*** Existe algún conflicto, es recomendable seguir analizando por otras vías.
  - ***410:*** Ya no disponible, similar al 404, el caso está inactivo.
  - ***412:*** Fallo de precondición, se recomienda seguir analizando por otras vías.
- ***Códigos 5XX:*** Error en el servidor, son:
  - ***500:*** Error interno, el caso está inactivo.
  - ***501:*** No implementado, el caso está inactivo.
  - ***502:*** Pasarela incorrecta, aparentemente inactivo pero se recomienda seguir analizando por otros medios.
  - ***503:*** Servicio no disponible, el caso está inactivo.

[1] Códigos de estado *HTTP*.

- ***504:*** Tiempo de conexión agotado, se recomienda reintentar la conexión y en caso de volver a fallar, continuar por otras vías alternativas.
- ***505:*** Versión *HTTP* no soportada, se recomienda analizar por otras vías.

Los códigos más comunes son los de conexión realizada con éxito (2XX) y en los casos cerrados los de error en el lado del cliente (4XX), principalmente el 404.

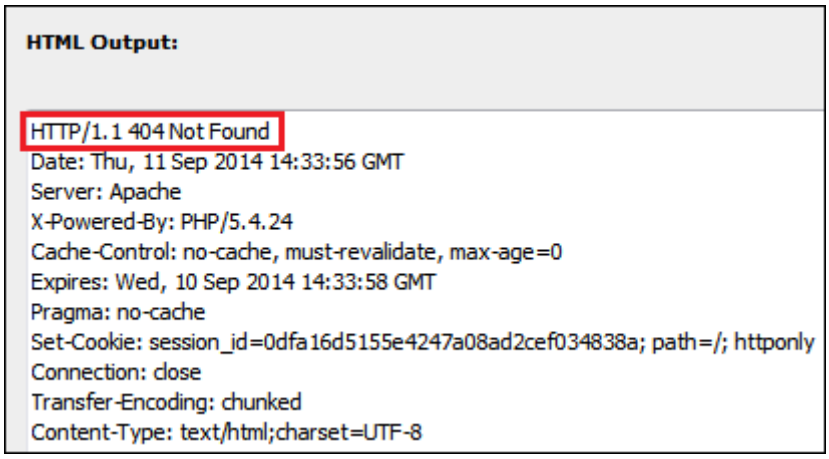


Ilustración 18: Ejemplo de código de inactividad *HTTP.*

No obstante, es frecuente el uso por parte de los *Piratas Informáticos*, de mecanismos de camuflaje o de evasión para evitar ser detectados. Estos mecanismos pasan por bloquear el *Phishing* a ciertas regiones geográficas de tal manera que, fuera de ellas, es imposible detectarlo a la vista, pues suelen mostrar mensajes o códigos (los anteriormente citados) que aparentan una web cerrada, con la intención de que pase desapercibida.

Para poder burlar estos mecanismos, el método más sencillo e inmediato es la conexión mediante *Proxy* (Ver Anexo).

En general un *Proxy* es un servidor que actúa como intermediario entre un cliente y el servidor que responde a sus peticiones. Su funcionamiento se basa en el control de flujo de datos entre ambos con diferentes mecanismos, entre otros, que es el que más interesa en este caso, el de poder prohibir tráfico en función de ciertos parámetros, como por ejemplo geográficos, como ya se ha comentado.

Para realizar una conexión de este tipo simplemente hay que conseguir la *IP* y el puerto de un *Proxy* de la zona geográfica que acepte el *Phishing* como válida y conectarse a través de él. Obviamente es vital conocer la procedencia del caso para poder localizarlo geográficamente y conectarse a *Proxies* válidos. Para ello y teniendo en cuenta que se trabaja con clientes de carácter internacional (en caso contrario no tendría sentido un bloqueo regional), es recomendable preguntar directamente a la empresa por la procedencia del caso, normalmente no tienen ningún problema en localizarlo, en caso contrario, se puede comprobar la extensión del *Dominio* para obtener una idea de dónde puede proceder.

Para realizar la conexión los navegadores suelen disponer de opciones para fijar *Proxies* de navegación, no obstante debido a que hay muchos tipos de navegadores y no se puede mostrar el procedimiento para todos, lo recomendable es utilizar algún tipo de herramienta que permita analizar la *Uri* accediendo mediante *Proxy* web. Este tipo de herramientas online permiten violar las restricciones que los *Proxies* fijan sobre los servidores, pudiendo establecer conexión con los mismos.

Algunas de estas herramientas son *Anonymouse* o *Hide My Ass!*. La primera de ellas es gratis y su uso muy simple, solo es necesario ingresar la *Uri* a la que se quiere acceder y automáticamente accede a ella como si se hiciese desde el navegador.

Ilustración 19: Página principal de Anonymouse.

Estas aplicaciones lo que hacen es camuflar la conexión de manera que los filtros anteriormente indicados son obviados. Lógicamente y para facilitar la usabilidad por parte del usuario, todo este proceso está oculto de cara al mismo.

En caso de querer realizar un análisis manual con *Proxies* a través del navegador de forma manual es necesario encontrar uno válido para el *Dominio* a analizar.

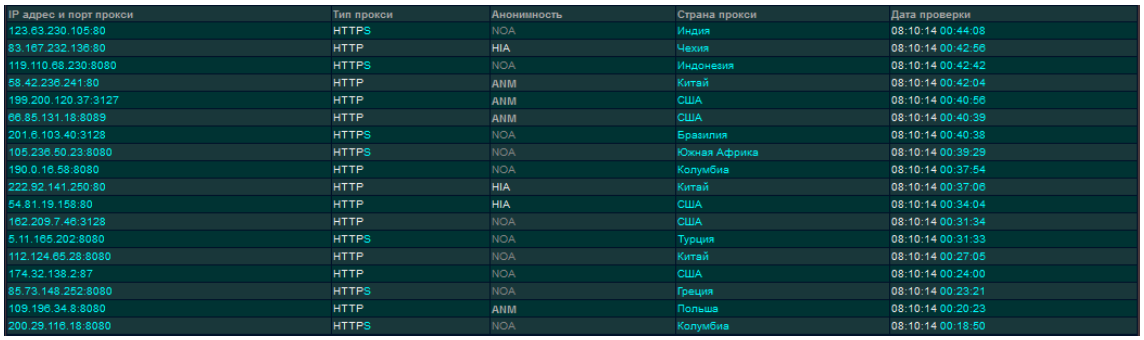
Para ello una vez localizada la procedencia geográfica de la *Uri*, se debe acceder a alguna página que proporcione *Proxies* como S*pys.ru*[1], entre otros. Hay que indicar que la web está alojada en Rusia, por lo que toda la información está en ruso, no obstante, es bastante intuitivo y con unos minutos de navegación rápidamente se llega a la información necesaria.

La idea es filtrar la lista por el país deseado y escoger un *Proxy* creado lo más recientemente posible comprobando las fechas que aparecen en la lista. En principio el protocolo de acceso no es relevante, no obstante en caso de obtener errores es interesante comprobar si permanece al cambiar a un *Proxy* con protocolo diferente.

Tras elegir el *Proxy* simplemente hay que copiar la *Ip* y el puerto de acceso (la cifra que aparece tras la IP a continuación de dos puntos) y generar la conexión a través del mismo mediante el navegador que se desee.

[1] http://spys.ru

Tras realizar la conexión ya se puede comprobar la actividad fraudulenta de la web.



IP адрес и порт прокси	Тип прокси	Анонимность	Страна прокси	Дата проверки
123.63.230.105:80	HTTPS	NOA	Индия	08:10:14 00:44:08
83.167.232.136:80	HTTP	HIA	Чехия	08:10:14 00:42:56
119.110.68.230:8080	HTTPS	NOA	Индонезия	08:10:14 00:42:42
58.42.236.241:80	HTTP	ANM	Китай	08:10:14 00:42:04
199.200.120.37:3127	HTTP	ANM	США	08:10:14 00:40:56
66.85.131.18:8089	HTTP	ANM	США	08:10:14 00:40:39
201.6.103.40:3128	HTTPS	NOA	Бразилия	08:10:14 00:40:38
105.236.50.23:8080	HTTPS	NOA	Южная Африка	08:10:14 00:39:29
190.0.16.58:8080	HTTP	NOA	Колумбиа	08:10:14 00:37:54
222.92.141.250:80	HTTP	HIA	Китай	08:10:14 00:37:06
54.81.19.158:80	HTTP	HIA	США	08:10:14 00:34:04
162.209.7.46:3128	HTTP	NOA	США	08:10:14 00:31:34
5.11.165.202:8080	HTTPS	NOA	Турция	08:10:14 00:31:33
112.124.65.28:8080	HTTP	NOA	Китай	08:10:14 00:27:05
174.32.138.2:87	HTTP	NOA	США	08:10:14 00:24:00
85.73.148.252:8080	HTTPS	NOA	Греция	08:10:14 00:23:21
109.196.34.8:8080	HTTP	ANM	Польша	08:10:14 00:20:23
200.29.116.18:8080	HTTPS	NOA	Колумбиа	08:10:14 00:18:50

Ilustración 20: Captura de pantalla de *Spys.ru*.

Llegado este punto ya se ha conseguido detectar si se está ante un *Phishing* activo o no. El siguiente proceso (uno de los más importantes) es el de ingresar o dar de alta el caso en la base de datos o en alguna plataforma privada de la cual la empresa de seguridad disponga.

A continuación se mostrarán los pasos que el autor de este documento ha creído más importantes para llevar un seguimiento lo más exhaustivo posible de cada caso. Obviamente cada empresa tendrá sus propias premisas a la hora de tratar esta información, por ello, las pautas y consejos que se van a mostrar deben ser consideradas como orientativas.

9.3.2 Seguimiento de casos

Lo primero que se debe hacer una vez verificado un caso de *Phishing* activo es, lógicamente, introducirlo en la *Plataforma de seguimiento*.

Debido a que la información contenida en la plataforma por cada caso es personal de cada empresa, es recomendable visitar el apartado de Eliminación, pues en el apartado correspondiente se muestra todo el contenido imprescindible que debería mostrarse para el seguimiento del caso. Además las siguientes líneas se fundamentarán en el hecho de que la información mostrada en dicho apartado ha sido entendida y asimilada.

El siguiente paso es notificárselo al cliente. Este paso es importante porque de esta manera el cliente podrá ingresar el caso en su propia base de datos para realizar su propio seguimiento.

Para ello lo ideal es enviar un correo de apertura de caso con la identificación que se le haya dado al caso en la *Plataforma de Seguimiento* y con una copia de la información mostrada por una herramienta de *WhoIs* (detallada en el siguiente apartado), esta información permitirá al cliente obtener una justificación tácita de porqué se está procesando el caso en caso de ser reclamados por alguien relacionado con el caso.

Para dotar de un identificador al caso en la plataforma es necesario primero realizar algunas comprobaciones.

En primer lugar se debería realizar una búsqueda a partir del *Dominio* denunciado entre todos los casos ya tratados. En caso de una búsqueda positiva, lo recomendable sería repetir los

pasos realizados para llevar a cabo el cierre del caso en el momento de su gestión. Con esto se puede ahorrar mucho tiempo pues la información recabada será, en la mayoría de los casos, válida para el nuevo caso al compartir dominio.

Hay que tener en cuenta que, en caso de coincidencia habría que aplicar las normas de coincidencia de *Phishing,* explicadas en el apartado Apertura de casos en la sección de Eliminación.

Una vez introducido el caso en la *Plataforma de seguimiento* se producirá a su análisis exhaustivo y a la realización de acciones (ver apartado Eliminación).

9.3.3 Obtención de información/ayuda

Una vez guardado el caso en la base de datos y notificado el mismo al cliente, es momento de recabar la información o de conocer las fuentes de soporte necesarias para, posteriormente, eliminar el caso.

La primera información a tratar es la proporcionada por la herramienta de *WhoIs* (ya sea la de la propia plataforma indicada en el Eliminación o una online pública).

Para poder interpretar la información es necesario saber lo que muestra dicha aplicación. Debido a que cada aplicación tiene sus preferencias a la hora de mostrar determinado contenido, los siguientes puntos se centrarán en la información mostrada por la herramienta *Central Ops*[1] (para ver una captura real de dicha información se puede observar la realizada para el apartado correspondiente a la sección Herramientas en el Anexo):

- ***Información de Dominio****:* Se muestra el nombre de dominio. Es la información que el DNS se encarga de traducir. Poco útil en lo que al cierre en sí se refiere debido a que los responsables de administrar la misma suelen requerir de terceros (los citados a continuación) para poder manejar toda la información contenida. Útil en los casos donde la única información que aparece en la *Uri* es una *IP***.**
  Hay que indicar que esta información no siempre se muestra, no obstante, el caso puede seguir siendo tratado, con la dificultad que entraña basarse únicamente en información de *IP*, pues el *Dominio* facilita el reconocimiento rápido del *Phishing* y la localización de ciertos contactos valiosos para el cierre**.**
  Por otro lado, en una gran parte de los casos, los responsables de los dominios son personas sin conocimientos de *Fraude Digital* o en todo caso, de las acciones a llevar a cabo, lo cual implica un esfuerzo por parte del analista para guiar en el proceso de cierre del mismo.
  Dentro de la información de *Dominio* los datos a tener en cuenta son los siguientes:
  - ***Registrador:*** El *Registrador* es la empresa que proporciona soporte a un *Dominio* registrado, reservándoselo al *Registrante* y dándolo de alta. Es uno de los elementos de contacto más útil, pues son los que tienen en propiedad el *Dominio* y quienes, en última instancia, serán los encargados de dar de baja el

[1] http://centralops.net/co/

Dominio, pues tienen acceso y administración directa con el mismo y sus correspondientes carpetas.

- ***Registrante:*** Es la persona o empresa encargada de contactar con el *Registrador* para dar de alta el *Dominio* en Internet. Responsable directo del *Dominio,* en muchos casos hace de puente entre el *Registrante* y el analista. En caso de poseer pleno acceso al *Dominio,* podría eliminar el contenido fraudulento sin necesidad de acudir a terceros.
- ***DNS[1]:*** Es el servidor encargado de traducir las direcciones web a *IP* de tal manera que se pueda acceder al ordenador que contiene la información a mostrar. En este caso aun no siendo de tan ayuda como el resto, el DNS siempre es un recurso a tener en cuenta ya que, al ser el encargado de direccionar al contenido de la *Uri*, es posible que puedan dar soporte para cerrar el caso.
- ***Administrador Web:*** Es la información relevante al administrador del dominio. En muchos casos suele coincidir con la información del *Registrante* puesto que en muchos casos, la entidad o persona que da de alta el *Dominio* también es la misma que la administra.
- ***Información Técnica:*** Información correspondiente a la empresa asociada al *Dominio,* suele coincidir con la información mostrada para el Administrador, al ser el técnico encargado de gestionar su contenido.

- ***El ISP[2]:*** Son los propietarios de la IP del sitio y primer elemento de contacto, pues tienen control total sobre la *IP*, pudiéndola dar de baja con el consiguiente cierre del domino y del fraude. Toda la información que se pueda recabar de esta entidad es de suma importancia para el caso. A menudo suelen dar un soporte muy escueto y son bastante reticentes a gestionar bajas de *IP*, pues se nutren de las mismas y requieren de evidencias muy contrastadas.

Todos estos datos podrían considerarse la documentación identificativa de un *Dominio,* es por ello que al notificar al cliente la apertura del caso es de vital importancia adjuntarle una copia del *WhoIs*. Con esta información, la empresa cliente verifica que el caso que les fue reportado en su momento es, efectivamente, un caso fraudulento.

Una vez obtenida toda la información posible de esta herramienta, se va a proceder a recabar información de contacto en la web del *Dominio* (en caso de aparecer especificado). El objetivo de este estudio es conseguir otras vías de comunicación. Útil, ya sea por mayor comodidad en su uso o, suponiendo que se trate de una empresa, por cuestiones de política en cuanto al soporte al usuario, pues muchas veces las vías de contacto oficiales no son las ofrecidas en el *WhoIs*.

Para empezar es interesante revisar toda la información corporativa que muestre la web. Cualquier dato que no aparezca en el *WhoIs* y permita un contacto con algún empleado o departamento, es recomendable tenerlo en cuenta.

[1] *Domain Name Server*.
[2] *Internet Service Provider*.

Normalmente la información corporativa se aloja al final de las páginas o tienen algún tipo de apartado dedicado en el menú principal. En caso de no ser localizable también puede existir algún apartado de contacto, que facilite emails o números de teléfono.

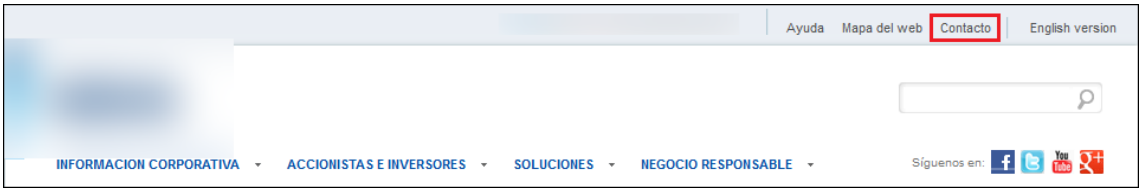


Ilustración 21: Acceso a la información de contacto en una conocida web.

Existen otros tipos de herramientas que permiten al analista obtener contactos de correo relacionados con el dominio.

Alguna de estas herramientas es *Abuse.net*. Esta aplicación muestra resultados de correo en función de un *Dominio* introducido.

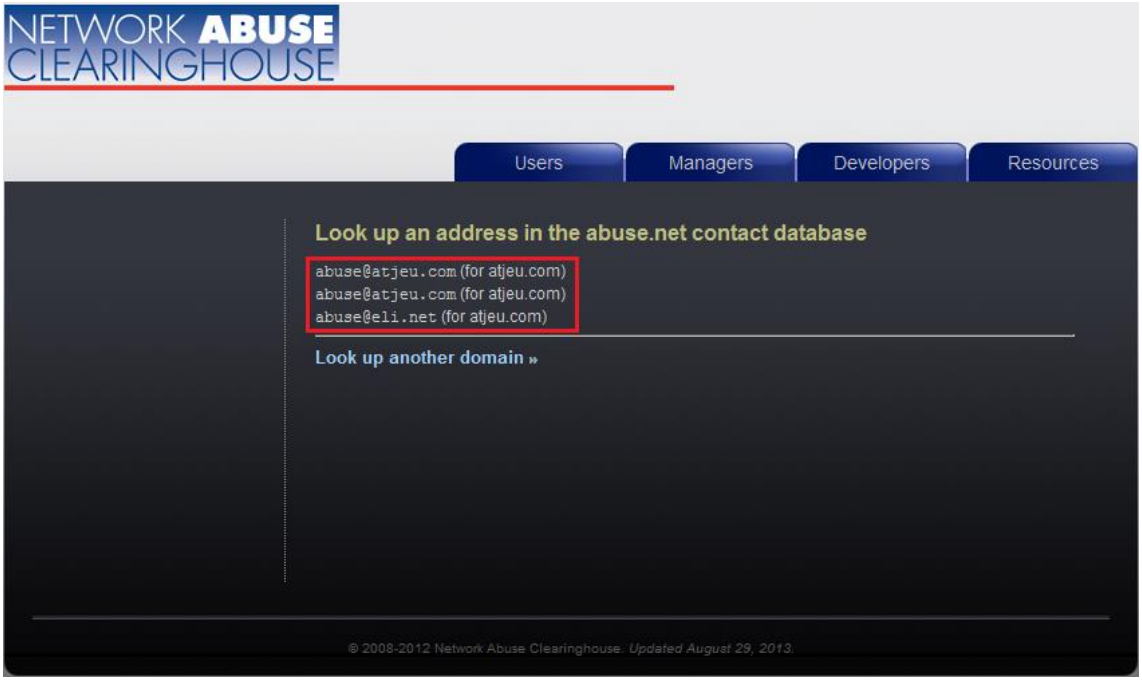


Ilustración 22: Captura de pantalla de la aplicación *Abuse.net*.

Normalmente los correos mostrados pertenecen a algún departamento de abuso, no obstante, hay que tener cuidado ya que, en caso de no encontrar resultados, sugiere un formato de correo por defecto que, en principio, no tiene porqué existir.

En caso de no encontrar información útil o relevante para el caso, se puede comprobar si existe algún tipo de soporte vía Chat o Formulario.

En el caso de haber un Chat, es frecuente encontrarse con acceso 24/7 al mismo, por lo que es una buena idea intentar explicar el caso por este medio. En caso de que el operador pudiese

proporcionar ayuda (algunos incluso pueden cerrar ellos mismos el caso), es esencial detallar al máximo el problema e indicar la *Uri* afectada. La mayoría de las veces el chat solo proporcionará ayuda en el apartado de Ventas de la empresa, por lo que es posible que no sea de demasiada utilidad, no obstante, en algunos casos, poco comunes eso sí, es posible que el departamento con el que se esté contactando a través de chat sea el departamento de abuso o de delitos informáticos. En estos casos suelen proceder al cierre indicando un retardo que no suele exceder las 24 horas. En el apartado Eliminación se mostrará detalladamente la información a proporcionar para una gestión óptima de la misma por parte del operador.

Si la persona que atiende no fuese la indicada, se podría solicitar, en caso de que no lo ofreciese por su cuenta, escalar el caso al departamento apropiado, pidiendo siempre criticidad máxima.

Es preciso indicar que muchas veces, aunque el soporte recibido no se ajusta a lo esperado, sigue siendo útil cualquier información que el operador revele acerca del caso, ya sean nuevos contactos o vías alternativas para la solicitud del cierre.

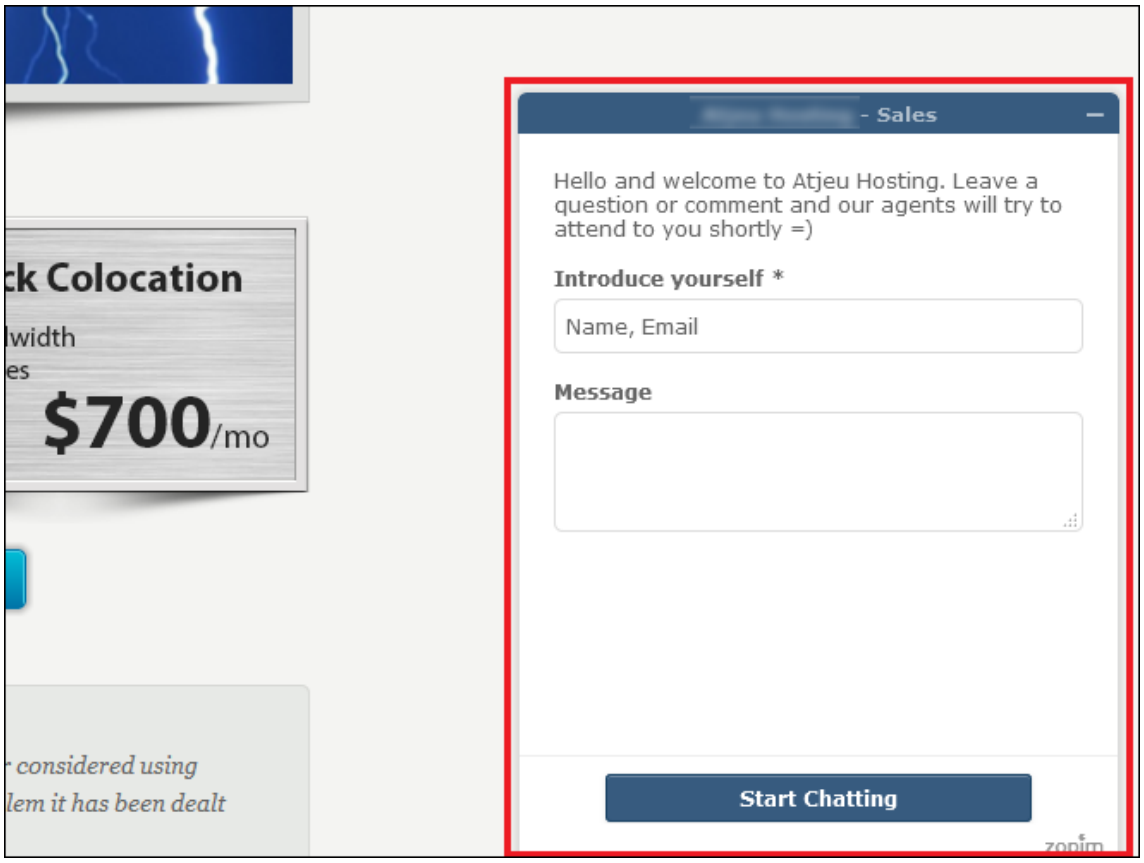


Ilustración 23: Ejemplo Chat de ventas en una web.

En caso de existir un formulario es importante, de nuevo, proporcionar la información del caso, diseccionada en los apartados que se muestren a rellenar para su mejor tratamiento en busca de ayuda.

Por la complejidad que entrañan ciertos formularios y la importancia para el caso que tienen los mismos, se procederá a explicar más en profundidad y con todo detalle toda la información a rellenar, así como la manera de hacerlo, en el apartado Eliminación.

Los formularios pese a su habitual lentitud, suelen ser el medio más común a la hora de informar de un cierre o, en todo caso, de la evolución respecto al mismo, por lo que es fundamental registrar todos los reportes informativos recibidos desde este medio (vía email) para esquematizar el seguimiento del caso por parte de la empresa.

Con todo lo explicado, ya se tendrían unas nociones básicas de cómo afrontar y empezar a tratar un caso de *Phishing* denunciado. No obstante, aunque el *Phishing* ocupe la mayor parte de los casos reportados, hay otros tipos de fraude que se deben tener en cuenta. Por ello, los siguientes puntos se centrarán en aportar algo de luz a la gestión de estos casos.

Hay que decir que, debido a que el documento gira en torno al *Phishing* fundamentalmente, no se va a profundizar demasiado en la gestión de dichos casos.

Como ya se ha indicado en alguna ocasión para ampliar información sobre estos casos, se recomienda visitar la sección correspondiente del Anexo.

9.4 Proceso analítico de un caso (Redirectores)

Como ya se ha puntualizado, los redirectores se suelen utilizar en conjunto con un *Phishing* para simular una falsa apariencia legítima. En estos casos, lo recomendable es incluir en la *Plataforma de Seguimiento* el *Phishing* como subcaso del *Redirector* y notificárselo al cliente, esto se debe a que la IP asociada es la misma tanto en el *Redirector* como en su *Phishing* asociado.

Obviamente en caso de comprobar dicha teoría y no cumplirse, es evidente que se trata de un caso diferente con un nuevo *Phishing*, por lo que habría que abrir un caso para el nuevo *Redirector* y el subcaso correspondiente para el *Phishing*.

Uno de los puntos más difíciles de controlar es el número de saltos que produce la *Uri*. Los saltos se conocen como todas las *Uri* por las que va pasando consecutivamente el *Redirector* hasta acabar en el *Phishing*. Debido a que los saltos son automáticos y no es posible detener el proceso en el navegador para obtener todas las direcciones, para su gestión, simplemente se tratará la *Uri* de origen. Esto se debe a que, como delito, es la dirección de más interés, pues, cerrando esta, el resto se vuelven inocuas.

Además en un hipotético caso en el que se consiguiese dar de baja la *IP*, se estaría cerrando el *Redirector* a la vez que el *Phishing*, con lo que se estaría cerrando caso y subcaso a la vez con las ventajas de cara al cliente que ello conlleva**.**

Como información adicional, cabe destacar que se dan casos en los que el navegador muestra un mensaje *HTTP* de tipo 301, este error muestra que la dirección ha sido movida permanentemente hacia otra dirección. Esta dirección suele ser el *Phishing*, sin embargo

puede tratarse de un nuevo redirector, por lo que es importante analizar de nuevo dicha *Uri* y en caso de ser necesario proceder a su gestión.

Ilustración 24: Captura de pantalla de un mensaje *HTTP* 301.

Con lo explicado se podría proceder a gestionar un caso básico de *Redirector* sin mayores inconvenientes. No obstante, existen casos extremadamente complejos de gestionar (algunos casos pueden llevar incluso meses cerrarlos), donde pueden entrar en juego hasta docenas de diferentes *IP* mutantes. Sin embargo, la preparación exigida y sobre todo la experiencia necesaria para su tratamiento, distan mucho del objetivo de este documento.

9.5 Proceso analítico de un caso (*Troyanos*)

En este apartado se van a mostrar los pasos a llevar a cabo para tratar correctamente un caso de *Phishing* asociado a un virus *Troyano*, concretamente *Troyanos Bancarios*.

9.5.1 Troyano bancario

Un *Troyano* (o caballo informático) es un virus cuya finalidad es obtener el control total o parcial de un ordenador objetivo, con la intención de robar información del mismo de manera transparente para el propietario.

Su patrón de actuación se basa en la creación de *Backdoors* (o puertas traseras en español) para dar acceso de manera remota a algún tipo de aplicación informática, que se encargará del robo de información confidencial. Esta aplicación actúa a voluntad por el ordenador objetivo en función de los privilegios que haya obtenido del usuario atacado.

Los *Troyanos* se componen de un cliente, el encargado de mandar las órdenes y un servidor, el encargado de recibirlas, ejecutarlas y devolver la respuesta obtenida.

En concreto, un *Troyano Bancario* es aquel que tiene como objetivo robar información confidencial asociada a bancos, como cuentas, tarjetas…etc.

Su manera de proceder para infectar los ordenadores objetivos, es ir asociados a correos corporativos (del banco a suplantar) falsos donde, con algún tipo de escusa, se solicita la

descarga de algún tipo de documento a cumplimentar por el cliente, como por ejemplo formularios, infectados con el *Troyano Bancario*.

Evidentemente, a simple vista es imposible detectar si se está ante un documento infectado, sin embargo, si se pueden observar evidencias claras en algunos casos como, por ejemplo, la descarga del documento como un archivo adjunto al correo o a través de enlaces que descargan automáticamente el archivo (procedimientos jamás empleados por una entidad bancaria legítima).

Por lo general y como en cualquier caso de virus *Troyano*, una vez infectado por cualquier modalidad de los mismos, es extremadamente complicado deshacerse de ellos, pues estos se instauran en el ordenador y actúan en segundo plano sin necesidad de que el usuario realice ninguna acción específica. Esta dificultad se ve acentuada por el hecho de que los *AntiVirus* comunes no suelen tener capacidad de desinfección de *Troyanos* o, al menos, de los más complejos.

9.5.2 Procedimiento

Lo primero que hay que tener en cuenta a la hora de gestionar un *Troyano Bancario* es que, el cliente, reportará un enlace que probablemente descargue un archivo comprimido o, directamente, se adjunte el archivo en un correo. Es necesario indicar que estas son las vías de infección más habituales para atacar en este entorno, no obstante, se dan casos mucho más extraños y variopintos, que por su complejidad y tratamiento (exclusivo para cada una de estas situaciones) no se van a tratar aquí.

Este archivo, en principio, contiene algún tipo de archivo que, al ejecutarlo, ejecuta un *Troyano* en segundo plano de manera totalmente transparente al usuario. Por ello, es vital no abrir dicho archivo y simplemente, limitar la actividad en el mismo a su descomprensión.

Una vez obtenido el archivo teóricamente infectado, este debe ser analizado por algún tipo de herramienta que muestre información vírica sobre el mismo y sobre todo, muestre un código identificativo, a ser posible en *MD5*[1]. Este código se crea a partir de un algoritmo criptográfico de seguridad, su utilidad se fundamenta en la capacidad de garantizar que, mediante este cifrado, el archivo original no ha sido alterado de cara a asegurar la integridad del mismo.

Respecto a las herramientas, normalmente las empresas de seguridad desarrollan sus propias aplicaciones con el objetivo de conseguir únicamente la información que crean necesario en el tratamiento del archivo por parte del departamento encargado de ello.

Sin embargo existen herramientas públicas que permiten un análisis similar y que cumplen una función parecida. Una de estas herramientas es la popular *Virus Total*[2] (ver el apartado Herramientas del Anexo).

[1] *Message-Digest Algorithm 5.*
[2] https://www.virustotal.com/es/

Esta aplicación proporciona análisis gratuitos de archivos en busca de virus. Una vez analizado un archivo o *Uri*, la herramienta muestra los diagnósticos realizados por hasta 53 *AntiVirus* diferentes, de tal manera que se generan datos estadísticos respecto a la actividad vírica del componente consiguiendo dar un veredicto sobre el mismo, evitando falsos positivos.

Por otro lado también proporciona diferentes códigos identificativos (entre ellos el citado *MD5*), nombre de la plataforma o programa asociado a la extensión del archivo (útil para orientarse en búsqueda de comportamiento malicioso), tamaño…etc.

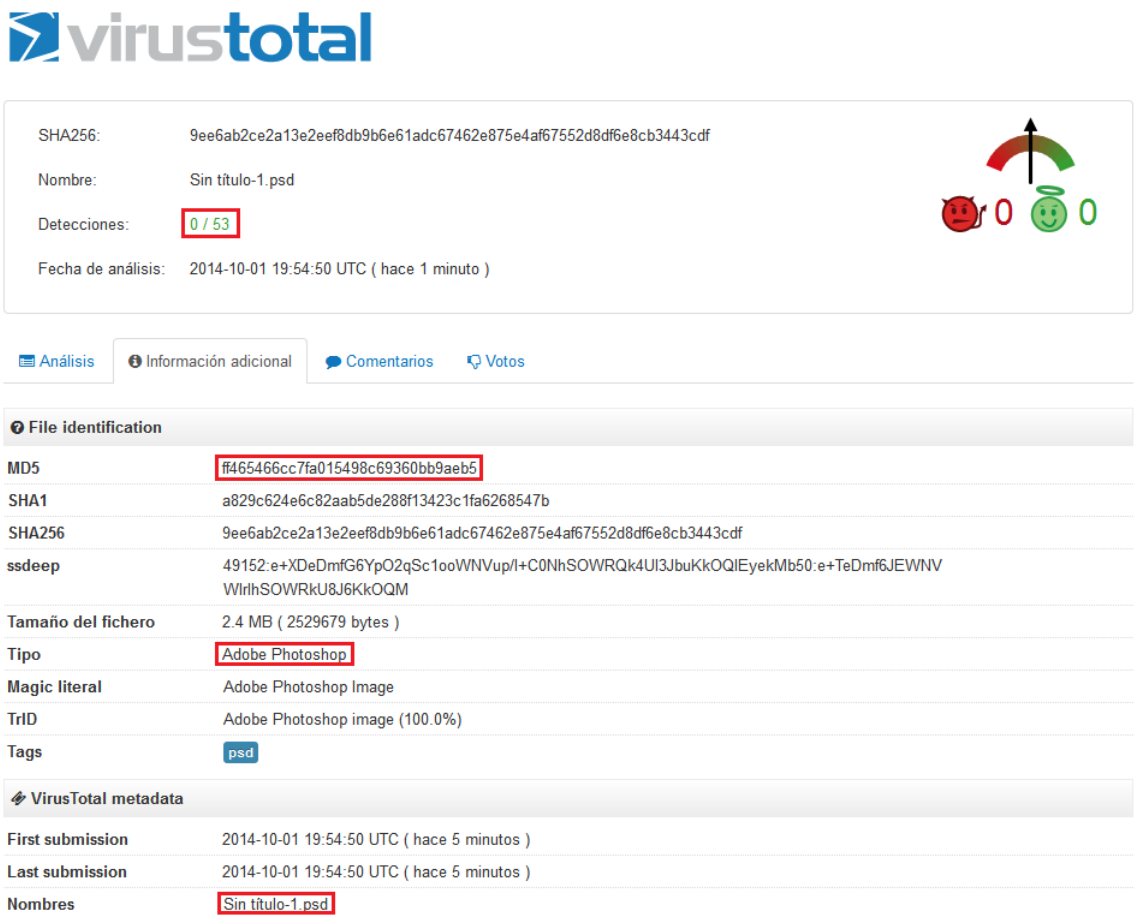


Ilustración 25: Muestra de la información mostrada por la herramienta *VirusTotal.*

Una vez obtenido el primer veredicto por parte de la herramienta y siendo este positivo, el siguiente paso es redactar un correo escalando el caso al departamento especializado correspondiente. En este correo se debe solicitar el análisis exhaustivo en función de la información obtenida por la aplicación, además de la explicación oportuna de lo que el cliente ha reportado y porqué.

Normalmente dichos departamentos no suelen demorar el tratamiento del caso más de 12 horas (debido a la criticidad de los reportes en los que se están implicados virus bancarios).

Una vez obtenido el informe de dicho departamento, simplemente se notifica al cliente la información extraída y en caso de verificar la virilidad del mismo, se procedería a su inclusión

en la *Plataforma de Seguimiento* realizando las acciones como si de un caso de *Phishing* se tratase (ver apartado Eliminación).

Tras comprender lo anterior, no es difícil llegar a la conclusión de que, realmente, el departamento antifraude no está realizando un análisis como tal sino, más bien, una gestión temporal actuando como puente entre el departamento encargado de ello y el cliente. La razón de esto es que los virus tienen una estructura y comportamiento que nada tienen que ver con la *Ingeniería Social* y en definitiva, con el entorno de operación de un *Phishing* convencional. El estudio de virus es una rama de conocimiento por sí misma y requiere de muchas horas y experiencia que, en principio, un departamento antifraude no tiene por qué tener.

9.6 Proceso analítico de un caso (Scam)

Este caso es muy particular y requiere de un tratamiento bastante peculiar.

9.6.1 SCAM

El S*cam* es una suplantación de identidad cuyo objetivo difiere del *Phishing* en la motivación, pues su objetivo no son entidades financieras ni plataformas de pago.

Su objetivo principal es estafar al cliente promocionando productos falsos (entre otros casos) en forma de ofertas en nombre de otra compañía o a través de correos electrónicos fraudulentos.

Es una variedad de fraude bastante extraña pero muy dañina y complicada de gestionar.

9.6.2 Procedimiento

La dificultad que entrañan es máxima, pese a ser bastante menos críticos que un *Phishing.* Esto es debido a que, en principio no tiene porqué existir robo de credenciales. Normalmente la web que suplanta suele ser otra empresa que no se oculta, por lo tanto, existe un objetivo claro con el que contactar.

Normalmente es la empresa afectada la que reporta el caso, denunciando que ellos no promocionan ese tipo de producto o en esas condiciones y solicitan que se elimine de inmediato el contenido.

La labor del departamento antifraude se basa en comprobar que, efectivamente, la información denunciada existe y está visible al público para, acto seguido, ponerse en contacto con la empresa que oferta el producto.

A dicha empresa es necesario indicarle detalladamente qué empresa es la denunciante y el porqué de la misma. Una vez hecho esto se solicitaría la eliminación del contenido a la mayor brevedad posible.

Hay que tener en cuenta que la empresa denunciada se beneficia de alguna manera de dicha oferta haciendo caer a las víctimas en compras o inversiones monetarias falsas. Esto implica que la empresa reportada, en un intento de maximizar beneficios, alargue la situación hasta llevar la situación a un estado insostenible para el cliente. Es por ello que los casos se pueden alargar durante semanas e incluso meses y sin llevar a cabo el más mínimo avance.

Otra situación común es que se realice la eliminación de parte del contenido, de tal manera que este sigue activo y con la suficiente información para seguir llevando a cabo la estafa. En este caso es necesario contactar de nuevo con la empresa indicando que el cliente no está conforme con la información eliminada.

También se dan casos donde la empresa propietaria de la web niega su capacidad de administración y por lo tanto la posibilidad de eliminar el contenido, con la consiguiente lucha por parte del departamento antifraude por demostrar lo contrario.

En definitiva, son casos con infinidad de escenarios y la mejor manera de conocerlos a fondo, es enfrentarse a ellos.

Es importante indicar que la labor de cierre de *Scam* no es, a priori, una labor directamente relacionada con un departamento antifraude debido a que el amplio abanico de comportamientos que este tiene, impide la elaboración de un protocolo de actuación estricto al que ceñirse. Más bien suele encontrarse como un servicio alternativo o extra proporcionado por la empresa de seguridad, con el fin de desmarcarse de sus competidores ofertando servicios más exclusivos.

Ilustración 26: Ejemplo de *Scam* suplantando a *YouTube*.

10.Eliminación

Finalmente y para concluir la estructura central de este documento, se van a indicar los pasos que realizar para, tras haber analizado un caso y haber obtenido toda la información posible del mismo, proceder al cierre o, al menos, iniciar los trámites para dar de baja la *Uri* fraudulenta.

Llegado este punto y para resumir, el analista ya habrá comprobado la actividad del fraude y habrá extraído toda la información posible del mismo.

Este proceso es el más crítico de todos, pues será el momento de contactar con los implicados directos en el caso y por ello, es necesario saber cómo hacerlo y que información dar.

Además, tras verificar el cierre, será necesario notificarlo y proceder a activar mecanismos de monitorización para comprobar la evolución de la *Uri* con el objetivo de que no se reactive.

Para explicar todo lo anterior lo más detalladamente posible se indicará, en primer lugar, cómo manipular e interpretar la información extraída, con quien contactar para poder gestionar el cierre, como registrar todas las acciones en la *Plataforma de Seguimiento* y finalmente, tras haber realizado todo lo anterior, verificar que se ha llevado a cabo la eliminación del fraude y detallar en que consiste el procedimiento de monitorización.

10.1 Interpretación y manipulación de la Información del caso (Acciones)

Con toda la información recabada, hay que saber que desechar y que utilizar. Como cada caso requeriría de un manual por sí mismo, aquí solamente se van a dar los conceptos genéricos más relevantes a la hora de manipular la información de caso.

A la hora de utilizar la información se hablará de lo que en este documento se denominarán "*acciones*". Las acciones son procesos de utilización de la información con la intención de evidenciar la fraudulencia del caso, al contacto o contactos con los que se está comunicando el analista. Estas acciones van desde simples correos, hasta, como ya se ha indicado en el apartado anterior, la cumplimentación de formularios.

Además toda acción deberá quedar debidamente registrada en la *Plataforma de Seguimiento*, pues el cliente requerirá de *Informes Diarios de Seguimiento* donde comprobará que tratamiento a recibido el caso a través de dichas acciones.

Como paso previo a lo que se va a mostrar a continuación, es necesario aclarar que en todo contacto que se realice, el analista nunca deberá personarse como responsable de la reclamación, pues es un eslabón que ejerce como simple intermediario entre la empresa cliente y los contactos. En definitiva, será la empresa de seguridad la que deberá ser presentada como responsable de la denuncia.

Por otro lado es preciso matizar que la detección del caso no corre a cuenta de la empresa de seguridad sino que esta, simplemente atiende una denuncia por parte de un cliente. Esto, que a priori pueda parecer no tener importancia, es relevante, pues libera de responsabilidades a la empresa de seguridad en caso de reclamaciones o conflictos por irregularidades en la detección del fraude.

10.1.1 *Correos de denuncia*

La principal y más común de las acciones.

El correo electrónico a lo largo del caso se convertirá, probablemente, en el canal de comunicación más usado para contactar con los implicados en el mismo, pues es la manera más rápida y directa de hacerlo, por ello, es indispensable saber que redactar y que estructura seguir.

Para empezar es imprescindible, obviamente, escribir en el idioma o idiomas que el contacto entienda. Con esto se asegurará que es capaz de interpretar la información y trabajar con ella sin dar lugar a equívocos.

No son pocos los casos en los que, por error, un correo redactado en un idioma desconocido para el contacto, es totalmente obviado e incluso archivado como *Spam*[1], con el consiguiente retraso en la eliminación hasta que se soluciona el problema o se consigue contactar por otros medios. Esto se debe a que, muchas veces, el contacto no se rige por un entorno empresarial donde se debería, al menos, mostrar un mínimo interés por saber que está recibiendo, sino que puede ser un particular con un correo privado al cual le llega mucho correo indeseable, confundiendo el enviado por el analista con uno de ellos.

Hay que destacar que este comportamiento no solo se da en particulares sino también, en casos excepcionales, en empresas. Los motivos pueden ser varios, desde correos con un contenido mal redactado, correos en idiomas que el contacto de la empresa no entiende o, el más común de ellos, reiteración excesiva en el envío de correos. Un flujo demasiado denso de emails, puede provocar que el cliente los califique de *Spam*, es por ello que se debe ser conciso y sobre todo, parco en el envío de correos.

El hecho de ser archivado como *Spam*, aunque a priori pueda parecer algo insignificante, puede ser muy grave. Estar filtrado como correo indeseable por un contacto, significa que cualquier correo enviado por el analista, será automáticamente obviado y enviado a una bandeja de *Spam* (que todos los clientes de correo tienen) del contacto. Esto supone la incapacidad de contactar por este medio con el implicado y la obligación de buscar medios alternativos de comunicación, los cuales no siempre se consiguen.

Esto es especialmente dañino cuando el bloqueo lo realiza una entidad importante para la gestión del caso, como pudiese ser un *ISP* pues, con frecuencia, son empresas que suelen estar relacionadas con varios casos, para los cuales ya se suprimiría dicha vía de comunicación.

[1] Correos no deseados o con remitente desconocido, cuyo contenido suele ser de tipo publicitario y que generalmente se envían de manera masiva.

Llegada esta situación, lo recomendable sería ponerse en contacto telefónico (en la media de lo posible) para reestablecer las comunicaciones. No obstante, debido a la criticidad de los casos, mientras se gestiona el desbloqueo se deberá contactar mediante los medios que el cliente posibilite, para retrasar la gestión del caso el menor tiempo posible.

Para acabar con el aspecto idiomático del correo, puntualizar que, el uso de traductores automáticos, si bien puede servir como una solución temporal, es recomendable evitarlos en la medida de lo posible. Esto se debe a que la traducción proporcionada por estas herramientas, suele ser demasiado literal, no sabiendo interpretar determinadas expresiones o composiciones gramaticales, con los fallos que se derivan de ello. Estos fallos dan una apariencia poco profesional y pueden generan desconfianza en el contacto.

Por otro lado, la densidad del mensaje debe ser lo más directo y estructurado posible. Salvo que la ocasión lo requiera (y así será en determinados casos) el mensaje deberá ser breve y conciso en lo que al problema en cuestión se refiere.

Por regla general, no suelen verse amigables los correos con alta densidad de contenido. El contenido técnico, necesario para explicar el caso adecuadamente y la tendencia a perder comprensión según se alarga la lectura, desfavorecen el cometido del mensaje, que es la rápida actuación y reacción para cerrar el caso.

En cuanto al contenido y la estructura, no hay nada estandarizado como válido, sin embargo, si existen unas maneras de presentar la información más adecuadas que otras y aquí se va a mostrar la que, en la práctica, parece más favorable.

Para empezar, en la introducción es esencial saber mostrar la intención del resto del mensaje y lo que se pretende conseguir. Con una o dos líneas introductorias debería bastar.

En lo que al contenido del mensaje se refiere, es imprescindible explicar el origen del caso, que implicación tiene el contacto en el mismo, así como pruebas que lo demuestren y que acciones podría llevar a cabo para ayudar a dar de baja el fraude.

Finalmente es recomendable adjuntar una copia del *WhoIs* donde se vea claramente que el contacto aparece implicado y en caso de ser necesario, ya que algunos organismos lo requieren, una captura de pantalla de que el caso permanece activo en el momento de la comunicación.

En cuanto a la conclusión del mismo, es preciso adjuntar información del analista y de la empresa, así como otros medios de comunicación, como por ejemplo el teléfono, para facilitar la respuesta y la colaboración del contacto con el caso.

Hay que decir que lo indicado anteriormente, se corresponde a correos enviados para reportar el caso por primera vez al contacto. En sucesivos correos, evidentemente, se deberá amoldar el contenido a lo solicitado por el contacto.

Para finalizar el apartado de correos, los contactos empresariales con los que se debe contactar deberían ser, en la medida de lo posible, contactos relacionados con departamentos de abuso como ya se ha indicado anteriormente. En caso de no tener un contacto de este tipo,

es recomendable contactar con departamentos de información o incluso ventas, solicitando que se escale el caso.

10.1.2 Formularios

Los formularios son el método más habitual de contacto vía web con las empresas. En la mayoría de los casos suele ser un procedimiento simple, pero que requiere de unos minutos hasta proporcionar todos los datos necesarios, no obstante, se dan casos en los que los requerimientos solicitados van más allá de lo que el analista puede proporcionar en un primer momento y complican notablemente la cumplimentación del mismo. Como el objetivo es dar una idea general, no se va a profundizar en estos casos y se va a mostrar la información a rellenar en los formularios más habituales.

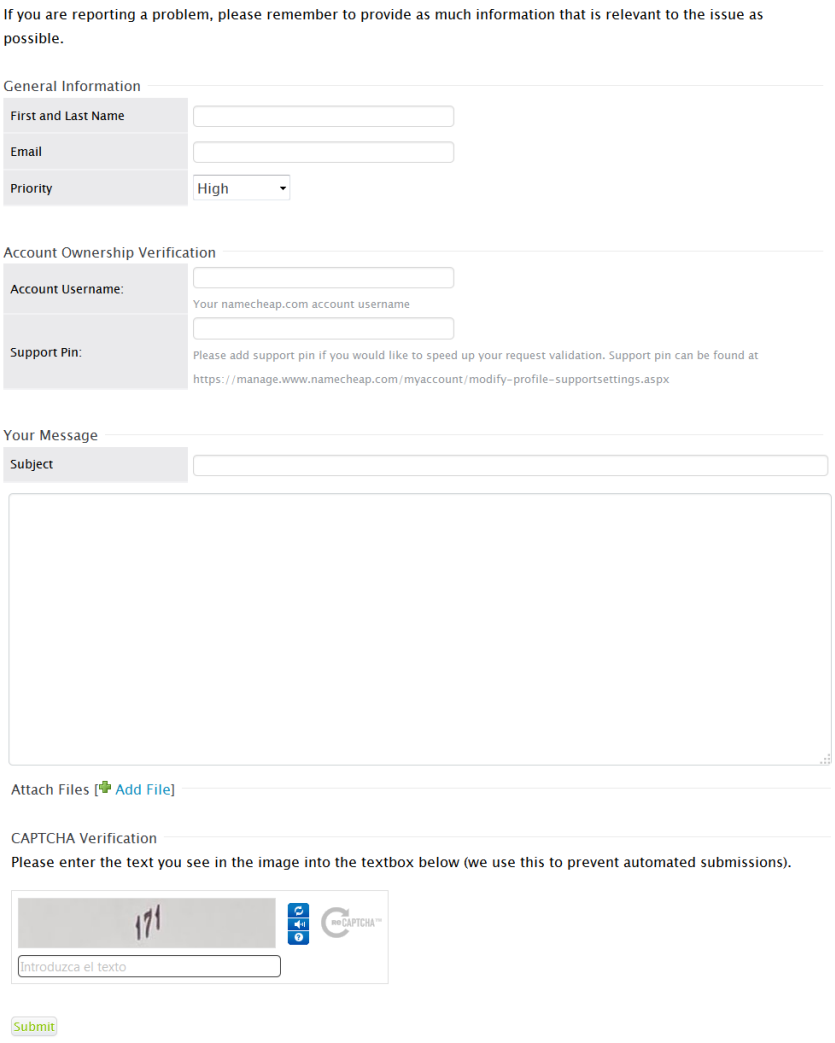


Ilustración 27: Ejemplo de formulario.

Por lo general los formularios suelen estar alojados en secciones de contacto en las web corporativas, sin embargo, en algunos casos se permite especificar qué tipo de contacto se quiere realizar en función del motivo del mismo. En estos casos habría que elegir un reporte de

tipo “Abuso” o en su defecto “*Phishing*”, si fuese posible. Además en muchos casos no harán distinción entre formulario y Ticket, por lo que es probable que al finalizar la cumplimentación se reciba un número de Ticket a consultar posteriormente, en la dirección de contacto facilitada por el analista, por lo que es importante que se esté atento a posibles actualizaciones del mismo.

Para poder explicar correctamente los datos a introducir, se va a utilizar un ejemplo de formulario tipo para facilitar la comprensión de lo mostrado.

- En primer lugar es necesario proporcionar un nombre al que se dirigirá el contacto al tratar el reporte. Debido a que el analista debe mantener el anonimato, el nombre proporcionado siempre será el de la empresa, seguido del nombre del departamento, para mostrar que es una denuncia por parte de una organización y no de un particular.
- Por otro lado es fundamental proporcionar un email de contacto con el que el contacto se comunicará con el analista para informar de la evolución del caso. En este caso se facilitará el email del departamento y nunca uno privado.
- También, en la mayoría de los casos, se solicitará indicar un tipo de prioridad. Lógicamente, en este tipo de casos es indispensable indicar la más alta posible para intentar conseguir el cierre o, al menos, alguna acción a la mayor brevedad posible.
- A veces es posible que se agilice el caso si se proporcionan datos de una cuenta registrada en la web como cliente. En estos casos se puede ignorar o, en caso de requerir un trato más rápido, darse de alta para aprovechar esta ventaja. En caso de tener una cuenta se suele solicitar un código asociado a la misma.
- En cuanto al cuerpo del reporte es necesario introducir un título identificativo. Para ello se debe poner una frase descriptiva del caso lo más breve posible.
- Para completar la información existe un apartado donde se pide detallar el objeto de la denuncia. En este apartado se procedería de la misma manera que al enviar un correo, respetando una estructura ágil y comprensiva y adjuntando una copia del *WhoIs* donde se evidencie que el contacto está implicado en el caso.
- Es posible que en determinados casos se pueda adjuntar algún tipo de archivo. En este caso una captura del caso demostrando que sigue activo en el momento del reporte podría resultar de ayuda, si bien no es significativo, pues el propio contacto se encargará de verificarlo por su cuenta.

Con esto ya se habría cumplimentado correctamente un formulario típico. Normalmente, una vez enviado el reporte, la empresa envía un correo de confirmación con las instrucciones a seguir a partir de ese momento. A partir de este punto el analista solo deberá estar al tanto de las actualizaciones del reporte para actuar en consecuencia.

Para finalizar, hay que decir que los formularios suelen ser un medio eficaz pero lento, ya que la cantidad de reportes que pueden obtener las empresas por parte de terceros es muy grande y de diversa índole, por lo que no se puede esperar una rápida actuación por su parte, incluso habiéndole asignado máxima prioridad.

10.1.3 Chat

Probablemente el medio más directo y recomendable en caso de existir, sin embargo son pocas las empresas que disponen de uno y menos aun las que proporcionan servicio antifraude por esta vía. Por lo general, van a ser en gran medida chats relacionados con ventas o soporte al cliente, que no tienen competencia en dicho campo. No obstante es igualmente interesante contactar para poner en constancia el caso y que sea reenviado al departamento oportuno.

En caso de contactar vía chat, lo primordial es presentar la empresa del analista como solicitante del cierre (al igual que en los formularios) y dar una breve explicación del caso incluyendo la *Uri* afectada y a ser posible, la *IP* de la misma.

Si el contacto está especializado en el campo del fraude, es probable que ofrezca soluciones a corto plazo o incluso cierres inmediatos en menos de un día si los datos proporcionados son contrastados, por ello es vital proporcionar la mayor cantidad posible de información relevante.

Además, son habituales los casos en los que el contacto, al no poder ofrecer soluciones inmediatas, proporciona un número o código de referencia de la conversación (similar al de los formularios), para poder realizar un seguimiento continuo posterior al contacto, por lo que, de nuevo, el analista debe realizar un seguimiento de toda acción realizada en el reporte.

10.1.4 Teléfono

La comunicación telefónica es vital cuando se trata de obtener resultados urgentemente, pues se asegura un trato personalizado y exclusivo con el analista a diferencia de los chats, donde el contacto puede estar atendiendo varios en paralelo.

El único inconveniente, a priori, puede ser el idioma. Muchas veces se va a contactar con lugares geográficamente muy remotos respecto a lo que se consideraría habitual y obviamente, en estos casos, es prácticamente imposible la comunicación telefónica si no se conoce la lengua en cuestión. Incluso con idiomas conocidos, como pueden ser el Inglés, Francés, o Español, varía mucho el acento y las expresiones de unas regiones a otras. Esto motiva que, incluso siendo conocedor de alguna de estas lenguas, en algunos casos sea difícil entender al receptor.

Obviando lo anterior y suponiendo una conversación eficaz y productiva, es recomendable abusar de los contactos telefónicos en la medida de lo posible.

Debido al carácter dinámico de una conversación en contraposición a lo estructurado del resto de formas de contacto, es difícil formar un guion a seguir, no obstante sí que se pueden indicar las pautas básicas.

Estas pautas consisten, como en los casos anteriores, en presentar en primer lugar a la empresa solicitante del cierre y a continuación explicar el caso detalladamente.

Hay que tener en cuenta que, al contactar telefónicamente con un particular, no hay nada que asegure que el mismo tenga capacidad de gestionar el caso, pues no es posible saber si el contactado tiene unos mínimos conocimientos de lo que se le va a reclamar.

Esto supone que, en muchas ocasiones, se contacte con gente que no entiende lo que se le está diciendo o, simplemente, sean incapaces de reaccionar ante el problema por falta de recursos. Esto que pueda parecer contradictorio es bastante lógico si se tiene en cuenta que dar de alta una página web está, hoy en día, al alcance de cualquier persona no necesariamente cualificada.

En caso de encontrarse con uno de estos contactos, el analista solo puede solicitar que el contactado actúe por su cuenta intentando trasladar la demanda a quién pudiese gestionarla, en este caso, su *Hosting*. Además se le facilitaría un teléfono o email de contacto para que contactase posteriormente comunicando que acciones ha llevado a cabo y lo conseguido con las mismas.

Con esto se finalizaría el apartado dedicado a las vías de comunicación con los contactos. Evidentemente no son todas las existentes y es posible que surjan algunas nuevas durante la gestión de los casos que no hayan sido mostradas aquí. No obstante, los pilares donde se fundamentan estas vías de comunicación alternativas están basadas en lo aquí mostrado y además, la mayoría de las veces, los medios más utilizados y más accesibles serán los explicados.

10.2 Con quién contactar

Una vez vistos los métodos de contacto, se va a proceder a mostrar los principales objetivos de estos.

Evidentemente no todos tienen la misma importancia, no obstante la suma de las aportaciones de todos ellos será la que colabore en mayor medida al temprano cierre del caso.

Lógicamente, es posible que aparezcan nuevos contactos en el proceso de tratamiento de un caso, sin embargo, estos son los más habituales.

10.2.1 Administrador/Propietario Dominio (Registrante)

Como ya se ha comentado, este contacto puede no ser un contacto corporativo y tratarse de cualquier tipo de persona anónima por lo que en este caso se requeriría de un trato menos técnico para poder hacerle llegar el problema con la mayor claridad posible.

En caso de tratarse, como ya se ha dicho, de un contacto no corporativo, es poco probable que tenga pleno acceso a las carpetas del *Dominio,* por lo que su ayuda será muy limitada, al menos de manera directa.

Teniendo en cuenta lo anterior, habría que solicitar que transmitiese el caso a su *Hosting* para que actuase en consecuencia.

En caso de que, efectivamente, se trate de un contacto corporativo, es muy posible que tenga pleno acceso a las carpetas de la web, por lo que simplemente tendría que eliminar la carpeta donde se alojase el fraude y notificárselo al analista.

Este contacto es de los primeros que hay que utilizar, pues tiene implicación directa en el caso y toda la información que pueda proporcionar es de vital importancia.

Además, puede ponerse en contacto con su *Hosting* o *Registrador*, otro de los pilares en la gestión, para solicitar ayuda lo cual ahorraría mucho trabajo al analista.

10.2.2 DNS

Los propietarios de los servidores *DNS*[1] son los encargados de encaminar la conexión desde el ordenador cliente hasta el ordenador servidor del contenido.

Sin ser un elemento de gran ayuda, sí suelen proporcionar algo de información sobre el camino que realiza la conexión, de tal manera que permiten encontrar nuevos dominios fraudulentos que puedan estar obstaculizando el caso, así como nuevos contactos que puedan ser consultados y que al no pertenecer al *Dominio* destino no hubiesen podido ser obtenidos por los métodos habituales.

Contactarlos suele ser una medida extraordinaria, solo viable cuando ni los contactos del *Dominio* ni el *ISP* parecen colaborar. A menudo el encargado del *DNS* es el mismo que el encargado del *Dominio*, por lo que en estos casos solo servirá como vía alternativa de contacto en caso de no obtener respuesta en los correo de abuso (Se podrán ver ejemplos en el apartado Casos Reales).

10.2.3 Registrador

También llamado *Hosting*, es el propietario del *Dominio* y el encargado de dar soporte al *Registrante* en lo que a la administración de la web se refiere.

Tienen pleno acceso a la información de *Dominio,* por lo que pueden eliminar el fraude de manera directa.

La manera más habitual que tienen de tratar los casos de *Phishing* es a través de formularios de abuso, bastante tediosos de cumplimentar, pero muy útiles y efectivos. Sin embargo, también es posible contactarles por diversos correos departamentales que, además, suelen poner al alcance del público desde la propia web corporativa, sin necesidad de recurrir a *WhoIs.*

Junto al *ISP* y el *Registrante*, el *Registrador* (o *Hosting)* es el contacto más prioritario a la hora de solicitar un cierre al ser el último eslabón de la cadena en lo que a capacidad de gestión se refiere.

[1] *Domain Name Server* o *Servidor de Nombres de Dominios*.

Normalmente, suele ser el contacto del que más información se suele sacar con las herramientas de análisis, por lo que en una gran mayoría de casos, se suele conseguir el cierre gracias a la colaboración de estos.

10.2.4 ISP

Siglas de *Internet Service Provider* (Proveedor de servicios de Internet), son los encargados de proporcionar una conexión de red al usuario, si bien en algunos casos (como el que se trata en este documento) también ofrecen servicios de alojamiento web al consumidor (*Hosting*). En este último caso son los últimos responsables de la *IP* y por lo tanto tienen pleno acceso sobre la misma pudiendo darla de baja (la alternativa óptima de todas las que se barajan al gestionar un cierre).

En cuanto a la labor de *Hosting*, su trabajo es muy similar al del *Registrante*, llegando incluso a solaparse sus funciones.

Por su versatilidad y capacidad de gestión de la web implicada, el *ISP* es, sin duda, la mejor baza que se puede jugar a la hora de contactar con intención de cerrar un caso lo más pronto posible, no obstante, como ya se ha comentado en el apartado correspondiente al *Análisis*, son muy reticentes a gestionar bajas de *IP* y suelen requerir de una gran cantidad de información que justifique dicho proceso.

Además es, probablemente, el contacto del que menos información se podrá sacar a partir de las herramientas de análisis. Como mucho se suelen encontrar un par de correos o teléfonos y, con suerte, alguno de ellos pertenecerá al departamento apropiado para gestionar el caso.

Una vez contactados y, suponiendo colaboración plena, llegado el cierre suelen ser muy rápidos en la gestión del mismo, dando márgenes de no más de 6 horas e incluso menos para dar de baja el dominio.

10.2.5 CERT Gubernamentales

El *CERT*[1], es un organismo encargado de gestionar incidentes informáticos en el ámbito empresarial (ver Anexo) o, como en el caso que ocupa, internacional entre otros muchos que no son relevantes al caso. Aunque siempre son informados al inicio de cada caso al informar al cliente de la apertura del mismo, es un recurso que se debe utilizar siempre en última instancia, pues su motivación se fundamenta en una labor mucho más compleja e importante como es la gestión de incidentes relacionados con *Ciberterrorismo* y derivados.

En casos muy extremos si se puede solicitar soporte a esos organismos, que podrían actuar directamente en el caso y exigir el cierre del *Dominio* de manera legal en caso de producirse un prejuicio desmedido al cliente o a cualquier otro organismo de importancia internacional o nacional elevada.

[1] *Computer Emergency Response Team.*

Todos los *CERT* tienen un correo de contacto que se puede encontrar con una simple búsqueda en Internet ya que éstos son públicos.

Respecto a los casos que requieran de contactar con *CERT* de este tipo, se hablará más adelante en la siguiente sección, sin embargo, más adelante se verá que, siempre que se envíen correos de abuso por primera vez, es recomendable poner en copia al *CERT Gubernamental* correspondiente. Esto se hace por si el caso se complicase en exceso y tuviesen que proporcionar ayuda legal. En este caso estarían al tanto de lo acontecido en el caso desde el principio y podrían revisar lo ocurrido para actuar en consecuencia.

10.3 Casos especiales

Es importante entender que no siempre se desarrollan los acontecimientos como se espera y mucho menos en un mundo tan cambiante como el del delito informático. A pesar de haber intentado elaborar una guía lo más fidedigna posible a las situaciones a encontrar en la vida real, es fácil encontrarse con casos que se desarrollen por caminos alternativos o incluso totalmente opuestos al aquí presentado.

Evidentemente es imposible controlar todos esos casos y mucho menos explicar aquí como proceder ante ellos, en estas circunstancias prima la experiencia del analista y la intuición sobre quien o quienes pueden ser útiles o importantes en el tratamiento del caso.

Por ello no se va a dar una guía de pasos alternativos, pues no existe tal, pero si se van a desglosar algunos puntos importantes que puedan servir de ayuda para abordar casos que se compliquen en exceso:

- ***Estudiar casos pasados***: Revisar casos ya cerrados recientemente o que hubieran tenido un patrón de actividad similar puede ser de gran ayuda para saber qué pasos realizar y evitar pérdidas de tiempo en busca de información que ya se sabe cómo obtener. La idea es aprender de lo realizado y sacar conclusiones de todos los casos gestionados que favorezcan el progreso del caso actual.
- ***Comprobar casos relacionados***: Aunque esto se debe hacer siempre antes de abrir un caso, en estas situaciones excepcionales es mucho más recomendable. La mayoría de los casos que se dan de alta por un analista son casos que ya tuvieron su antecedente en otro momento anterior, si por suerte el analista ya trabajó en alguno de ellos, la gestión del caso podría simplificarse en gran medida.
- ***Utilizar herramientas alternativas***: En Internet hay multitud de herramientas con fines similares a las aquí mostradas pero que devuelven resultados ligeramente diferentes. La capacidad de personalización de muchas de ellas o la simple programación de las mismas, pueden hacer que se devuelvan extras de información que no se pueden obtener con las habituales. Estos extras de información pueden ser relevantes para un caso, como pudiesen ser contactos nuevos, nuevas *Uri* relacionadas,…etc.
- ***CERT Gubernamentales***: Como ya se ha explicado, estos organismos pueden ser de ayuda en casos de extrema necesidad, al tener autoridad legal sobre los dominios de un ámbito geográfico, pueden exigir el cierre de *IP's* de manera inmediata, si se les

proporciona información suficiente y contrastada. Lógicamente este hecho está muy restringido y es muy improbable que se llegue a tal extremo, por lo que no se debe confiar en que suceda tal cosa. Sin embargo sí se dan casos en los que dan soporte interesándose por la evolución de los mismos cada cierto tiempo y proporcionando recomendaciones al analista para poder seguir avanzando.

- ***Esperar novedades***: Finalmente si nada de lo anterior ayuda puede ser ventajoso dejar el caso durante unos días y continuar gestionando otros que haya en paralelo. Con esto se consigue tiempo para que los contactos lleven a cabo las acciones oportunas y, quizás, se proporcione nueva información al analista para poder continuar con el caso.

Para finalizar cabe indicar que no hay ningún caso que sea imposible de gestionar al cierre. Cuesten más o menos, todos pueden ser cerrados en mayor o menor tiempo, aunque esto no quiere decir que siempre esté en manos del analista dicho cierre, a veces se requiere de colaboraciones entre organismos de seguridad para aunar fuerzas y conseguir llevar a cabo una gestión exitosa del caso. No obstante, estos casos representan un porcentaje ínfimo de todos a los que se va a enfrentar el analista en su vida laboral y no deben suponer una preocupación en el desempeño de su trabajo. Un ejemplo de estos casos es el que se verá en la sección Casos Reales, donde las llamadas *bullet proof ISP* entran en juego.

10.4 Plataforma de Seguimiento

Una vez vistas todas las acciones posibles de llevar a cabo y los contactos a los que comunicar el caso, es evidente que se requiere de algún tipo de soporte donde registrar todas las comunicaciones y las acciones realizadas.

La *Plataforma de Seguimiento* no deja de ser el núcleo de la actividad del analista, pues cada día deberá revisar la información almacenada en ella para poder hacer un mapa de ruta de cada caso.

Como es lógico la estructura de la *Plataforma de Seguimiento* es totalmente personal y cada empresa decidirá que es o no esencial de registrar a la hora de gestionar el caso, no obstante, a continuación se van a mostrar los puntos que, como mínimo, debería contemplar para un óptimo registro de las acciones llevadas a cabo para después mostrar cómo llevar a cabo un proceso de alta y de baja de un caso.

10.4.1 Identificador de caso

Evidentemente es necesario un identificador para cada caso gestionado. Este identificador debería ser autodescriptivo, es decir, dar la suficiente información para que el analista rápidamente sepa de qué caso se trata.

Como recomendación, en el identificador debería aparecer un código interno de información asociada a la entidad suplantada y, por ejemplo, la fecha de alta del caso.

Por ejemplo si se estuviese ante el caso de un Banco Ficticio, un tipo de código para dicha entidad podrían ser sus siglas, BF, asociadas a la fecha de alta, por ejemplo:

BF27012015

Este identificador, será el que se utilice para contactar con la entidad afectada informando del caso en los correos de apertura, información de avance y cierre del mismo, por lo que sería necesario proporcionar de antemano la tipología de código a utilizar a dicha entidad, para que pudiesen organizarlo en sus bases de datos a la par que la *Plataforma de Seguimiento*.

Por otro lado y para evitar confusiones habría que incluir algún símbolo o carácter especial que faciliten al analista la identificación de casos reabiertos o de subcasos.

Por ejemplo el símbolo "*" podría utilizarse para asociar un identificador a la reapertura de un caso antiguo que se haya reactivado, en el ejemplo anterior sería:

*BF27012015**

Con esto el analista sabría que está ante un caso ya gestionado anteriormente y podría continuar en el punto en que fue dejado.

En caso de tratarse de un subcaso (más adelante se explicarán en detalle) podría poner un prefijo al identificador, por ejemplo, una "S":

SBF27012015

Si por algún motivo diese la coincidencia de que se tratase de la reapertura de un subcaso, se podrían combinar ambos identificadores:

*SBF27012015**

El identificador de cada caso debería estar siempre visible en el apartado general donde aparezcan todos los casos gestionados.

10.4.2 URI

La *Uri* es una cadena de caracteres que identifica la dirección web asociada al fraude.

Es esencial que esta se almacene pues, sin ella, es imposible localizar la web que aloja el fraude.

Es importante tratar las *Uri's* de manera diferente a si pertenecen a *Phishing y Redirectoes* o a *Troyanos.*

En el caso de que pertenezca a un Phishing o a un *Redirector h*ay que tener en cuenta que al almacenar la *Uri* se debe comprobar la raíz de la misma en la que se encuentra el fraude, es decir, en que carpeta del servidor se ha alojado.

Para ello, lo primero que hay que conocer es la estructura de las *Uri's*:

http://www.dominio.ru/Carpeta/Subcarpeta1/.../SubcarpetaN/archivo.html

Una vez conocida la estructura, la idea es ir probando *Uri's* extraídas a partir de la básica. Esto se consigue eliminando partes de la misma partiendo del archivo y retrocediendo por las subcarpetas y carpetas hasta comprobar en qué carpeta contiene el fraude.

Por ejemplo en el caso de la *Uri* anterior la secuencia de pruebas sería la siguiente:

http://www.dominio.ru/Carpeta/Subcarpeta1/.../SubcarpetaN

http://www.dominio.ru/Carpeta/Subcarpeta1

http://www.dominio.ru/Carpeta

http://www.dominio.ru

En cada prueba pueden darse dos posibilidades:

- ***Que se muestre el Phishing como en la Uri inicial:*** En este caso se seguiría con las siguientes pruebas hasta dar con la carpeta que lo contiene.
- ***Que se muestre el contenido de la carpeta en el servidor:*** En este caso habría que probar cada archivo para comprobar cual pertenece al *Phishing*. Esta segunda opción es la óptima, pues permite localizar de manera inequívoca el fraude e indicar al responsable el archivo concreto que debe eliminar.

Ilustración 28: Ejemplo de muestra de contenido de una carpeta en el servidor.

Es posible que un caso contenga varias *Uri's* asociadas, en este caso la que debería aparecer en el apartado general es la más representativa de todas ellas o, en su defecto, la primera *Uri* reportada. El resto de *Uri's* debería estar incluidas en la información detallada del caso.

10.4.3 Fecha de apertura/Cierre

Importantes para conocer cuánto tiempo ha transcurrido desde que el caso se abrió hasta que se cerró.

Deberían aparecer en el apartado general junto al *Identificador* y la *Uri.* Además también es interesante registrar las horas de apertura y cierre para obtener mayor precisión aún.

Esta información será proporcionada al cliente afectado para que ellos también puedan llevar el control del caso desde que fue abierto hasta que se cerró.

10.4.4 WhoIs

Una vez dentro de la información de cada caso, es imprescindible tener a mano toda la información posible del mismo. El *WhoIs* es el punto de partida óptimo para comenzar a realizar acciones, por lo que, tener uno siempre visible dentro del caso puede ahorrar mucho trabajo.

10.4.5 Estado del caso

Puede haber tres tipos:

- ***Abierto:*** El caso está en proceso de gestión y no se ha eliminado todavía.
- ***Cerrado:*** El caso ha sido eliminado, notificado y puesto en monitorización permanente.
- ***Reabierto:*** El caso pertenece a un fraude ya gestionado que por cualquier motivo se ha reactivado y vuelve a estar en proceso de gestión.

10.4.6 Observaciones

Como se ha repetido en varias partes del documento, no todos los casos son iguales. Cada uno tiene sus particularidades que lo hacen especial en la gestión. Cualquier dato o percepción anómala que el analista observe en el análisis del caso, debe notificarla en el apartado destinado a ello.

Por ejemplo, es recomendable anotar posibles *Uri's* afectadas pero que no han sido comprobadas, *Ip's* involucradas, contactos especiales encontrados, acciones que haya que llevar a cabo en un determinado momento…etc.

10.4.7 Acciones

Evidentemente lo más importante es registrar las acciones llevadas a cabo a lo largo del proceso de gestión.

Para ello es importante indicar que tipo de acción se han realizado de las siguientes:

- ***Envío de correo electrónico:*** Se ha enviado un email a determinado contacto, es importante anotar la dirección de correo del contacto.
- ***Recepción de correo electrónico:*** Se ha recibido una respuesta a un correo enviado anteriormente, a una comunicación por chat o a un formulario cumplimentado, es importante anotar la respuesta obtenida.
- ***Contacto por Formulario:*** Se ha cumplimentado un formulario y se permanece a la espera de respuesta. Es importante apuntar la web donde se ha rellenado el formulario y, en caso de haberlo recibido, el número de ticket recibido para posteriores actualizaciones.
- ***Actualización de ticket:*** Se ha recibido una nueva respuesta en un ticket abierto por un formulario anteriormente cumplimentado. Se anotará la respuesta obtenida en la actualización.

- ***Contacto por Chat:*** Se ha contactado vía chat en alguna web relacionada con el caso. Se deberá anotar la web y la respuesta obtenida, tanto si ha sido inmediata como si se permanece a la espera de la misma.
- ***Contacto vía telefónica:*** Se ha realizado una llamada telefónica a algún contacto relacionado con el caso. Se anotará el número y la respuesta obtenida, así como cualquier detalle que pueda ser importante.

En cualquiera de las acciones realizadas es primordial indicar la hora a la que se llevaron a cabo para llevar un control entre el momento del contacto y la respuesta al mismo.

10.5 Apertura de casos

Controlados ya los parámetros que se deberían registrar en la *Plataforma de Seguimiento*, es momento de conocer el procedimiento a llevar a cabo cuando se vaya a abrir un nuevo caso.

En primer lugar, suponiendo que la *Uri* a dar de alta está activa, es necesario comprobar si ya está en algún caso abierto gestionándose o se trata de algún caso antiguo ya cerrado y que podría haberse reactivado. Para ello se realizaría una búsqueda por *Dominio* exclusivamente entre todos los casos almacenados.

Una vez comprobadas las coincidencias, se pueden dar tres situaciones respecto a las coincidencias:

- ***La nueva Uri difiere en la IP:*** Simplemente se abriría un nuevo caso totalmente independiente del resto.
- ***La nueva Uri comparte IP y tipo de fraude en un caso ya cerrado:*** Por ejemplo, se quiere abrir un caso de *Phishing* y se encuentra otro caso de *Phishing* ya cerrado, con el mismo *Dominio* e *IP.* Se trataría de una reapertura de caso, por lo que habría que abrir un caso nuevo pero indicando que se trata de una reapertura (Ya sea en el Identificador como se indicó anteriormente o en algún apartado dedicado a observaciones). En esta circunstancia en particular, habría que comprobar cuál fue la acción o acciones determinantes en la resolución del caso la primera vez para repetirlas e intentar cerrar el caso de nuevo.
- ***La nueva Uri comparte IP y tipo de fraude en un caso abierto:*** En esta caso no habría reapertura lógicamente y se trataría de un caso que ya se está gestionando, simplemente se añadiría la *Uri* al caso ya abierto junto a la original y se notificaría al cliente la nueva *Uri* encontrada.
- ***La nueva Uri solo comparte IP y es un tipo de fraude distinto:*** Por ejemplo se quiere abrir un caso de *Phishing* y se encuentra un caso con el mismo *Dominio* e *IP* pero que pertenece a un *Redirector*. En este tipo de casos como el patrón de acceso es primero al redirector y desde este al *Phishing*, este último se abriría como un subcaso del anterior.

Hay que indicar que se pueden dar algunos casos muy extraños como por ejemplo, *Uri's* exactamente iguales pero que difieren en la *IP,* algo a priori, imposible. Lógicamente estos casos son altamente improbables, por lo que no se tratarán en este documento.

Entendidos los conceptos a tener en cuenta para abrir el caso, simplemente quedaría mandar los correos de notificación al cliente afectado en caso de que fuese necesario y proceder a la gestión del mismo.

10.6 Verificación de cierre de caso

Llegado este punto, ya se tienen todos los medios al alcance para proceder al cierre de un caso. Sin embargo, el cierre definitivo no es tan sencillo como pudiese parecer, pues intervienen varios factores en ello que no siempre se tienen en cuenta.

Suponiendo que se haya recibido una notificación en la que se indique que un caso ha sido eliminado, es momento de proceder a su comprobación.

El primer paso y el más simple, consiste en realizar la misma labor que se llevó a cabo para comprobar la actividad de un nuevo caso. En caso de obtener resultados de actividad negativos en todas las pruebas se podría confirmar que, efectivamente, el caso está cerrado.

Una vez verificado, es necesario incluir la/s *Uri*/s en algún tipo de aplicación de monitorización que permita mantener una vigilancia constante sobre la misma. Esto es necesario debido a que hay muchas posibilidades de que el caso sea reabierto en un futuro o de que forme parte de otro.

Este tipo de aplicaciones mantiene un control sobre las *Uri* que se le introduzcan y muestran alertas en caso de variaciones en su actividad.

Una vez puesto en monitorización, es necesario informar del cierre al cliente y de proceder a cambiar su estado a “Cerrado” en la *Plataforma de Seguimiento* (ver el apartado correspondiente en la sección de Eliminación).

Para informar al cliente simplemente se le mandará un correo informándole del identificador del caso con el nuevo cambio de estado.

Además de lo anterior, es recomendable contestar al contacto que haya informado del cierre para que sea consciente de que se ha recibido el reporte y se ha eliminado el caso. Con esto se consigue que el contacto de por finalizada la gestión del mismo y cerrar formalmente la comunicación.

Con este apartado se finaliza la estructura principal del documento, para finalizar se mostrará un resumen explicativo de todo lo mostrado que permitirá sintetizar más rápidamente todo lo aprendido.

10.7 Proceso de monitorización

Este proceso realiza un seguimiento continuo sobre las *Uri’s* que se le indiquen con el fin de detectar variaciones en el comportamiento de las mismas.

Aunque aquí se ha hablado de que el proceso intenta detectar reactivaciones, en realidad, hace mucho más que eso.

El comportamiento de una *Uri* puede variar en muchos puntos y no necesariamente implican una reactivación. Así, pueden darse casos de *Uri's* cerradas que presentan cierta actividad anómala, como por ejemplo, proporcionar conexión válida a una página en blanco. Sobre el papel podría decirse que ha sido reactivada, pero en realidad no supone ningún peligro, pues carece de contenido.

Estos cambios de actividad, sin embargo, deben ser siempre controlados y notificados, pues aunque no impliquen una reactivación, sí podrían serlo en un futuro.

10.8 Informes Diarios de Seguimiento

Como es lógico, las empresas cliente necesitan *feedback* de sus casos, más aún cuando se trata de algo tan delicado como el *Fraude Online*.

Hay que tener en cuenta que, en un campo donde cada hora que transcurre puede alterar la gestión de un caso, es vital notificar, pasado el menor tiempo posible, toda la información recabada al cliente.

Se recomienda que el *feedback* sea diario, a ser posible, cada 6 horas. Con esto se estará informando 4 veces al día al cliente de todo lo que acontece en torno a los fraudes relacionados con su empresa.

Con la información enviada, el cliente se puede hacer un mapa esquemático del proceso que están siguiendo sus casos por ello, es muy importante saber qué información es relevante y cuál no.

10.8.1 Información del Seguimiento

La información mínima relevante a enviar es la siguiente:

- ***Identificador:*** Es el elemento más importante y con el que el cliente podrá organizar los casos que se están gestionando, normalmente suelen tener unos códigos propios que mapean junto a los que les han llegado en el informe para poder organizar los casos en paralelo.
- ***Acciones realizadas:*** Evidentemente el cliente necesita saber cómo se está gestionando el caso, enviarle las acciones realizadas desde el último informe, permite demostrar que el tratamiento ha sido el adecuado.
- ***Respuestas obtenidas:*** Con las acciones el cliente sabrá que se ha llevado a cabo para intentar el cierre, pero también necesitan saber que respuestas se están obteniendo, con el fin de comprobar si las acciones realizadas están siendo efectivas o no.

Evidentemente todo lo anterior debe ir acompañado de las horas exactas en las que se realizaron.

En definitiva, los informes de seguimientos son una especio de resúmenes de casos, que permiten demostrar que el analista ha trabajado correctamente los casos de la entidad. Esto, a priori inocuo para la empresa de seguridad, tiene un efecto positivo y es que, en caso de encontrar un caso extremadamente complicado de cerrar, el cliente no puede culpar a la empresa de seguridad de una mala gestión si esta demuestra cada día que está llevando a cabo su labor de manera estricta y rigurosa.

10.9 Almacenamiento de Información

Un aspecto que no se ha comentado hasta ahora pero que es clave, es la delicadeza de la información que se está manipulando.

No hay que olvidar que se están gestionando casos de entidades financieras y similares por lo que, toda información que se recopile con herramientas privadas o que sea proporcionada por el cliente mismo, tales como datos asociados a un *Troyano*, correos recibidos o enviados, formularios cumplimentados…etc, deben ser puestos a buen recaudo dentro de servidores dedicados propiedad de la empresa de seguridad y nunca expuestos a terceros, salvo previo consentimiento de los implicados.

No hay que olvidar que las empresas de seguridad también son objetivos del ciberataque, por lo que hay que extremar las precauciones siempre que se maneje información susceptible de ser robada.

Por ejemplo una buena forma de mantener la información a salvo es mantenerla en los llamados *CPD*[1].

Un *CPD* es una ubicación donde se sitúan los servidores destinados a almacenar toda la información correspondiente a los clientes de la empresa, así como las operaciones realizadas sobre la misma.

Estos servidores suelen estar en posiciones estratégicas, aisladas del resto de componentes de la empresa. Además, disponen de variados mecanismos de seguridad cuyo objetivo, es preservar la impunidad del *CPD* ante un intento de robo o ataque.

[1] *Centro de Procesado de Datos.*

Ilustración 29: Servidores en un *CPD*.

Estas construcciones suelen tener unos diseños específicos donde se controla hasta el más mínimo detalle, acondicionamiento del habitáculo, aislamiento eléctrico, cámaras de seguridad, detectores de movimiento, alarmas, medidas antiincendios, sumideros antiinundaciones... todo está controlado y diseñado para crear un espacio teóricamente infranqueable e inaccesible para aquellos que no dispongan del permiso correspondiente.

En el apartado correspondiente del Anexo se profundizará más en detalle sobre estos sistemas.

11.Casos Reales

Vista la gestión de un *Phishing* (o fraudes relacionados), es momento de ver algunos casos reales[1] y de qué manera se deberían gestionar siguiendo la guía aquí creada para asimilar lo leído hasta ahora.

Por simplicidad todos los casos aquí mostrados corresponden a *Phishing* o *Redirectores*, pues la gestión de *Troyanos Bancarios* y *Scam* es algo más compleja y lo que se busca es asentar los conocimientos adquiridos en este documento.

11.1 Suplantación a Google

Este caso corresponde a un email recibido el cual contiene un fichero de formato *.pdf* donde se dan instrucciones para recibir un supuesto premio en metálico en nombre de Google.

El aspecto del correo es el siguiente:

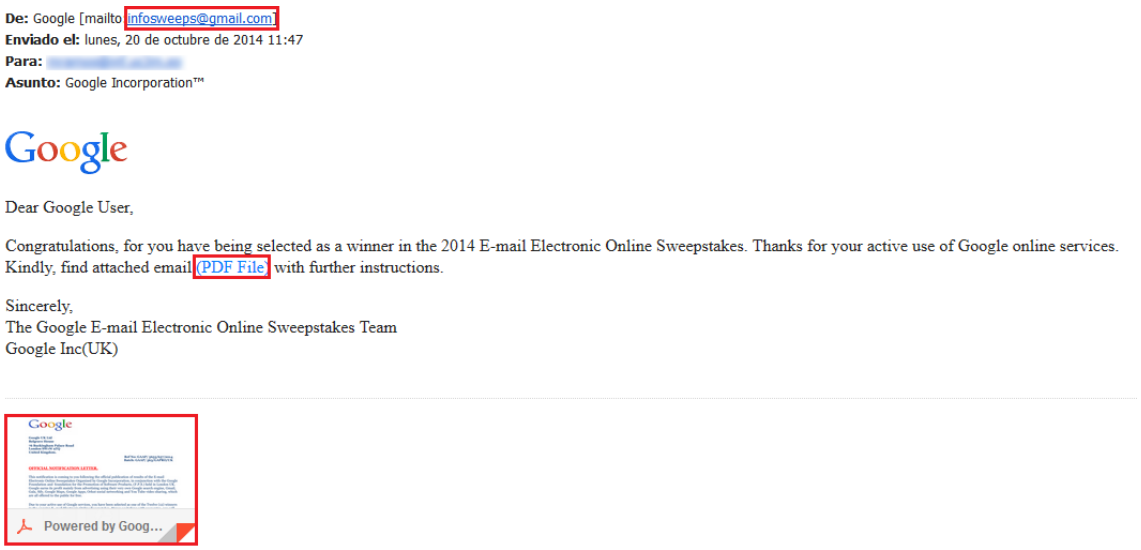


Ilustración 30: Correo de *Phishing* a Google.

El primer paso es comprobar si este correo es realmente legítimo o un intento de estafa, es decir, se va a proceder a la Detección del *Phishing*.

Lo primero que hay que hacer es analizar cuidadosamente desde donde procede el correo. En este caso se puede comprobar que el email del remitente es *infosweeps@gmail.com*. Teniendo en cuenta, como se ha explicado en este documento, que los correos corporativos

[1] *Todos los casos que se van a mostrar corresponden a Phishing reales, esto quiere decir que en el momento en que se redactaron estas líneas permanecían activos. Ninguna de las acciones que aquí se van a enseñar han sido llevadas a cabo realmente, por lo que el autor no tiene implicación alguna en el cierre de los mismos.*

deberían proceder de cuentas corporativas, esta dirección de correo resulta sospechosa, pues *infosweeps* no parece corresponderse a ningún departamento de Google.

Además, un truco que puede despejar dudas, es realizar una búsqueda en Internet con la dirección de correo electrónico. En este caso tras realizar la búsqueda, vemos que la primera entrada que nos muestra el buscador corresponde a una página de recopilación de *Phishings* (donde uno de ellos es exactamente el analizado en este caso) por lo que es un claro indicio de que se está ante un intento de estafa y que debería ser descartado y reportado inmediatamente.

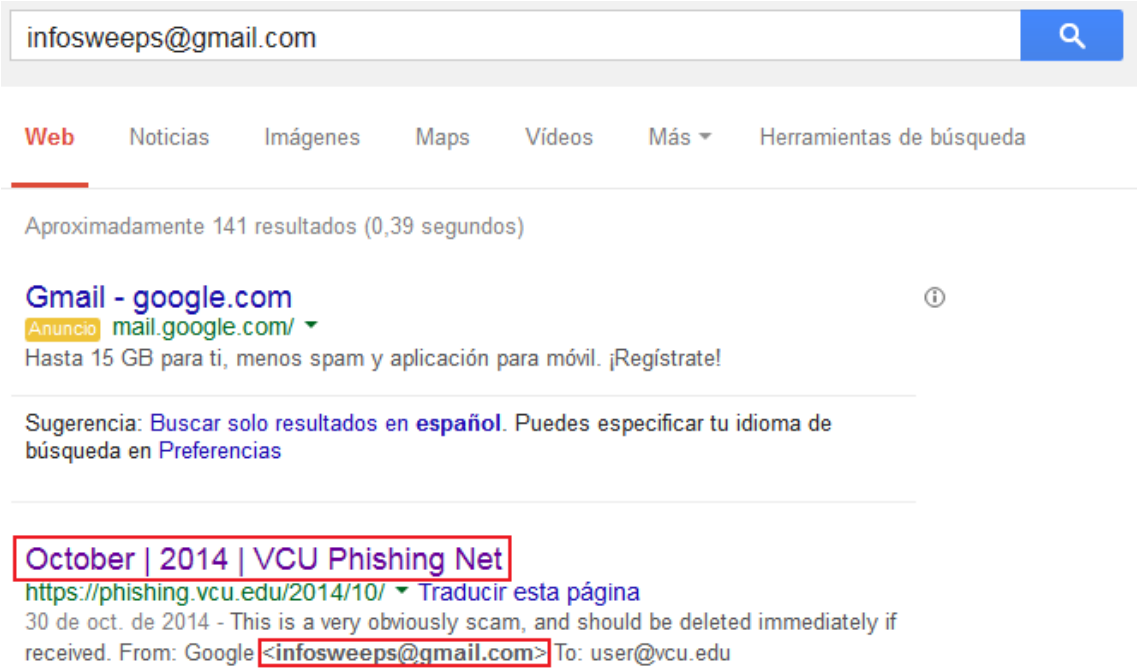


Ilustración 31: Resultado de la búsqueda del supuesto remitente fraudulento en Google.

Como este truco no siempre resulta, se va a continuar el proceso de detección ignorando el hecho de que ya se ha descartado como legítimo.

Lo siguiente que llama la atención es que el correo está escrito en Inglés, aunque no tiene que implicar necesariamente un caso de fraude, sí es extraño que se proceda a la entrega de un premio desde un país extranjero con el que el destinatario no tiene nada que ver.

Además, en este caso, la empresa implicada es Google, evidentemente, como empresa internacional que es, no debería tener problemas en el empleo de varios idiomas para comunicarse con sus clientes, por lo que en este caso en particular si es un indicio claro de *Phishing*.

Continuando con el cuerpo del mensaje, en la firma del mismo se puede ver como el departamento del que supuestamente procede el correo es "*Electronic Online Sweepstakes Team*", lógicamente no es posible conocer todos los departamentos de los que dispone Google pero, de nuevo, se puede realizar una búsqueda por Internet. Si dicho departamento existiese,

probablemente como resultado de la búsqueda se obtendría algún tipo de página corporativa de Google con acceso directo a información del mismo.

En este caso lo que se obtiene, lejos de cualquier página corporativa, es una cantidad innumerable de resultados con usuarios preguntando de donde proceden correos con tal departamento como remitente e, incluso, algunas entradas afirmando que corresponde a un caso de *Phishing* masificado.

Al igual que en el caso del email remitente podría darse por concluida la detección positiva, pero como el objetivo es contemplar todas las posibilidades, se va a continuar hasta agotar todos los elementos de análisis para la posible detección del fraude.

Visto el cuerpo del correo, es momento de comprobar el archivo adjunto. El propio cuerpo del mensaje advierte de que es un documento en formato *.pdf* por lo que en este caso, a priori, no habría *Uri's* implicadas en el mensaje. No obstante, el hecho de contener archivos adjuntos, ya de por sí, es un elemento altamente sospechoso de fraude, pues como bien se ha dicho, las entidades oficiales no utilizan estos recursos para el envío de información.

Hay que recalcar que, como en cualquier caso susceptible de ser fraudulento, cualquier archivo relacionado puede estar infectado, por lo que se intentará, en la medida de lo posible, dar por concluida la detección evitando acceder a cualquier archivo. En caso de no ser esto posible, el acceso deberá hacerse previo análisis de los mismos por parte de antivirus domésticos y herramientas de detección de confianza como *Virus Total*. En este caso tras realizar el análisis se comprobó que el archivo estaba libre de código malicioso y que su apertura era, en principio, segura (Ver captura en el apartado de la herramienta *Virus Total* del Anexo).

Abierto el archivo, lo primero que llama la atención es el estilo del mismo. Los colores si pretenden simular ser los corporativos de Google (Rojo, Azul…etc), sin embargo, el empleo de los mismos parece poco "profesional", dando más un aspecto de documento doméstico que oficial. Además, de nuevo, el contenido y las instrucciones de pago están redactados en inglés, por lo que se imposibilitaría la supuesta entrega del premio para alguien que no dominase la lengua.

Al margen de lo anterior, hay tres detalles que destacan sobre el resto y que no dejan lugar a dudas de que el caso es un positivo de *Phishing*.

- El primero, es el hecho de que el premio se entregue en libras británicas, moneda que en el país del destinatario no es válida.
- El segundo, el hecho de que se solicite contactar con un supuesto administrador al que proporcionarle una cuenta bancaria.
- El tercero, el contacto del supuesto administrador.

Con los dos primeros ya se podría concluir el caso como *Phishing* pero, además, si se analiza el correo de contacto del administrador, "*sergeybrin@gpawardprom.com*" es fácil ver que el *Dominio* del mismo no pertenece a Google. De hecho, si se intenta acceder al *Dominio* en Internet, el resultado es una página en blanco, con lo que aquí podría darse por finalizada la detección con un positivo en *Phishing*.

Google

Google UK Ltd
Belgrave House
76 Buckingham Palace Road
London SW1W 9TQ
United Kingdom.

Ref No: GAAP/ 5653/657/2014
Batch: GAAP/ 563/GAPRO/UK

OFFICIAL NOTIFICATION LETTER.

This notification is coming to you following the official publication of results of the E-mail Electronic Online Sweepstakes Organized by Google Incorporation, in conjunction with the Google Foundation and foundation for the Promotion of Software Products, (F.P.S.) held in London UK. Google earns its profit mainly from advertising using their very own Google search engine, Gmail, Gala, Sify, Google Maps, Google Apps, Orkut social networking and You Tube video sharing, which are all offered to the public for free.

Due to your active use of Google services, you have been selected as one of the Twelve (12) winners in the ongoing E- mail Electronic Online Sweepstakes. Hence we believe with your prize, you will continue to be active in your patronage to Google and its Products. A Bank Draft of £950,000.00 GBP {Nine Hundred and Fifty Thousand Great British Pounds} will be issued in your name by our Foreign Payment Bureau and also a certificate of prize claim will be processed alongside your Bank Draft.

You are advised to get back to us with the following details below for the Processing of your Claims:

FOREIGN PAYMENT RELEASE FORM.
(1) Your Contact Address:
(2) Your Contact Telephone/Mobile Number:
(3) Your Nationality/Country:
(4) Your Full Names:
(5) Occupation:
(6) Age/Gender:
(7) Marital Status:
(8) Private Email Address:
(9) Ever Won An Online Lottery?
(10) How Do You Feel As A Winner?

Mode of Prize Remittance.

1. Bank Transfer: (Bank Transfer of your official winning prize to your bank account).

2. Courier Delivery Of your Certified Winning Cheque/Bank Draft in your Name and other Winning Documents safely to you.

NB: You are advised to contact our Foreign Payment Bureau through the claims administrator with the details below for the processing of your payment.

.....

Sergey Brin,
Claims Administrator,
Email: sergeybrin@gpawardprom.com

.....

Congratulations from the Staffs & Members of Google Board Commission.

Ilustración 32: Documento adjunto en el caso de *Phishing* a Google.

Acabado el proceso de Detección, es el momento de proceder a recabar información en el proceso de Análisis.

En este caso, al ser un *Phishing* que no afecta a una entidad bancaria y que no contiene *Uri´s* implicadas, la única vía de análisis posible es recabar información acerca del único *Dominio* involucrado, "*gpawardprom.com*".

Si se realiza un *WhoIs* del *Dominio* (ver ejemplo de captura completa en la sección *WhoIs* del Anexo), se obtienen los siguientes resultados:

- El registro o *Hosting* corre a cargo de la empresa "*1and1.com*", la cual dispone de un departamento de abuso a tenor del email de abuso mostrado, "*abuse@1and1.com*".

Ilustración 33: Información del *Registrador* del *Dominio* "*gpawardprom.com*".

- El *Registrante* del *Dominio* parece ser un particular llamado Maynard Taylor con email de contacto "*taylormaynard993@yahoo.com*" procedente de Estados Unidos con domicilio en la ciudad Hesperia, California, en la calle St. Wilson 4036, con número telefónico (760)9473454[1].

Ilustración 34: Datos del *Registrante* del *Dominio* "*gpawardprom.com*".

[1] *Hay que recordar que todos los datos mostrados son absolutamente públicos, por lo que su exposición en este documento no violan ningún derecho del individuo.*

Con estos datos llama la atención toda la información que se consigue del *Registrante* con una simple búsqueda, donde se puede localizar su domicilio sin margen de error. Esto lleva a dos conclusiones:

- El *Registrante* ha sido víctima de un *hackeo* a su página web, donde alguien está realizando el *Phishing* a Google en nombre de su dominio.
- El *Registrante* es el propio *Pirata Informático* autor del *Phishing.*

La segunda opción parece remota e improbable, pues ningún ladrón expondría sus datos tan a la ligera. Sin embargo, es sorprendente la cantidad de personas que, sin conocimientos básicos de seguridad, se lanzan a probar fortuna en el delito Online sin unas medidas de protección mínimas ante su identificación, originando auténticos despropósitos como el escenario contemplado en el segundo punto.

Evidentemente se va a suponer que el caso planteado corresponde a la primera suposición, es decir, detrás del *Phishing* hay *Piratas Informáticos* con conocimientos avanzados o profesionales que no cometerían errores tan absurdos.

Por otro lado, la información respectiva a la *IP* obtenida, dice que el *ISP* también es *"1and1.com",* pero añade un correo más, que parece corresponder al departamento técnico, "*arin-role@oneandone.net*".

Llegado este punto se habría concluido el proceso de Análisis. Es momento de mostrar las acciones a llevar a cabo para proceder a la Eliminación.

Con los datos obtenidos hay que centrar los esfuerzos en el *Registrador* (e *ISP*), "*1and1.com*" que es quien puede administrar el dominio. Como se ha obtenido un correo de abuso, lo principal es mandar un correo explicando el caso a la dirección proporcionada por el *WhoIs abuse@1and1.com* poniendo en copia al *CERT* estadounidense para tenerlos informados del caso por si en un futuro fuese necesario contactar con ellos.

Recibido este correo la empresa se pondría en contacto con el *Registrante* (del cual también se conocen los datos y será el siguiente contacto a utilizar) para gestionar la baja de su *Dominio* de tal manera que el falso correo de administración proporcionado por el documento adjunto en el email sea inutilizado. Es indispensable mandar el correo en un idioma con el que la empresa trabaje, en este caso, al tratarse de un *Dominio* estadounidense, es recomendable hacerlo en inglés.

En el cuerpo del correo se deberá identificar la empresa denunciante (nunca al analista) e informar de que se ha sido informado de un caso de *Phishing*, que está afectando a un cliente en concreto del *Registrador*.

En concreto se solicitará el cierre del *Dominio* con la intención de inhabilitar el email fraudulento que corresponde al supuesto administrador de Google y se proporcionará la información relativa al cliente.

Además, como prueba, siempre se adjuntará una copia del *WhoIs* obtenido donde, efectivamente, se demuestre que la empresa contactada está involucrada en el la gestión del caso.

abuse@1and1.com

Phishing detected

Hello,

We are ____ an IT Security Company From ____, I contact you because I've received a suspected Phishing email from Google. Its content is attached in a screenshot of it.

The registrant is a user called Maynard Taylor and his email is taylormaniard993@yahoo.com. Can you contact him and proceed to remove the domain? Currently the domain shows nothing and it is being used in fake email account manager on the attachment to the email.

The Whols is the next:

Domain Name: gpawardprom.com
Registry Domain ID: 12200173
Registrar WHOIS Server: whois.1und1.info
Registrar URL: http://1and1.com
Updated Date: 2014-02-21T00:00:00Z
Creation Date: 2014-02-21T00:00:00Z
Registrar Registration Expiration Date: 2015-02-21T00:00:00Z
Registrar: 1&1 Internet AG
Registrar IANA ID: 83
Registrar Abuse Contact Email: abuse@1and1.com
Registrar Abuse Contact Phone: +1.8774612631
Reseller:
Domain Status: clientTransferProhibited
Registry Registrant ID:
Registrant Name: Maynard Taylor
Registrant Organization:
Registrant Street: 4036 Wilson St
Registrant City: Hesperia
Registrant State/Province: CA
Registrant Postal Code: 92345
Registrant Country: US
Registrant Phone: +1.7609473454
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: taylormaynard993@yahoo.com

Ilustración 35: Ejemplo de correo de abuso enviado a *1and1.com*.

Además de la información proporcionada habría que adjuntar una captura del cuerpo del mensaje del *Phishing*, además del *.pdf* adjunto al mismo.

Con esto simplemente habría que esperar una respuesta. No obstante como se dispone de la información de contacto del *Registrante*, no estaría de más enviarle otro correo a él informándole, de nuevo en su idioma, de que puede estar siendo víctima de una suplantación

de identidad que le afecta de manera directa. La idea es la misma que la del anterior correo pero en el sentido inverso, es decir, informar al *Registrante* para que contacte con su empresa de *Hosting*, *1and1.com* y que esta le proporcione soporte.

Una vez recibida respuesta de cualquiera de los dos contactos y, suponiendo que el caso se haya gestionado hasta el cierre del *Dominio,* solo quedaría comprobar si dicho cierre ha sido efectivo para dar por cerrado el caso.

Para ello, se accedería al *Dominio* reportado como fraudulento y se tendría que comprobar que se obtiene un mensaje de tipo 4XX, a ser posible un 404, que indique que el *Dominio* no existe.

Para ello como el navegador no siempre es fiable, se podría recurrir a algún tipo de herramienta de análisis de código *HTML*, así como de herramientas que camuflen el origen de la conexión. De esta manera no habría duda de la actividad de la página y podría verificarse la respuesta obtenida por el contacto y proceder al cierre definitivo del caso.

11.2 *Redirector* a *Phishing* de Barclays

Este caso es algo más complicado que el anterior, pues implica a un *Redirector* que finaliza en un *Phishing*, por lo que supondría la gestión de un caso (*Redirector*) y un subcaso (*Phishing*) en paralelo.

Este caso corresponde a una *Uri* fraudulenta, probablemente asociada a algún correo de los que ya se han visto algunos ejemplos anteriormente en este documento.

Como la estructura y contenido de los correos suele ser similar y ya se ha hecho un análisis exhaustivo de uno parecido en el caso anterior, se va a proceder directamente al proceso de Detección analizando la actividad de la *Uri.*

Para comenzar la *Uri* bajo sospecha es la siguiente:

http://jyyoi.com/blog/wp-includes/images/smilies/textfiles/Pool=69/

Esta *Uri,* de entrada, ya no contiene un *Dominio* conocido de la entidad *Barclays*, por lo que se puede asegurar que es altamente sospechosa de fraude.

Lo primero que hay que hacer es echar un vistazo entrando desde el navegador, para ver cómo se comporta en un primer momento. Una vez realizada la conexión se puede ver que, efectivamente, lleva a una página asociada a la entidad bancaria *Barclays*. Hasta aquí todo podría parecer normal, sin embargo, hay un detalle que delata a la *Uri*.

Si se presta atención, la *Uri* que aparece en el navegador ha cambiado, de hecho, ni siquiera la estructura es la misma, se ha convertido en una *Uri de Datos*.

Estas *Uri's* son una modalidad bastante compleja que, si no se conoce, puede llevar a la confusión.

Lo primero que hay que entender es que las *Uri de Datos* no son direcciones web. Son direcciones que contienen algún tipo de dato (imágenes, texto, *HTML*…etc) codificado, bien en *Base64* o a través de la normativa *ASCII*. De esta manera se obtiene un código de bits representativos del dato a mostrar que, previa decodificación, será mostrada por el navegador.

La complicación que tienen estas *Uri's* es que al no poseer una estructura de dirección web, no existe un *Dominio* que investigar, por lo tanto el tratamiento habitual queda inhabilitado para este caso.

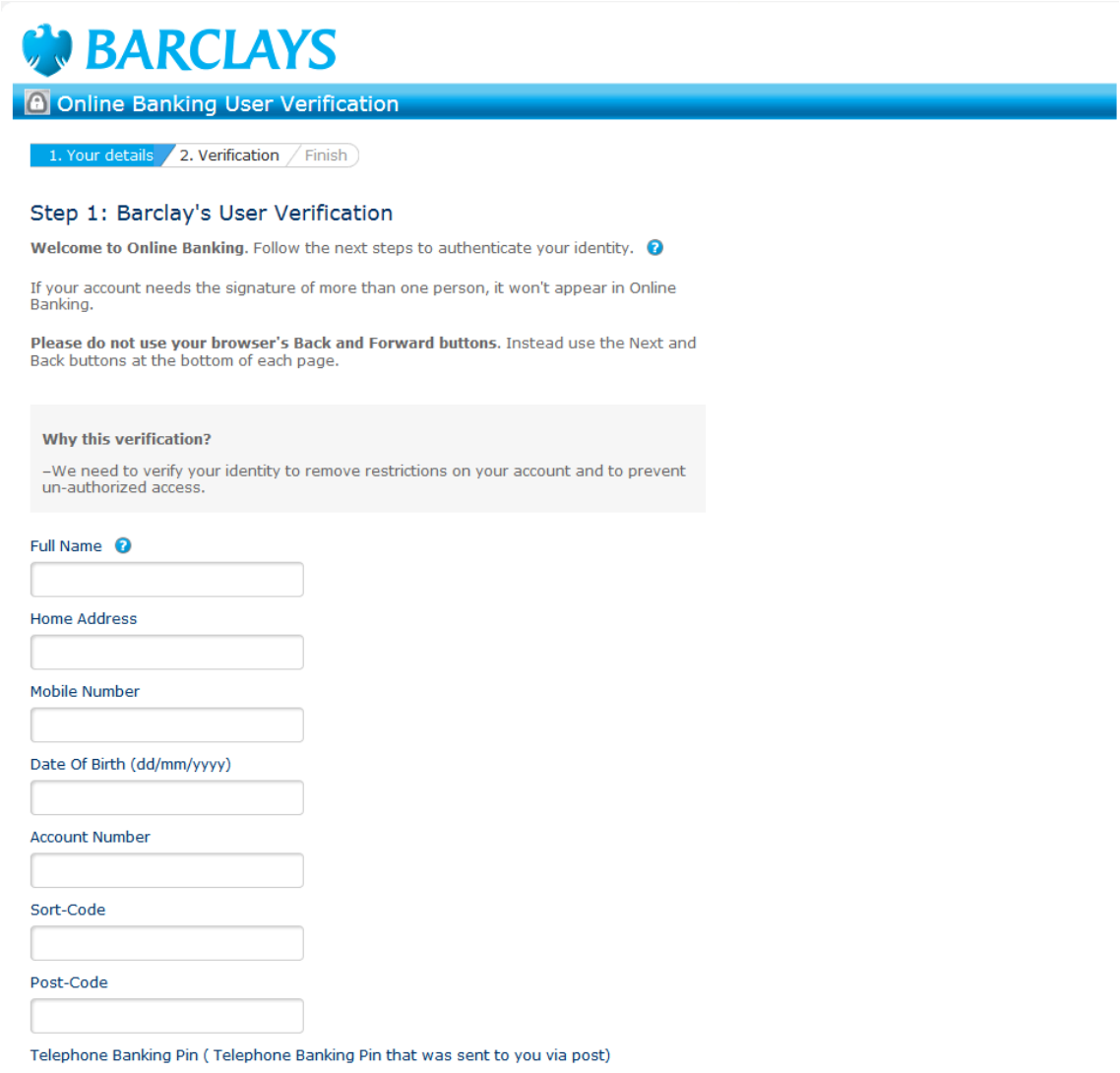


Ilustración 36: Captura de la información mostrada (*Phishing*) por la *Uri de Datos*.

Llegado este punto se dispone de dos *Uri's*, la original:

http://jyyoi.com/blog/wp-includes/images/smilies/textfiles/Pool=69/

Y la correspondiente al supuesto *Phishing* que, por extensión de la misma (4 páginas) no se va a indicar aquí al completo, sino solo la parte más relevante de su estructura:

data:text/html;base64,PCFET0NUWVBFIGh0bWwgUFVCTElD…

Vistas las *Uri's* involucradas y, teniendo en cuenta que la segunda no tiene un proceso de análisis que se corresponda con algún *Dominio,* solo queda centrarse en el *Redirector*.

Focalizar los esfuerzos solamente en la primera *Uri* no quiere decir que se vaya a dejar de lado la segunda ni a obtener un resultado diferente al habitual pues, suponiendo que el *Redirector* fuese dado de baja, la *Uri de Datos* no podría actuar por sí misma, por lo que el caso quedaría completamente cerrado.

Analizando el *Redirector* se ve rápidamente que el *Dominio* no pertenece a *Barclays* sino a "*jyyoi.com*". Lo primero que se debe hacer es entrar a dicho *Dominio* para comprobar qué tipo de web contiene.

Al entrar se puede ver lo que parece una página de diseño web, bastante lejos de la actividad que realiza *Barclays*, por lo que podría darse el *Phishing* por detectado en este punto aunque, como de costumbre, se va a seguir hasta completar el proceso de Detección.

Si se entra en la información de la web, se puede leer que la procedencia de la misma es Tailandia y aparece un correo de contacto, *design@jyyoi.com* que posteriormente en el proceso de análisis será recabado junto a otra información.

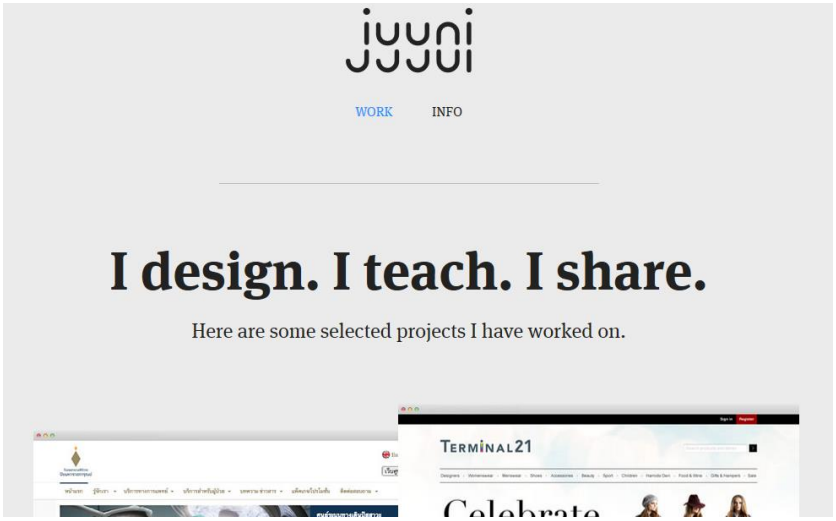


Ilustración 37: Captura de la web contenida en el *Dominio "jyyoi.com"*.

Siguiendo con el análisis de la *Uri*, es el momento de comprobar en qué parte del servidor está alojado el *Phishing*. Para ello se han realizado pruebas eliminando una a una todas las carpetas indicadas hasta obtener las siguientes pruebas:

http://jyyoi.com/blog/wp-includes/images/smilies/textfiles/Pool=69/

http://jyyoi.com/blog/wp-includes/images/smilies/textfiles (Redirigía a la anterior)

http://jyyoi.com/blog/wp-includes/images/smilies (Error de conexión)

http://jyyoi.com/blog/wp-includes/images (Error de conexión)

http://jyyoi.com/blog/wp-includes (Error de conexión)

http://jyyoi.com/blog (Conexión correcta pero sin *Phishing*)

Tras realizar la última prueba se puede llegar a la conclusión de que el *Phishing* está alojado en el *Blog* asociado al dominio.

Ilustración 38: Captura del blog asociado a la *Uri*: *http://jyyoi.com/blog*.

Con el análisis realizado se puede llegar a la conclusión inequívoca de que se está ante un caso de *Phishing.*

No obstante por si quedase alguna duda, un análisis mediante *WhoIs* podría dar la pista definitiva para su detección, además de servir como punto de enlace para el siguiente paso, el Análisis.

En este caso el *WhoIs* delata la procedencia del *Dominio* que nada tiene que ver con la entidad suplantada, por lo que ya se puede proceder a recabar información en el proceso de Análisis.

Como en el caso de *Google*, en el *WhoIs,* se obtienen los siguientes resultados (ver ejemplo de captura completa en la sección *WhoIs* del Anexo):

- El registro o *Hosting* de la web pertenece a la empresa *Enom*, de la cual se muestra un correo del departamento de abuso *abuse@enom.com* y un teléfono de contacto, probablemente en inglés por la procedencia, que es (425)2982646.

```
Domain Name: JYYOI.COM
Registry Domain ID: 1356901775_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.enom.com
Registrar URL: www.enom.com
Updated Date: 2014-11-20T18:07:38.00Z
Creation Date: 2007-12-17T11:13:16.00Z
Registrar Registration Expiration Date: 2015-12-17T11:13:00.00Z
Registrar: ENOM, INC.
Registrar IANA ID: 48
Registrar Abuse Contact Email: abuse@enom.com
Registrar Abuse Contact Phone: +1.4252982646
Domain Status: clientTransferProhibited
```

Ilustración 39: Captura de la información del *Registrador* del *Dominio* "*jyyoi.com*".

- El *Registrador* es Tailandés, su nombre es Somkiat Apisuttimaitree, con domicilio en Bangkok en la calle 1 Fortune Town 22nd., Dindaeng y teléfono (662)6421100. También aparece su email asociado, "*somkiat@netdesign.ac.th*"

```
Registrant Name: SOMKIAT APISUTTIMAITREE
Registrant Organization: NETDESIGNHOST.COM
Registrant Street: 1 FORTUNE TOWN 22ND.,DINDAENG
Registrant City: BANGKOK
Registrant State/Province:
Registrant Postal Code: 10320
Registrant Country: TH
Registrant Phone: +66.26421100
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: SOMKIAT@NETDESIGN.AC.TH
```

Ilustración 40: Captura de la información del *Registrante* del *Dominio* "*jyyoi.com*".

Además si se echa un vistazo aparece un email de contacto asociado al *Dominio, jyyoi@yahoo.com* en el apartado técnico.

Respecto al *ISP*, la información obtenida indica que el propietario es *Cat Telecom*, con correo de soporte "*support@idc.cattelecom.com"* y de abuso "*abuse@idc.cattelecom.com*".

Recabada toda la información es el momento de proceder al cierre trabajando con los contactos obtenidos.

En primer lugar siempre hay que contactar con el contacto más prioritario que sea el que más responsabilidad sobre el *Dominio* pueda tener, es decir el *ISP*.

En este caso se mandarían correos de abuso a los contactos del mismo arriba indicados y se esperaría respuesta.

En segundo lugar hay que informar al *Registrador* o *Hosting* del caso enviándole un correo a la dirección de abuso obtenida, siempre poniendo en copia al *CERT* regional, en este caso el tailandés.

Además y como en el caso de *Google*, al disponerse de información del *Registrador*, convendría avisarle mediante un correo a su dirección personal ("*somkiat@netdesign.ac.th*") de que su blog ha sido *hackeado* y se ha alojado un *Redirector* a un *Phishing* en él. Hay que tener en cuenta que no tiene por qué ser un contacto especializado en materia de seguridad, por lo que es indispensable, siempre que se contacte con particulares, detallar al máximo y de la manera más fácil el grueso del problema. De nuevo se le solicitará que contacte con su *Hosting* para que solventen el problema a la mayor brevedad posible.

En este punto solo habría que esperar una respuesta positiva por parte de cualquiera de los tres contactos, a ser posible del *ISP*. En caso de demorarse esta, se pueden seguir realizando acciones en paralelo, por ejemplo, entrar en la web del *Registrador* "*enom.com*" y comprobar si tienen otras vías de comunicación disponibles.

En este caso disponen de un departamento de abuso online que permite reportar el caso previa cumplimentación de un formulario. Tras esto, solo quedaría esperar, de nuevo, una respuesta al mismo.

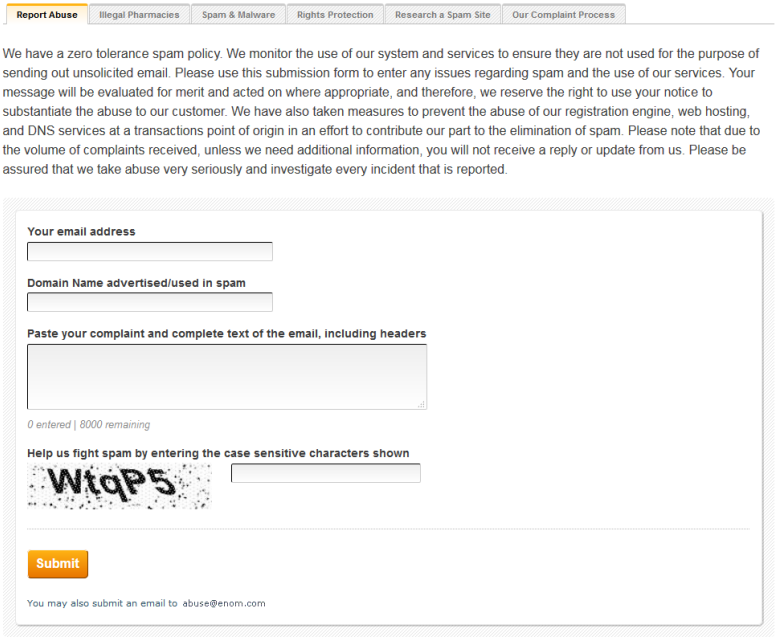


Ilustración 41: Captura del formulario de abuso solicitado por el *Hosting "enom.com"*.

Obtenida respuesta, como en el caso anterior, simplemente habría que comprobar la veracidad del mismo y, en caso de estar dado de baja el *Redirector*, se cerrarían tanto el caso principal (*Redirector*), como el subcaso del mismo (*Phishing*).

11.3 Supuesto *Redirector* camuflado hacia *Phishing BBVA.*

Este caso es fraude similar al anterior, un *Redirector* que finaliza en un *Phishing*. Sin embargo, hay una diferencia entre ambos que se descubrirá más adelante.

Para empezar se ha recibido un correo con apariencia corporativa perteneciente a la entidad bancaria *BBVA*, concretamente a su sede en México *Bancomer*.

En el cuerpo del mensaje se puede leer un requerimiento de alta con la excusa de la activación de una supuesta actualización de seguridad en una supuesta plataforma de seguridad del banco.

BBVA Bancomer

REMITENTE: Se requiere iniciar el proceso

Plataforma Julio 2013

Permiso SEGOB: 20456784PS03
Vigencia del Permiso: Del 15 de Julio de 2013 al 14 de Agosto de 2013.

Estamos realizando una actualización a la plataforma de seguridad móvil Y requerimos actualice de inmediato o se registre ya que esta plataforma estará activa por seguridad en 24 horas totalmente gratis. Esto es para reforzar sus sistemas de pagos, servicios, transferencias y saldos.

Para terminar este proceso de actualización de sus servicios ve al siguiente enlace AQUÍ.

LE TOMARA SOLO UN MINUTO PARA CONCLUIR CON LA NUEVA PLATAFORMA

http://www.bancomer.com.mx/minisitios/Sitio_bancomerMovil_3/Registro/

Alertas Bancomer

- Plataforma Seguridad Móvil
- Plataforma Seguridad Banca en Línea
- y mucho más...

Ante cualquier consulta puede contactarnos a nuestro servicio de atención a Clientes, 01800 2262663, disponible las 24 Horas del Día o a través de nuestra pagina Web www.bancomer.com

Saluda Atentamente a usted
Ejecutivo Financiero: Sr. Adolfo Gutiérrez Leyva

Ilustración 42: Cuerpo del mensaje suplantando a *BBVA Bancomer*.

Evidentemente todo suena bastante extraño, pues no se informa de que plataforma es, no se tiene precedentes de la misma y arroja muy poca información que permita al cliente sentirse lo suficientemente informado como para proceder al alta de manera confiada y segura.

Si se presta atención aparece una *Uri* que a priori, parece totalmente legítima:

http://www.bancomer.com.mx/minisitios/Sitio_bancomerMovil_3/Registro/

Como se puede comprobar el *Dominio* es *www.bancomer.com.mx*, para comprobar que dicho *Dominio* pertenece realmente a la entidad original, basta con entrar manualmente a través del navegador a la página de dicha entidad.

Ilustración 43: *Dominio* legítimo propiedad de *BBVA Bancomer*.

Hecha la comparación se puede ver que, efectivamente, ambas coinciden por lo que no debería haber peligro aparente.

Sin embargo hay algo sospechoso en esta *Uri*, si se accede a la misma la *Uri* destino, como en el caso anterior cambia completamente. Aunque en este caso sigue conservando la tipología de dirección web, el *Dominio* desaparece y se obtiene la *Uri* siguiente:

http://201.116.211.85

Lo que se obtiene es una *IP* asociada a un *Dominio* oculto. Evidentemente, no hace falta realizar ningún análisis para tacharlo de fraude, pues existiendo un *Dominio* conocido para la entidad bancaria, no tiene sentido que utilizasen direcciones no identificables por el cliente.

Pero, ¿Cómo es posible que una web legítima redirija a un *Phishing*?, la respuesta es sencilla, simplemente no es una web legítima.

Existen multitud de métodos para enmascarar *Uri's* de manera que parezcan lo que no son. Los más conocidos son los famosos *Acortadores de Uri's*, herramientas que permiten formatear la dirección a otra completamente diferente. Las herramientas públicas que prestan este tipo de servicios no suelen ser personalizables, por lo que la *Uri* acortada tiene un formato prefijado y es fácil que los filtros de *AntiVirus* o *Spam* lo detecten. Sin embargo, existen herramientas que los propios *Piratas Informáticos* crean, que les permite personalizar la web acortada de tal manera que le puedan dar el aspecto que deseen.

También existen otros métodos, como la inclusión de scripts que se encarguen de la redirección al *Phishing* prefijado por el delincuente.

Estos son solo dos ejemplos de la multitud de herramientas y posibilidades que hay para camuflar el origen de una *Uri* y, en definitiva, de su identidad.

Aclarado esto y detectada la trampa, el proceso sería exactamente igual al realizado hasta ahora con la diferencia de que no se abriría un caso para el *Redirector* pues, en realidad, no existe tal, de hecho es la misma *Uri* solo que simplemente sufre una modificación léxica en tiempo de conexión. Por ello simplemente se abriría un caso de *Phishing* con la *Uri*:

http://201.116.211.85

Con esto simplemente se llevaría a cabo el proceso ya conocido con normalidad hasta obtener el cierre del mismo con una diferencia, en este caso no existe *Dominio* conocido, solo se dispone de una *IP*. Aunque esto limita la cantidad de información que se puede obtener, el análisis de *WhoIs* se puede llevar a cabo con normalidad.

En este caso el *WhoIs* (ver ejemplo de captura completa en la sección *WhoIs* del Anexo) no muestra información de *Registrante* o *Registrador*, sin embargo nos muestra lo siguiente:

- Aparece información sobre los dominios mexicanos que parecen estar detrás de la *IP*, concretamente *"reduno.com.mx"* y *"uninet.net.mx"* así como sus correos asociados, uno de ellos, correspondiente a un departamento de abuso, "*abuse@uninet.net.mx*". Además también aparecen un par de números telefónicos que, debido a la poca información recabada, probablemente sea necesario contactar.

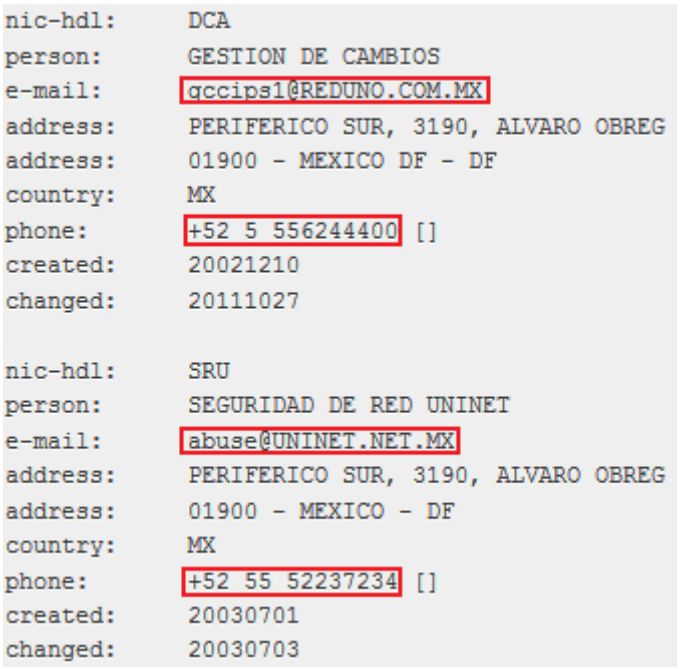


Ilustración 44: Captura de la información obtenida en el *WhoIs* de la *IP* 201.116.211.85.

Aunque aparece algo más de información del *Dominio*, ciertamente solo es útil lo señalado arriba.

Si se intenta acceder a los dominios de dicho correo se puede comprobar que, actualmente, no muestran información alguna, por lo que es posible que los correos estén obsoletos y los dominios que actúan como *ISP* no estén activos..

El primer paso es enviar un correo, como hasta ahora, al contacto de abuso "*abuse@uninet.net.mx"* poniendo en copia en este caso al *CERT* mexicano.

De nuevo habría que esperar una respuesta aunque, como bien se ha dicho, ante la posibilidad de que los correos no estén operativos, es conveniente contactar con los números telefónicos en paralelo, pues hay que recordar que urge cerrar el caso.

11.4 Subdominio *Redirector* a *Phishing* de Barclaycard

Este caso es una combinación de los dos anteriores. Para empezar se dispone de una *Uri* que ha sido reportada como fraudulenta:

http://barclaycardus.dream.epsilon.com/1d8474e01layfousibyiu57yaaaaaark7yaetc5hgluyaaaaa/C?V=emlwX2NvZGUBAVNJTkdMRV9UUkFOU0FDVElPTl9EVAEwOC8yMi8yMDE0AVNJTkdMRV9UUkFOU0FDVElPTl9BTU9VTlQBNTIuNTABUEFSVE5FUk5BTUVfU0VDT05EX1RFTVABUEFSVE5FUk5BTUVfU0VDT05EX1dFTV9IVE1MAWdfaW5kZXgBAUZOQU1FAU1JS0UBbF9pbmRleAEBTEFTVDQBNDI1MQFwcm9maWxlX2lkATExNjM5MDI5ODUBUEFSVE5FUk5BTUVfRklSU1RfVEVNUAFQQVJUTkVSTkFNRV9GSVJTVF9XRU1fSFRNTAFfUExJU1RfSURfATY4OTc1NDM4AV9XQVZFX0lEXwE4Mjk3NDQ3MzMBbWFpbGluZ19pZAExMTQ3MjM1MjMBQlJBTkQBSEFDAVBBUlRZX0lEATI0NzgzOTg5AVRQQ19DT0RFAU1YAUNNSUQBZGVmYXVsdC5wbmcBZW1haWxfYWRkcgFtaWtlQG1hbHRlcmNvcnAuY29tAV9TQ0hEX1RNXwEyMDE0MDgyMzIwNTIxMwFMTkFNRQFNQUxURVIBcHJvZmlsZV9rZXkBODU5NjcyNDI5&kZr//WbZRhV7xwRdVNBhMg

En este caso se ha decidido poner al completo la dirección para demostrar que a simple vista es evidente que hay algo raro en ella.

En primer lugar la longitud es extremadamente larga para ser una web corporativa, lo que ya da una pista del posible origen fraudulento de la misma.

En segundo lugar, si se observan las carpetas, son caracteres aleatorios, sin ningún orden lógico, algo que no tiene sentido cuando deberían tener nombres que identificasen la procedencia de la página mostrada en el servidor. Otro indicio de fraude.

Respecto al *Dominio* podría parecer legítimo, pero esto va a ser analizado más adelante, cuando se muestre el *Phishing*.

Analizado el aspecto de la *Uri* solo queda comprobar su actividad. Si se accede a la misma se puede ver cómo lleva, aparentemente, a una página de *Barclaycard* que solicita unas credenciales personales. Sin embargo, de nuevo, la *Uri* ha cambiado, ahora es más corta aunque dispone del mismo dominio:

https:// barclaycardus.dream.epsilon.com/?domainCPC=HCL&referrerid=ALRTDOLLMT

Mirando desde el punto de vista de un usuario normal, esta web, a priori, podría parecer 100% legítima. Hay que tener en cuenta que el usuario no tiene por qué conocer los dominios asociados a *Barclaycard* (aunque debería) y, el mostrado "*barclaycardus*", parece bastante lógico. Además, estéticamente, la apariencia es exactamente igual a una web legítima, por lo que en este aspecto no se podría detectar fraude. Se podría decir que contiene todos los ingredientes para conformar un fraude totalmente efectivo de cara al usuario común.

Si se analiza desde un prisma más profesional, el *Dominio* tiene varios elementos que le delatan.

El primero es el acrónimo "*us*" al final del mismo. Con este acrónimo se está intentando indicar que la página pertenece a un *Dominio* estadounidense (*us*=United States). Sin embargo, este

no es el método que se llevaría a cabo para indicar el emplazamiento de un *Dominio,* para ello existe el conocido *ccLTD*. El *Dominio de nivel superior geográfico* se compone de dos caracteres precedidos por un punto, por ejemplo en el caso anterior, para indicar que era un *Dominio* mexicano el *ccLTD* era "*.mx*".

En este caso al no aparecer dicha composición en la *Uri* podría decirse que el *Dominio* es sospechoso y efectivamente, si se accede al *Dominio* legítimo se puede comprobar que es "*barclaycard*" seguido del correspondiente *ccLTD*, por lo que podría tacharse de fraudulento.

En segundo lugar el dominio contiene varios puntos, esto requiere un análisis cuidadoso. Para alguien sin unos conocimientos previos no será fácil detectar el *Dominio,* pues aparecen varios puntos utilizados como separadores que pueden confundir. En realidad, este *Dominio* es un *Subdominio*. Para poder identificar el *Dominio* principal, a partir del cual se ha formado el *Subdominio,* simplemente hay que coger la palabra que se sitúe, partiendo desde el final, entre el *ccLTD* o *gTLD* y el primer punto encontrado. En este caso sería "*epsilon.com*" la cual, es evidente, no tiene nada que ver con *Barclaycard* y se trata de un fraude.

Acabado el proceso de Detección, es momento de pasar al Análisis. Como siempre, se va a realizar un análisis con *WhoIs* (ver ejemplo de captura completa en la sección *WhoIs* del Anexo) para comprobar que información hay detrás del *Dominio*.

La información mostrada es la siguiente:

- El registro o *Hosting* de la misma corre a cargo de NETWORK SOLUTIONS, LLC y proporcionan correo de abuso con dirección, "*abuse@web.com*" y un teléfono de contacto para dicho departamento, (800)3337680.

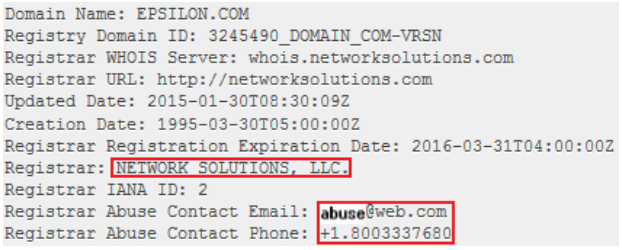


Ilustración 45: Captura de la información del *Hosting* del *Dominio "epsilon.com"*.

- El *Registrante* en este caso no es un particular sino una empresa llamada Epsilon Data Management localizada en Texas, EE.UU, con email "*jgaythorpe@epsilon.com*" y teléfono (469)2620836.

Ilustración 46: Captura de información del *Registrante* del *Dominio "epsilon.com"*.

- Además aparece información del administrador, en este caso llamado Errol Singley procedente de la ciudad de Irving, Texas, con domicilio en la calle 6021 Connection Drive, con correo "*domainregmaint@epsilon.com*" y teléfono (469)2620836.

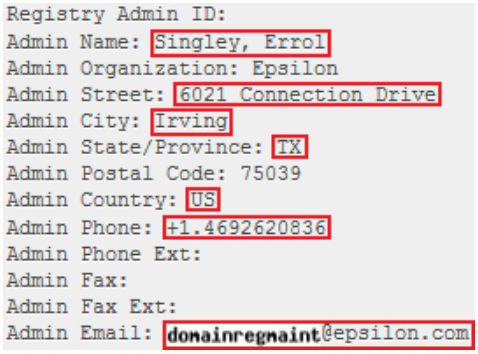


Ilustración 47: Captura de información del administrador del *Dominio "epsilon.com"*.

Teniendo en cuenta que para abrir un *Subdominio* es requisito indispensable ser propietario del *Dominio*, es posible que la empresa detrás de este último haya sido *hackeada* y hayan abierto varios S*ubdominios* fraudulentos a partir de ella.

En cuanto al *ISP,* el *WhoIs* muestra que la propia "*epsilon.com*" actúa como y muestra algún que otro correo más, aunque no parecen demasiado relevantes. No así, podrían ser de utilidad en caso de que los obtenidos hasta ahora no diesen frutos a corto plazo. Además aparecen algunos teléfonos asociados a dichas cuentas que también podrían ser de ayuda en dicho caso.

```
OrgAbuseHandle: RFU24-ARIN
OrgAbuseName:   Fu, Rich
OrgAbusePhone:  +1-212-457-7233
OrgAbuseEmail:  rich.fu@epsilon.com
OrgAbuseRef:    http://whois.arin.net/rest/poc/RFU24-ARIN

OrgTechHandle: RFU24-ARIN
OrgTechName:   Fu, Rich
OrgTechPhone:  +1-212-457-7233
OrgTechEmail:  rich.fu@epsilon.com
OrgTechRef:    http://whois.arin.net/rest/poc/RFU24-ARIN

RTechHandle: IIP5-ARIN
RTechName:   IP admin, IP admin
RTechPhone:  +1-212-457-7000
RTechEmail:  DeliverabilityTeam@epsilon.com
RTechRef:    http://whois.arin.net/rest/poc/IIP5-ARIN

RAbuseHandle: EDM4-ARIN
RAbuseName:   Email Deliverability Management
RAbusePhone:  +1-212-457-7333
RAbuseEmail:  deliverabilityteam@epsilon.com
RAbuseRef:    http://whois.arin.net/rest/poc/EDM4-ARIN
```

Ilustración 48: Captura de información mostrada por el *WhoIs* del *ISP*.

Con estos datos, para proceder al cierre habría que seguir el procedimiento habitual.

Primero se contactará mediante un correo de abuso con NETWORK SOLUTIONS y, además, como se tiene el correo del administrador del dominio, se le mandaría otro a él directamente. En caso de no obtener respuesta se podría intentar de nuevo con los datos del *Registrante*.

Por otro lado, si se accede al dominio, dispone de una sección de contacto donde se solicita la cumplimentación de un formulario. Aunque no es un formulario destinado a la gestión de abusos o reportes de fraude, quizás pueda ser de ayuda, al menos, como punto de contacto para avisar del caso y que se proporcionen nuevos contactos por parte del dominio.

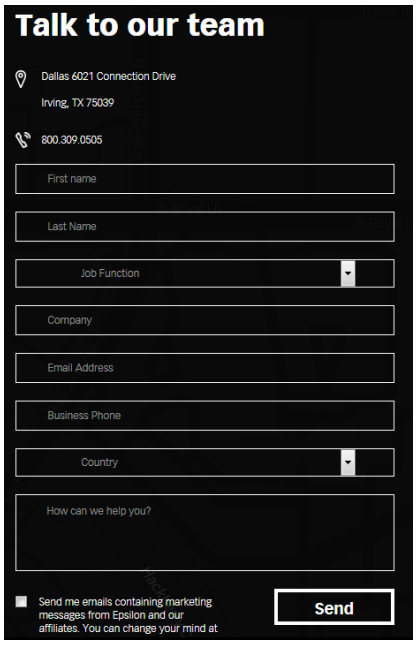


Ilustración 49: Captura del formulario disponible en el dominio "*epsilon.com*".

El *Hosting* también dispone de varios métodos de contacto, no obstante, si se navega por la web, se puede comprobar que es fácil perderse y los métodos de contacto no son fáciles de localizar. Además, no existe ningún método específico para reportar fraudes y simplemente disponen de un formulario de contacto genérico, por lo que se estaría en la misma situación que con el formulario del dominio.

11.5 Fraude procedente de un *Bullet Proof ISP*

Aunque en el Anexo se va a profundizar en detalle sobre el concepto de *ISP a prueba de balas*, aquí se va a realizar una pequeña introducción, para saber qué hacer en caso de encontrarse con un caso como este.

En primer lugar hay que indicar que el caso que se va a mostrar a continuación es muy improbable que se dé, no obstante como existen, se van a dar algunas pautas que seguir para intentar gestionarlo dentro de las capacidades del analista.

Un *ISP a prueba de balas*, resumiendo, es un *ISP* propiedad de alguna organización delincuente cuya existencia se justifica únicamente en la creación de *Fraude Online*.

Como se puede imaginar, cerrar un caso donde la propia *ISP* está involucrada en el fraude, es extremadamente complicado. Hay que recordar que el *ISP* es el propietario de la *IP* y el *Dominio*, es decir, los que administran los mismos, por lo tanto son el mejor contacto con el que trabajar a la hora de gestionar casos.

En este caso en particular al ser un *ISP* fraudulento, de poco sirve contactar con el *Registrante*, el *Registrador* o el *ISP*.

En casos tan particulares como este habría que pedir ayuda a organismos institucionales apropiados y sería una de las pocas circunstancias donde contactar pidiendo ayuda directamente a los *CERT* gubernamentales estaría justificado.

Aun así es poco probable conseguir una gestión eficiente del mismo y mucho menos aún conseguir un cierre que resultase efectivo. Pues es relativamente sencillo dar de baja un dominio fraudulento, pero no así evitar que este se reactive a las pocas horas.

Además, el proceso contra el *ISP* es de carácter legal en este caso, por lo que el analista estaría atado de pies y manos y tendría que dejar hacer a la justicia pertinente. Como mucho, podría dar soporte o reportar información en caso de que el *CERT* la solicitase para ayudar en el cierre.

Los casos de *ISP a prueba de balas* son casos que se detectan como tal con el paso del tiempo.

Si se cierra una *Uri* reportada en un corto periodo de tiempo, lo que a priori podría parecer una gestión óptima quizás, simplemente, se trata de una estratagema por parte de los *ISP*. A estos les conviene cerrar pronto las *Uri* denunciadas con el fin de quitarse de encima a las empresas de seguridad lo antes posible. El problema viene cuando a los pocos días, o incluso horas, el caso se reactiva y así sucede durante unos cuantos cierres. Si, además, el *ISP* se

muestra excesivamente colaborador, o todo lo contrario, pero nunca dentro de lo habitual, se puede empezar a sospechar que pertenezca a uno de estos tipos.

Otro rasgo característico es la proliferación de *Uri's* fraudulentas en un corto periodo de tiempo, todas contenidas en la misma *IP* (y por tanto mismo *ISP*). Se pueden dar casos de hasta 20 *Uri's* enlazadas en el mismo caso gestionadas a la vez. Dada esta situación, la alta cantidad de *Uri's* implicadas impiden que el caso se pueda cerrar, al menos, a corto plazo, por lo que conviene notificar las circunstancias del caso al cliente y continuar con otros que el analista pueda gestionar.

Hasta aquí, se han visto 5 casos. Resumiendo, con estos casos se ha intentado mostrar el protocolo de actuación escalando la dificultad progresivamente desde el menos complejo hasta el más difícil e improbable:

- ***Phishing simple:*** El caso de Google implicaba un delito por fraude de los más habituales. Sin complicaciones reseñables, podría ser uno de los miles que circulan día a día por la red.
- ***Redirector simple a Phishing:*** En el caso de *Barclays* se tenía un *Redirector* simple, es decir, no camuflado, que redirigía hacia un *Phishing* convencional. Aunque la *Uri de datos* implicada podría confundir su gestión es, de hecho, más simple que el de una *Uri* convencional, pues en este caso gestionando el cierre del *Redirector*, la *Uri de datos* queda inhabilitada.
- ***Falso Redirector a Phishing:*** En el caso de *BBVA*, se gestionaba lo que, a priori, parecía un caso similar al anterior, un *Redirector* que llevaba a un *Phishing*. Sin embargo al analizar el supuesto *redirector* se podía observar que no era tal. Simplemente era la misma *Uri* del *Phishing* procesada por un *acortador de Uri's* personalizado. En este caso simplemente se analizaba la *Uri* original como un *Phishing* más. En realidad, la complicación de este caso viene determinada por la formación del analista pues, sin conocimiento previo de este tipo de herramientas, es prácticamente imposible entender el caso correctamente y probablemente acabaría gestionándose, erróneamente, como el anterior.
- ***Redirector camuflado a Phishing:*** Este caso implicaba a *Barclaycard* y es bastante parecido al de *Barclays,* pero con un matiz importante. En este caso se tenía un *Redirector* y un *Phishing* simples alojados en un *subdominio*. La dificultad residía en la correcta interpretación de la estructura del dominio que, para alguien no informado, podría parecer legítimo.
- ***Bullet Proof ISP:*** El caso más complicado e improbable de todos, tanto, que no se pueden poner ejemplos reales debido a la dificultad de encontrar un caso activo de dicho tipo. En este caso se supone un *Phishing* cuya administración corre a cargo de las llamadas *ISP a prueba de balas*, las cuales pertenecen a organizaciones delincuentes. Su cierre es prácticamente imposible y este deberá correr a cargo de organismos gubernamentales y no de empresas de seguridad independientes.

Vistos estos cinco casos, lógicamente, existen muchas más complicaciones, pero aquí se han querido mostrar estas 5 debido a que abarcan todos los niveles de dificultad desde lo más simple a lo más complejo.

Como ya se ha comentado en alguna ocasión existen circunstancias que pueden sucederse cada mucho tiempo y de las que, de hecho, es posible que no haya antecedentes, pues la tecnología avanza y con él, el *Fraude Online*. Un ejemplo de esto son las conocidas en seguridad como *IP's* mutantes. Casos en los que, para una sola *Uri*, pueden intervenir hasta una docena de *IP* para dar soporte al dominio. La complejidad de estos casos es extrema y no es objetivo de este documento instruir en estos aspectos.

12. Conclusiones

Conocidos los perjuicios que está produciendo el *Phishing* hoy en día y tras ver cómo combatirlo, es momento de pararse a pensar qué futuro depara el *Fraude Online*.

No hay que olvidar que el *Ciberdelito* es una tipología de delito relativamente joven, como se ha comentado ya, los primeros casos de *Phishing* no se dieron hasta los años 90, si bien no se tomaron en serio hasta su expansión definitiva en 2004 aproximadamente, hace poco más de 10 años.

Esto quiere decir que, lejos de estar ante la erradicación del *Fraude Online* (de hecho no existe delito erradicable), probablemente se estén viviendo los años de mayores cambios y evoluciones del mismo. Esta evolución es difícil de predecir cuándo parará, en caso de que esto ocurra, pues es una evolución que va de la mano del progreso tecnológico, el cual, por razones obvias, jamás cesará.

La idea de las empresas de seguridad es trabajar combatiendo los delitos existentes actualmente, pero el principal hándicap es, precisamente, la evolución del delito. No se puede combatir lo que no se conoce, por lo que cada nueva versión o mejora que se crea para el delito online, implica un estudio desde cero por parte del sector de seguridad para poder frenarlo. Desafortunadamente, estas mejoras aparecen cada día, por lo que es extremadamente complicado seguirle el ritmo.

El hecho de ir continuamente un paso por detrás del delito, hace que, desgraciadamente, este jamás cese demostrando, como bien afirmaba Gene Spafford en la cita incluida en la Introducción, que no existe la seguridad completa.

Como todo proceso cuyo fin sea preservar la seguridad y la legalidad de cualquier acción, las empresas de seguridad tienen que centrarse en mitigar los efectos del *Ciberdelito*, para ello es indispensable la anticipación del mismo. Teniendo en cuenta que la tecnología, en este caso en particular juega en contra, la única arma que tienen las empresas de seguridad para ser eficientes es la velocidad de reacción.

Como todo, la velocidad de reacción se puede entrenar y mejorar. Es complicado pero quizás, las empresas de seguridad tendrían que centrarse más en mejorar los procesos de monitorización globales. Estos sistemas son los primeros que toman contacto con el delito en cuanto lo detectan, por lo que, limitar estos sistemas a la simple detección del delito es demasiado simple y desaprovecha el potencial que se podría explotar de dichos sistemas.

Podrían implementarse bloqueos temporales que mejorasen fruto del aprendizaje como si de una *IA*[1] se tratase, o perfeccionar el análisis de tráfico global de la red.

Las mejoras son infinitas pero, quizás, la más influyente de todas sea la formación académica.

[1] *Inteligencia Artificial.*

Los mayores ataques informáticos han sido ejecutados por auténticos genios en el mundo de la seguridad informática y esto no es por casualidad.

Mentes privilegiadas que han obtenido unos conocimientos fuera de lo común con la única ayuda de su afán por aprender y de manera, en muchos casos, completamente autodidacta. Si el mundo del delito goza de tan extraordinarias mentes, el lado opuesto, el de los que luchan a favor de la ley, no debería ser menos. Pero para ello, hace falta educación, formación académica altamente especializada, prácticamente de élite, a la que debería poder acceder cualquier persona involucrada en la seguridad informática.

Lógicamente los impedimentos que hacen imposible masificar dicha formación, abarcan un amplio campo de obstáculos, tanto socioeconómicos como políticos, que no entran en la intención de este documento discutir.

Volviendo al factor evolutivo, es necesario tener en cuenta cual es la principal amenaza. De todos los casos registrados en 2014 casi el 60%[1] pertenecían a *Phishing*, esto quiere decir que hay que centrar los esfuerzos en combatir esta faceta del fraude por encima de cualquier otra.

Si se combina el dato anterior con el que indica que más del 46%[1] de los casos proviene de EE.UU, la conclusión es clara, EE.UU deberá reforzar en la medida de lo posible todos sus sistemas de seguridad ya que de ellos depende que resto del mundo coja el relevo para minimizar el número de casos, el cual es extremadamente alto a día de hoy.

El *Phishing* crece, esto es un hecho incuestionable pero, ¿Cómo? Ya se ha hablado de que se están viviendo años de cambios y evoluciones, pero no se ha indicado en que aspectos.

Cada día que pasa los delincuentes encuentran una nueva brecha que explotar en el mundo del *Fraude Online* y, teniendo en cuenta que es una tecnología que se nutre de la llamada *Ingeniería Social*, la proliferación de las denominadas *Redes Sociales* está proporcionando un trampolín único en la historia a los delincuentes para multiplicar exponencialmente el número de víctimas al que llegar.

Facebook, Twitter, Instagram… no hay red social de ámbito internacional que se libre del *Phishing*, de hecho, algunas (como *Facebook*[2]) ya disponen de su propio departamento especializado para combatirlo y es que no hay que ser un experto para poder utilizar dichas redes en nuestro beneficio mediante el uso de *Phishing*, Internet está repleto de tutoriales de cómo llevar a cabo casos de fraude que no le llevarían a un usuario medio ni 5 minutos de su tiempo ponerlos a funcionar. *Uri's Redirectores* en el estado de las cuentas que aprovechan un *Open-Redirect*, aplicaciones de *Ingeniería Social* creadas única y exclusivamente para proporcionar sencillos métodos de creación de *Phishing*… son algunas de las maneras que existen hoy en día para engañar a la gente.

Esto lleva a la conclusión de que estas plataformas, las *Redes Sociales*, tienen una gran labor por delante en cuanto a seguridad se refiere, pues son protagonistas directos del *Fraude Online* y su colaboración es vital.

[1] Fuente: S21sec.

[2] https://www.facebook.com/help/217910864998172/

De nuevo, es necesario mencionar la formación dada al usuario. Afortunadamente, las entidades objetivo de *Phishing* son claramente identificables. Toda entidad bancaria, o empresa que efectúe transacciones monetarias con algún tipo de pasarela de pago, es una víctima potencial del *Fraude Online*. Entonces, ¿Por qué no adelantarse a los acontecimientos? Si se conoce el peligro que se corre es lógico prepararse contra él.

Pocas son las empresas que advierten a sus clientes del peligro que corren de manera directa. Es verdad que cada vez hay más concienciación y que existe información en algunas web corporativas sobre el riesgo del *Phishing* pero esto no es suficiente.

Es inaceptable que empresas líderes mundiales en el procesamiento de pagos, no dispongan de un departamento técnico o una sección en su página, enfocada única y exclusivamente en dar soporte en este aspecto al cliente.

Si es cierto que disponen de departamentos de abuso donde reportar los casos. Pero estos departamentos existen en su gran mayoría para establecer colaboraciones con empresas de seguridad (como se ha visto en los Casos Reales) y no para el cliente en sí. De hecho, la gran mayoría de clientes ni siquiera saben que existen dichos departamentos o a qué se dedican.

Hace falta concienciación pública y abierta. Los clientes necesitan ser informados y sentirse respaldados del peligro real que corren antes de que sea tarde. Esa situación actualmente no se da, es algo que hay que cambiar drásticamente y que depende única y exclusivamente de las empresas.

Para finalizar, el futuro próximo se ve como unos años donde, si la seguridad y la concienciación no avanzan en consonancia a la gravedad del problema, es probable que lo vivido hasta ahora sea solo una muestra muy pequeña de lo que puede estar por llegar.

13.Anexo

13.1 Herramientas

A continuación se mostrarán capturas de pantalla que permitan complementar las explicaciones mostradas en la guía de análisis de casos.

- *Central Ops*

La siguiente captura corresponde a la información mostrada al seleccionar que la aplicación de *WhoIs* muestre toda la información posible. Cabe indicar que, como se ha indicado en el apartado correspondiente, mucha de esta información no es necesaria o, al menos, de vital importancia para la gestión de los casos.

Address lookup

canonical name **bbva.com.**
aliases
addresses **89.107.176.126**

Domain Whois record

Queried **whois.internic.net** with "**dom bbva.com**"...

Dominio
Registrador
DNS

```
Domain Name: BBVA.COM
Registrar: MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
Whois Server: whois.melbourneit.com
Referral URL: http://www.melbourneit.com
Name Server: DNSBBVA1.BBVAMOVIL.COM
Name Server: DNSBBVA3.BBVAMOVIL.COM
Status: ok
Updated Date: 03-jul-2014
Creation Date: 14-aug-1997
Expiration Date: 29-jan-2015

>>> Last update of whois database: Wed, 17 Sep 2014 19:12:04 UTC <<<
```

Queried **whois.melbourneit.com** with "**bbva.com**"...

Dominio
Registrador

```
Domain Name: bbva.com
Registry Domain ID: 416845_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.melbourneit.com
Registrar URL: http://www.melbourneit.com.au
Updated Date: 2014-07-03T16:05:17Z
Creation Date: 1997-08-14T04:00:00Z
Registrar Registration Expiration Date: 2015-01-28T13:00:00Z
Registrar: Melbourne IT Ltd
Registrar IANA ID: 13
Registrar Abuse Contact Email: abuse@melbourneit.com.au
Registrar Abuse Contact Phone: +61.386242300
Domain Status: ok
Registry Registrant ID:
```

```
Registrant Name: Banco Bilbao Vizcaya Argentaria, S.A.
Registrant Organization:
Registrant Street: Paseo de la Castellana 81
Registrant City: Madrid
Registrant State/Province: Madrid
Registrant Postal Code: 28046
Registrant Country: ES
Registrant Phone: +349.15379984
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: gestion.dominios@bbva.com
Registry Admin ID:
Admin Name: Gestion de Dominios
Admin Organization:
Admin Street: Paseo de la Castellana 81
Admin City: Madrid
Admin State/Province: Madrid
Admin Postal Code: 28046
Admin Country: ES
Admin Phone: +349.15379984
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: gestion.dominios@bbva.com
Registry Tech ID:
Tech Name: Departamento Tecnico
Tech Organization:
Tech Street: Paseo de la Castellana 81
Tech City: Madrid
Tech State/Province: Madrid
Tech Postal Code: 28046
Tech Country: ES
Tech Phone: +349.15379984
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: gestion.dominios@bbva.com
Name Server: DNSBBVA1.BBVAMOVIL.COM
Name Server: DNSBBVA3.BBVAMOVIL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdrprs.internic.net
>>> Last update of WHOIS database: 2014-09-17T18:56:29Z
```

Registrante

Admin. Web

Info. Técnica

DNS

Network Whois record

IP

Queried **whois.ripe.net** with "-B **89.107.176.126**"...

```
% Information related to '89.107.176.0 - 89.107.176.255'

% Abuse contact for '89.107.176.0 - 89.107.176.255' is 'bbvalir-abuse.es@bbva.com'

inetnum:        89.107.176.0 - 89.107.176.255
netname:        BBVA
descr:          Banco Bilbao Vizcaya S.A.
country:        ES
admin-c:        CB5163-RIPE
tech-c:         CB5163-RIPE
status:         ASSIGNED PA
mnt-by:         MAINT-AS15810
changed:        ehernandez@grupobbva.com 20060512
source:         RIPE

role:           Comunicaciones BBVA
address:        Banco Bilbao Vizcaya Argentaria S.A.
address:        C/ Batanes, 3
address:        28760 Tres Cantos, Madrid
address:        SPAIN
```

Ilustración 50: Captura de Central Ops.

De lo mostrado hay que resaltar que solo es de vital importancia la información de *Registrador*, *Registrante* y *Contactos de la IP*. El resto de información simplemente debe usarse como soporte o apoyo en caso de que los contactos principales no sean de ayuda.

13.1.1 VirusTotal

La siguiente captura que se va a mostrar corresponde a la información devuelta por el análisis realizado al archivo adjunto en el caso del *Phishing* de *Google* (ver apartado Casos Reales).

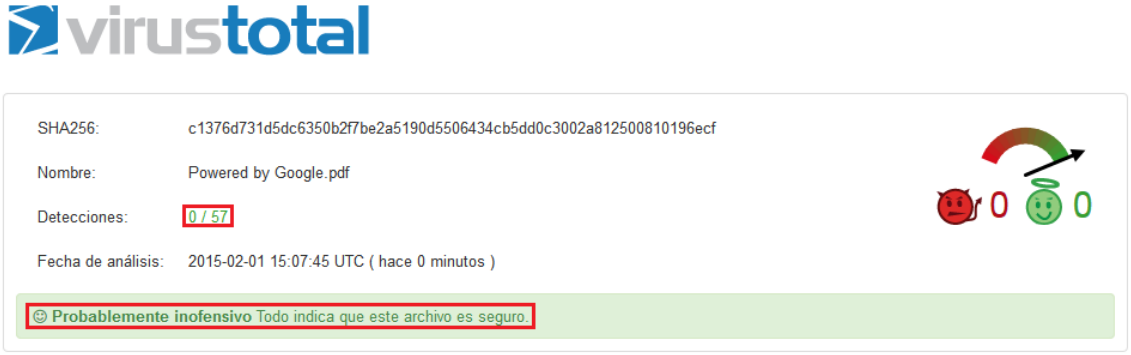
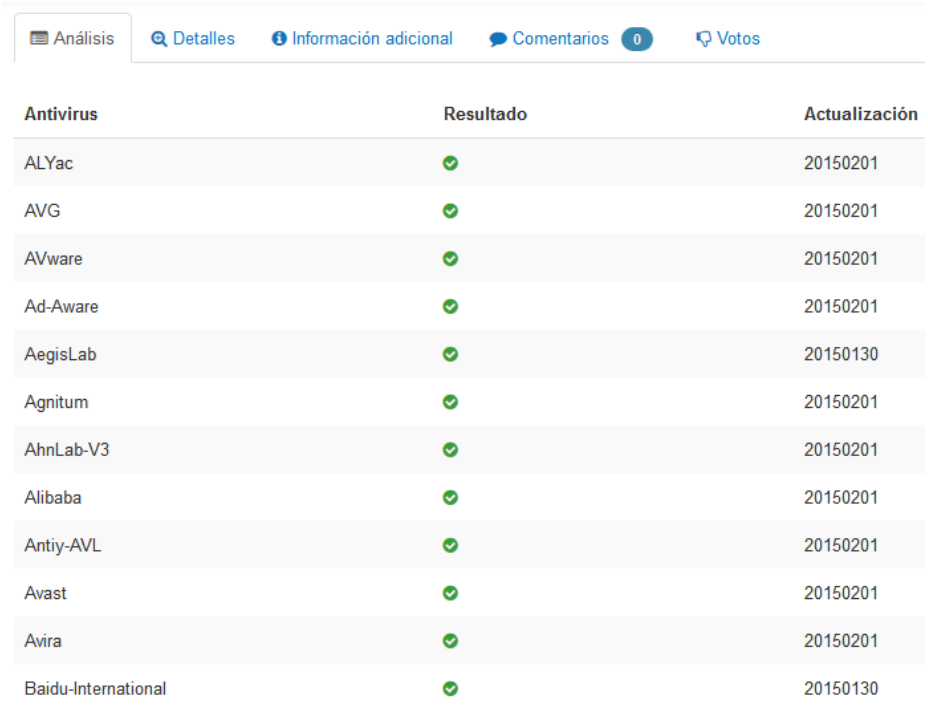


Ilustración 51: Captura de *VirusTotal* con resumen de actividad maliciosa.

Más concretamente se van a desglosar algunos de los antivirus que esta completa herramienta utiliza para realizar las comprobaciones. En total son 57 de los cuales se mostrarán una pequeña parte como muestra.

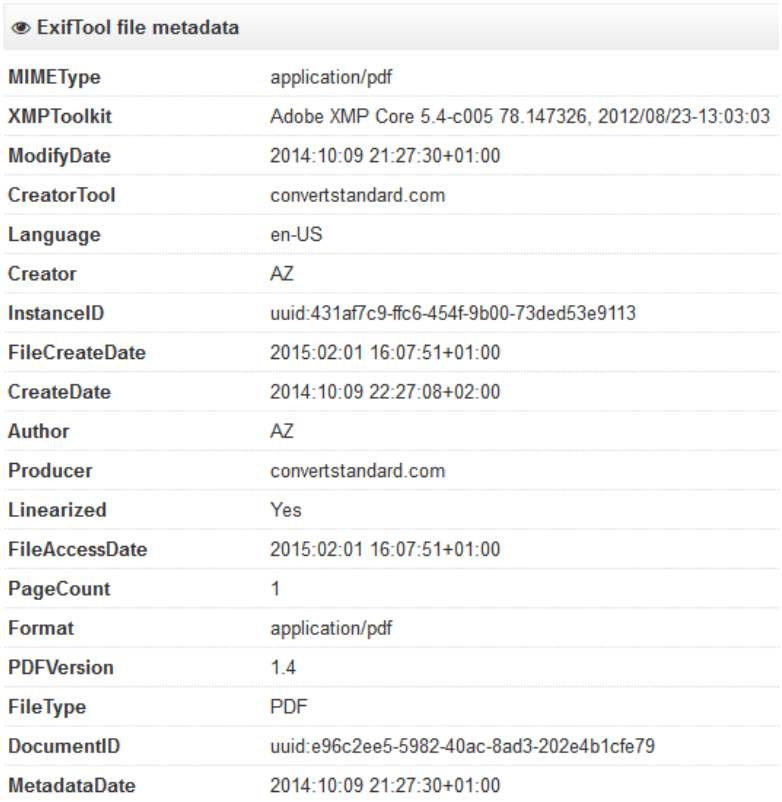


Análisis | Detalles | Información adicional | Comentarios 0 | Votos

Antivirus	Resultado	Actualización
ALYac	✓	20150201
AVG	✓	20150201
AVware	✓	20150201
Ad-Aware	✓	20150201
AegisLab	✓	20150130
Agnitum	✓	20150201
AhnLab-V3	✓	20150201
Alibaba	✓	20150201
Antiy-AVL	✓	20150201
Avast	✓	20150201
Avira	✓	20150201
Baidu-International	✓	20150130

Ilustración 52: Muestra de Antivirus analizados en *VirusTotal*.

Por último va a mostrarse la información detallada que la herramienta proporciona respecto al archivo.



ExifTool file metadata

MIMEType	application/pdf
XMPToolkit	Adobe XMP Core 5.4-c005 78.147326, 2012/08/23-13:03:03
ModifyDate	2014:10:09 21:27:30+01:00
CreatorTool	convertstandard.com
Language	en-US
Creator	AZ
InstanceID	uuid:431af7c9-ffc6-454f-9b00-73ded53e9113
FileCreateDate	2015:02:01 16:07:51+01:00
CreateDate	2014:10:09 22:27:08+02:00
Author	AZ
Producer	convertstandard.com
Linearized	Yes
FileAccessDate	2015:02:01 16:07:51+01:00
PageCount	1
Format	application/pdf
PDFVersion	1.4
FileType	PDF
DocumentID	uuid:e96c2ee5-5982-40ac-8ad3-202e4b1cfe79
MetadataDate	2014:10:09 21:27:30+01:00

Ilustración 53: Información detallada mostrada en *VirusTotal* del caso *Google*.

Existe algo más de información que la herramienta proporciona, sin embargo, con la indicada es más que suficiente para contrastar si un archivo es peligroso o no.

Para más información se recomienda visitar la página[1].

13.1.2 Rex Swain

Como se comentó en el apartado de Análisis, esta herramienta muestra mucha más información de la que este documento pretende utilizar en el cierre de un caso, no obstante, se va a mostrar una captura de un análisis realizado sobre un dominio real aleatorio, para mostrar la información útil respecto al escenario que se ha presentado.

Ilustración 54: Captura *RexSwain*.

[1] https://www.virustotal.com/

13.1.3 Wannabrowser

Esta herramienta tiene una finalidad similar a la anterior, sin embargo, muestra bastante menos información aunque no menos útil. De hecho esta herramienta ha sido la recomendada en el apartado de Análisis para comprobar la actividad de un caso.

La siguiente captura muestra información sobre el código de estado *HTTP* obtenido al realizar la conexión a un dominio aleatorio. Como se puede comprobar el resultado es de tipo ***200***, por lo que la web está activa.

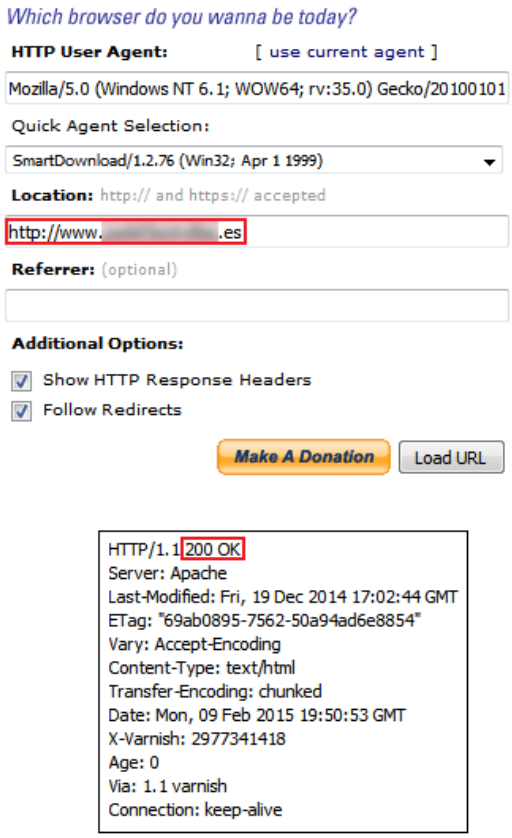


Ilustración 55: Captura Wannabrowser.

13.2 CERT

Como ya se ha comentado, el *CERT* (Computer Emergency Response Team) es el departamento encargado de responder emergencias informáticas. Estas emergencias pueden ser de cualquier tipo y se caracterizan por tener un carácter urgente y prioritario sobre cualquier otro tipo de incidente.

Un *CERT* puede ser de varios tipos, si bien este documento se ha centrado en los empresariales e internacionales, existen varios más como:

- De sector.
- Comercial.

- *Infraestructuras Críticas*.
- Sector Público o Administración.
- Militar.
- Para pequeñas y medianas empresas.

Los *CERT* encargados de las *Infraestructuras Críticas* son los más importantes y críticos, pues tienen la labor de proteger elementos estratégicos vitales para el transcurso normal de la sociedad. Centrales eléctricas, Centrales Nucleares, Hospitales, Transporte…etc. Son elementos con alto riesgo de ser objetivos de ataques y, en caso de producirse tal, las consecuencias podrían ser catastróficas para la sociedad.

La necesidad de crear este departamento especializado nació en 1988 como respuesta al ataque del *Gusano Morris*.

Además de la gestión de incidentes, también proporcionan soporte e información para mejorar la seguridad en los sistemas con el fin de evitar futuros ataques.

Las principales funciones se centran en proteger a la comunidad de incidentes graves de seguridad, establecer mecanismos de seguridad para la información susceptible de ser robada, conservar evidencias de los casos gestionados, fomentar el uso de la seguridad entre la comunidad…etc.

Además también realizan una labor activa mediante la búsqueda de vulnerabilidades para evitar futuros ataques, así como el desarrollo de software para la creación de herramientas informáticas con el fin de aplicarlas en los casos gestionados.

Los *CERT* gubernamentales se reparten entre las siguientes regiones:

- Norte América.
- Centro América.
- Sur América.
- Europa.

La inexistencia de *CERT* en determinados continentes, hace que proliferen los ataques desde los mismos. Por ejemplo, Nigeria está siendo una de las mayores productoras de *Phishing* debido a que no hay mecanismos de detección que impidan la proliferación de los mismos.

Por otro lado existe una asociación global de *CERT's* que se encarga de operar a nivel global.

En España, el *CERT* es propiedad del CCN[1] asociado al servicio de inteligencia denominado como CNI[2].

[1] Centro Criptológico Nacional.
[2] *Centro Nacional de Inteligencia.*

13.3 Proxy

Un *Proxy* es, fundamentalmente, un servidor. La función principal de este servidor es la de actuar como intermediario o punto de reunión entre los dos extremos de una conexión web.

La lógica de su existencia se basa en la multitud de servicios que un *Proxy* proporciona a los *Host* (tanto cliente como servidor).

Existen tres tipos de *Proxy*:

- ***Proxy web:*** Intercepta la navegación web. Es el tipo que afecta directamente a este documento y en el cuál se centrará la atención.
- ***Proxy FTP*[1]*:*** Un *Proxy* que actúa de intermediaria en la transferencia de archivos entre dos *Host*.
- ***Proxy ARP*[2]*:*** *Proxy* que actúa como enrutador en una red.

En función de si el *Proxy* tiene intención de actuar en el propio *Host* peticionario o es un elemento externo el que lo crea, un *Proxy* puede ser local, en el primer caso o externo, en el segundo. Además, en función de si admite o no conexiones de cualquier dispositivo que se conecte a él, podrá ser abierto o cerrado respectivamente. El *Proxy* abierto mejora mucho la fluidez y la velocidad de la conexión pero, como todo lo que gira en torno a un *Proxy*, también tiene un lado malo y es que este hecho puede ser explotado para utilizar un *Proxy* para su uso indebido, como el envío de correo masivo o *Spam*.

Ilustración 56: Esquema de navegación mediante un servidor *Proxy*.

En cuanto a las ventajas que un *Proxy* proporciona son varias, principalmente, un *Proxy* permite filtrar las conexiones de tal manera que se pueden controlar varios parámetros. Uno de los parámetros más destacables es el número de conexiones permitidas.

[1] *File Transfer Protocol* o *Protocolo de Transferencia de Archivos.*
[2] *Address Resolution Protocol* o *Protocolo de Resolución de Direcciones.*

Un *Proxy* puede establecer una cantidad máxima de conexiones con el objetivo de evitar, por ejemplo, un ataque *DoS*[1] o *DDoS*[2]. Evidentemente existen maneras de violar dicho filtro, pero como punto de partida es una buena manera de proteger un recurso.

Otra ventaja es el ahorro de recursos. Cuando varios servicios se conectan a un *Proxy* solo uno de ellos puede trabajar en el mismo instante de tiempo, por lo que la eficiencia es máxima.

Además, un *Proxy* permite *cachear* una petición de tal manera que puede guardarse la respuesta recibida a un recurso para posteriores peticiones que requieran de la misma, por lo que la eficiencia y la velocidad también aumentan en este sentido.

Otra de las medidas que puede tomar un *Proxy* es modificar la petición o la respuesta en una conexión a partir de algoritmos. Esta capacidad viene definida por el administrador del *Proxy*, que es quién estipula de qué manera se modifican las mismas.

Finalmente un *Proxy* puede denegar ciertas conexiones que considere prohibidas, por ejemplo, conexiones que el administrador considere que no pueden ser gestionadas por el servidor de respuesta.

Por otro lado, todas estas ventajas también se ven contrarrestadas por algunos inconvenientes. El principal y más importante, el anonimato.

Cuando las peticiones salen de un *Proxy* hacia un servidor, este último no conoce el origen primero de la petición, solo conoce como origen al propio *Proxy* por lo que el verdadero peticionario podría realizar cualquier tipo de conexión con intenciones maliciosas y la víctima nunca podría identificarlo en un primer momento.

Otra desventaja importante es la carga a la que se ven sometidos. Al actuar como intermediario de un recurso objetivo de infinidad de peticiones, es el *Proxy* el que tiene que gestionar todas y cada una de ellas con la consiguiente carga de trabajo.

Además, en general, un *Proxy* suele generar desconfianza a los usuarios debido a que no deja de ser un elemento entrometido en medio de una conexión que además, guarda copias de las respuestas (*cachea*), lo cual no está demasiado bien aceptado por los usuarios. Esta desconfianza ha propiciado los llamados *Proxies* transparentes, que de forma obligatoria y mediante un cortafuego redirigen todas las conexiones hacia un *Proxy* preconfigurado por la entidad propietaria.

Por otro lado este *cacheo* implica que se puedan estar almacenando copias antiguas de una respuesta y se le envíe al cliente unos datos obsoletos, aun existiendo unos más actualizados.

En definitiva un *Proxy* es un elemento muy útil siempre y cuando exista una configuración del mismo acorde a lo que se pretende conseguir y se utilicen con fines éticos y no maliciosos.

[1] *Denial of Service* o *Denegación de Servicio.*
[2] *Distributed Denial of Service* o *Denegación de Servicio Distribuida*.

13.4 Bullet Proof ISP

Teniendo en cuenta que los *ISP* son organizaciones con plena potestad sobre sus dominios web, era de esperar que dichas organizaciones tardeo temprano fuesen creadas por grupos delincuentes con el fin de crear estafas masivas.

Este es el caso de las llamadas *ISP a prueba de balas*, las cuales están gestionadas por organizaciones delincuentes con el único fin de generar innumerables webs de *Phishing* que les reporten obvios beneficios.

Aunque en un principio este término estaba reservado para aquellos *ISP* que proporcionaban cierto margen a sus usuarios en cuanto al tipo de contenido que se les permitía subir en sus dominios, en el ámbito de la seguridad esta nomenclatura ha ido degenerando hasta reservarse casi exclusivamente al caso anteriormente mencionado.

Combatir dichas organizaciones es extremadamente complejo, de hecho, son los organismos legales y judiciales los que se deben hacer cargo del problema.

Ilustración 57: Publicidad de un *Bullet Proof ISP.*

Su inquebrantable actividad suele verse propiciada por el aprovechamiento de vacíos legales en cuanto a la normativa y restricciones que imperan en Internet. Es por ello que cada cierto tiempo se suelen revisar las mismas con el fin de dar cada vez menos margen a dichas organizaciones y evitar que puedan llevar a cabo su actividad impunemente.

Aunque no son pocas las organizaciones detrás de dichas *ISP*, es verdad que se suelen dar muy pocos casos relacionados con las mismas. Esto se debe a que actualmente son organismos muy perseguidos y penados por lo que cada vez son más cautos en sus acciones.

Geográficamente suelen repartirse por Asia y Rusia y algunas de ellas han causado auténticos estragos en la red mundial, como RBN[1] o Voze Networks.

Una de las más conocidas, McColo, hasta su cierre en 2008 se estimaba que había generado un 66% del *Spam* mundial.

[1] *Russian Bussiness Network*.

13.5 CPD

Los *CPD* son espacios dedicados única y exclusivamente al almacenamiento y procesado de datos de vital importancia para una organización o institución. Debido a la criticidad de dichos datos, es necesaria una infraestructura capaz de salvaguardarlos de manera eficaz y de manera permanente.

Para llevar a cabo dicha protección se hacen uso de variados diseños en su estructura. El más importante de todos ellos es el diseño aislado. Un *CPD* siempre está (o debería estar) aislado completamente del resto de la actividad de la organización, tanto humana como computacional. Es decir, un *CPD* es un componente independiente y autosuficiente que no necesita de terceros para llevar a cabo su función.

Sin embargo, este hecho no excluye a un *CPD* de correr los riesgos de cualquier otro componente informático, como el riesgo de sufrir incendios, inundaciones, *hackeos*…etc. Es por ello que se hacen indispensables otros diseños complementarios.

Entre estos diseños se pueden contar falsos suelos y techos, cuadros eléctricos independientes, acondicionamiento individual de la sala en la que se encuentra, controles de temperatura y humedad con alarma incorporada o la creación de accesos flexibles y espaciosos.

En lo que a seguridad se refiere tampoco se escatiman mecanismos. Son habituales los detectores por huella, teclados numéricos, detectores de movimiento, cerraduras electromagnéticas, así como cámaras de seguridad y otros mecanismos más convencionales.

Evidentemente todo lo indicado supone un precio que hay que pagar por tal nivel de seguridad, aislamiento y el hecho no menos importante de proporcionar servicio continuo. Es por ello que los *CPD* son elementos caros de base, cuyo precio aumenta proporcionalmente al número de mecanismos y diseños de seguridad que se le incorporen.

En definitiva los *CPD* son componentes informáticos extremadamente punteros y elitistas, los más completos debido a su elevado precio los hace asequibles solamente a organizaciones y empresas de gran envergadura, que necesitan una seguridad prácticamente infranqueable para el principal objetivo de ataques informáticos en una empresa, los datos que permiten que la organización funcione en el día a día.

Ilustración 58: Parte del *CPD* de Google.

14.Bibliografía

20 Minutos. (15 de Febrero de 2015). Recuperado el 16 de Febrero de 2015, de http://www.20minutos.es/noticia/2377651/0/ciberataque/roban-millones/bancos/

Abuse.net. (s.f.). Recuperado el 7 de Octubre de 2014, de https://www.abuse.net/

Altonivel.com.mx. (s.f.). Recuperado el 21 de Enero de 2015, de http://www.altonivel.com.mx/los-10-hackers-mas-famosos-del-mundo.html

AnonyMouse. (s.f.). Recuperado el 17 de Septiembre de 2014, de http://anonymouse.org/

APWG. (s.f.). Recuperado el 7 de Julio de 2014, de http://apwg.org/

Atjeu hosting. (s.f.). Recuperado el 25 de Septiembre de 2014, de http://www.atjeu.com

BBVA. (s.f.). Recuperado el 26 de Agosto de 2014, de https://www.bbva.es/particulares/index.jsp

Bejerano, P. J. (25 de Noviembre de 2013). *ElDiario.es*. Recuperado el 30 de Enero de 2015, de http://www.eldiario.es/turing/inteligencia-artificial_0_200530122.html

Bernardo Quintero. (12 de Julio de 2006). *Hispasec*. Recuperado el 9 de Julio de 2014, de http://unaaldia.hispasec.com/2006/07/troyanos-bancarios-y-evolucion-del.html

BitDefender. (26 de Enero de 2015). Recuperado el 30 de Junio de 2014, de http://www.bitdefender.es/news/facebook-se-convierte-en-la-cuarta-empresa-m%C3%A1s-suplantada-en-los-ataques-de-phishing-1659.html

Bitvida. (13 de Septiembre de 2014). *BitVida*. Recuperado el 23 de Enero de 2015, de http://bitvida.com/2014/09/el-gran-hack-de-ee-uu-mas-de-160-millones-de-usuarios-afectados.html

Borghello, C. (s.f.). *Segu Info*. Recuperado el 3 de Noviembre de 2014, de http://www.segu-info.com.ar/malware/spam.htm

bugBlog. (s.f.). Recuperado el 31 de Enero de 2015, de http://blog.buguroo.com/tag/open-redirect/

Cáceres, J. (s.f.). *Apañados.es*. Recuperado el 28 de Agosto de 2014, de http://www.apañados.es/tenemos-que-apanar/internet-tutoriales-y-trucos/514-ejemplo-phishing-por-email.html

Castro, L. (s.f.). *About*. Recuperado el 26 de Agosto de 2014, de http://aprenderinternet.about.com/od/SeguridadPrivacidad/tp/Cinco-Consejos-Para-Evitar-Ser-Victima-De-Phishing.htm

CentralOps. (s.f.). Recuperado el 17 de Septiembre de 2014, de http://centralops.net/co/

Cliatec. (3 de Enero de 2012). Recuperado el 6 de Febrero de 2015, de http://www.cliatec.com/blog/proyecto-cpd-2

CNPIC. (s.f.). Recuperado el 11 de Febrero de 2015, de http://www.cnpic.es/Preguntas_Frecuentes/Que_es_una_Infraestructura_Critica/index.html

Dergarabedian, C. (6 de Mayo de 2015). *iProfesional*. Recuperado el 22 de Enero de 2015, de http://www.iprofesional.com/notas/115496-Cmo-fue-el-robo-de-datos-a-Sony-y-cul-es-el-impacto-en-usuarios-argentinos?page_y=0

Desarrolloweb.com. (s.f.). Recuperado el 12 de Febrero de 2015, de http://www.desarrolloweb.com/faq/que-es-proxy.html

Digita.com. (29 de Octubre de 2009). Recuperado el 2 de Febrero de 2015, de http://digitta.com/2009/10/uris-de-datos-data-uris.html

ElHacker.net. (s.f.). Recuperado el 11 de Febrero de 2015, de http://foro.elhacker.net/redes/instalar_servidor_proxy-t356009.0.html

Eset. (12 de Mayo de 2012). Recuperado el 1 de Julio de 2014, de http://www.eset.com.uy/threat-center/index.php?subaction=showfull&id=1336788823&archive=&start_from=&ucat=2&n=2

Gobierno de Aragon. (s.f.). *Gobierno de Aragon*. Recuperado el 9 de Septiembre de 2014, de http://www.aragon.es/DepartamentosOrganismosPublicos/Organismos/InstitutoAragonesEmpleo/AreasTematicas/Formacion/Certificados/ci.06_Preguntas_Frecuentes.detalleInaem

Gobierno del principado de Asturias. (s.f.). Recuperado el 9 de Septiembre de 2014, de https://www.asturias.es/portal/site/trabajastur/menuitem.0d568be1513873965b3ff5af331081ca/?vgnextoid=31691b21d382e210VgnVCM10000098030a0aRCRD&i18n.http.lang=es

González, S. (21 de Junio de 2103). *Mailify*. Recuperado el 7 de Julio de 2104, de http://blog.mailify.es/email-marketing-2/evolucion-de-los-envios-masivos-de-phishing-entre-2011-2013/

Hack Story. (22 de Julio de 2013). Recuperado el 31 de Enero de 2015, de http://hackstory.net/Ingenier%C3%ADa_social

Isit. (s.f.). Recuperado el 7 de Julio de 2014, de www.isit.es/en/Seguridad/Troyanos-bancarios-o-la-evolucion-del-phishing.html

Karmany.net. (30 de Abril de 2012). Recuperado el 1 de Septiembre de 2014, de http://www.karmany.net/seguridad/49-general/151-reportar-reconocer-y-denunciar-la-suplantacion-de-identidad-phishing

López, M. (24 de Julio de 2013). *Panda Security*. Recuperado el 26 de Agosto de 2014, de http://www.pandasecurity.com/spain/mediacenter/consejos/10-consejos-para-evitar-ataques-de-phishing/

Mcanerin International. (s.f.). Recuperado el 3 de Febrero de 2015, de http://www.mcanerin.com/en/articles/ccTLD.asp

NorfiPc.com. (s.f.). Recuperado el 26 de Diciembre de 2014, de http://norfipc.com/internet/servidores-dns.html

Pascual, A. (27 de Marzo de 2013). *Teknautas*. Recuperado el 12 de Enero de 2015, de http://www.elconfidencial.com/tecnologia/2013/03/27/el-mayor-ataque-hacker-de-la-historia-ralentiza-internet-a-nivel-global-4573

PhisTank. (s.f.). Recuperado el 1 de Agosto de 2014, de http://www.phishtank.com/

PhisTank. (s.f.). Recuperado el 2 de Febrero de 2015, de https://www.phishtank.com/target_search.php?target_id=5&valid=y&active=y&Search=Search

PhisTank. (s.f.). Recuperado el 3 de Febrero de 2015, de http://www.phishtank.com/phish_detail.php?phish_id=2628694&frame=details

Privacy Rights ClearingHouse. (s.f.). Recuperado el 8 de Febrero de 2015, de https://www.privacyrights.org/

Ranchal, J. (6 de Junio de 2014). *MuySeguridad.net*. Recuperado el 28 de Agosto de 2014, de http://muyseguridad.net/2014/06/06/ataque-de-phishing

Reuters. (8 de Noviembre de 2013). *ElEconomista.es*. Recuperado el 8 de Febrero de 2015, de http://www.eleconomista.es/tecnologia-internet/noticias/5294525/11/13/LastPass-asegura-que-el-ciberataque-a-Adobe-afecto-a-152-millones-de-usuarios.html#.Kku87UOF1oqii3i

RT. (26 de Agosto de 2013). Recuperado el 22 de Enero de 2015, de http://actualidad.rt.com/actualidad/view/103929-crimen-digital-conocidos-delitos-informaticos

S21Sec. (17 de Octubre de 2011). *Blog S21Sec*. Recuperado el 1 de Julio de 2014, de http://blog.s21sec.com/2011/10/estados-unidos-principal-foco-de.html

S21Sec. (2014). *Información privada S21Sec.* Madrid.

S21Sec.com. (s.f.). Recuperado el 10 de Septiembre de 2014, de http://www.s21sec.com/

Seguridad Online. (s.f.). Recuperado el 9 de Septiembre de 2014, de http://seguridadonline.net/que_es_seguridadonline.html

SeguridadPc.net. (s.f.). Recuperado el 26 de Enero de 2015, de http://www.seguridadpc.net/troyanos.htm

Softonic. (1 de Enero de 2015). Recuperado el 30 de Junio de 2014, de http://articulos.softonic.com/frases-celebres-informatica-ordenadores

Spys.ru. (s.f.). Recuperado el 7 de Octubre de 2014, de spys.ru/en/

VirusTotal. (s.f.). Recuperado el 1 de Octubre de 2014, de https://www.virustotal.com/es/

WannBrowser. (s.f.). Recuperado el 11 de Sepiembre de 2014, de http://www.wannabrowser.com/

Web Security. (s.f.). Recuperado el 26 de Agosto de 2014, de http://www.websecurity.es/como-identificar-y-prevenir-phishing

Who.is. (s.f.). Recuperado el 1 de Febrero de 2015, de https://who.is/whois

Wikipedia. (s.f.). Recuperado el 30 de Septiembre de 2014, de http://es.wikipedia.org/wiki/MD5

Wikipedia. (s.f.). Recuperado el 6 de Octubre de 2014, de http://es.wikipedia.org/wiki/Scam_baiting

Wikipedia. (s.f.). Recuperado el 27 de Octubre de 2014, de http://es.wikipedia.org/wiki/CISM

Wikipedia. (s.f.). Recuperado el 21 de Enero de 2015, de http://es.wikipedia.org/wiki/Hacker_%28seguridad_inform%C3%A1tica%29

Wikipedia. (s.f.). Recuperado el 21 de Enero de 2015, de http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

Yahoo. (26 de Enero de 2015). Recuperado el 30 de Junio de 2014, de https://es-us.noticias.yahoo.com/cu%C3%A1les-4-tipos-fraudes-digitales-comunes-142409310.html

15. Glosario

A

AntiVirus
Software cuya labor consisten en el análisis, detección y eliminación de diversos tipos de virus, así como cualquier otro tipo de software malicioso. 94

B

Backdoor
Traza de código en un sistema o aplicación, que permite la entrada al mismo obviando cualquier sistema de seguridad con la intención, maliciosa o no, de obtener una entrada secreta 56

BotNet
Red de ordenadores que, tras ser infectados por un malware, actúan conjuntamente para llevar a cabo una labor común aprovechando el desconocimiento de sus propietarios. Suelen ser usadas, por ejemplo, en ataques de denegación de servicio. 14

C

Caché Web
Memoria intermedia que permite almacenar documentos para reducir ancho de banda y sobrecarga de recursos en un servidor. 114

ccLTD
Código de dos caracteres utilizado como extensión de los dominios para indicar el empplazamiento geográfico de estos. 97

Cibercrimen
Todo delito o actividad criminal perpetrado a través de Internet. 14

Cibercriminal
Individuo que utiliza la red para beneficiarse por medio de técnicas o mecanismos ilegales. 15

Ciberterrorismo
Modalidad de terrorismo que utiliza el *Ciberdelito* como metodología 69

CPD
Ubicación que almacena los datos necesarios para el correcto procesamiento de la información por parte de una organización 78

Cuenta Fantasma
Cuenta creada con objetivo temporal, normalmente sin datos personales relevantes y que pasará a un estado permanente de inactividad una vez el usuario haya visto satisfecha la motivación de su apertura 17

D

DDoS
Ataque *DoS* que se beneficia de una *BotNet* para realizar un ataque a mayor escala 114

DNS
Servidor que se encarga de mapear *IP's* a nombres de *Dominio*. 29

Dominio
Red que identifica un conjunto de dispositivos conectados a Internet. 3

DoS
Ataque informático que inutiliza un servicio o recurso mediante la saturación del mismo a partir de peticiones masivas de conexión 114

F

Feedback

Anglicismo que se refiere a la retroalimentación proporcionada por el analista a la empresa cliente..... 45

G

gTLD

Còdigo de tres o más caracteres que se utiliza como extensión de un dominio y está reservado a cierto tipo en particular de organizaciones. 97

Gusano informático

Es un programa malicioso con capacidad de autoreplicarse a sí mismo para propagarse a otros ordenadores .. 112

H

Hacker

Individuo con altos conocimientos en seguridad informática, cuyas acciones tienen como objetivo poner a prueba infraestructuras digitales supuestamente seguras, con el fin de sayudar a mejorar la protección de las mismas. 15

Hacktivista

Hacker cuyas acciones no tienen motivación criminal ni delictiva sino una finalidad política o ideológica..... 16

HTTP

Protocolo de transferencia de hipertexto 48

HTTPS

Protocolo de transferencai de hipertexto de manera segura. 32

I

Infraestructuras Críticas

Infraestructuras estratégicas imprescindibles para el desarrollo de servicios indispensables para la comunidad112

Ingeniería Social

Conjunto de técnicas psicológicas y habilidades sociales cuyo empleo se destina a la obtención de información de terceros. 30

Inteligencia Artificial

Especialidad computacional que se enfoca en la creación de sistemas capaces de emular el comportamiento de la mente humana mediante la toma de decisiones lógicas y el desempeño de acciones en consecuencia de estas 103

IP

Etiqueta numérica asociada a un dominio que lo identifica de cara a Internet 23

ISP

Empresa encargada de proporcionar conexión a Internet a sus clientes..... 24

K

Keylogger

Software mailicioso cuya labor es capturar las teclas pulsadas por el usuario para recabar información privada del mismo..... 26

M

MD5

Algoritmo criptográfico que pretende garantizar la integridad de un archivo mediante el cifrado del mismo 57

T

U

W