



Murcia
control y auditoria

www.murcia.org

www.seguridadsi.murcia.org

Miguel Ángel
Hernández Ruiz

hernandezrma@gmail.com



Phishing

Cada día son más las empresas e instituciones que realizan operaciones bancarias por internet. Este crecimiento, a pesar de augurar un buen futuro al e-commerce no es carente de amenazas. Una de estas amenazas es lo que conocemos como phishing, y que representa un gran peligro si dentro de la organización no se encuentra instaurada una cultura de seguridad informática, una buena metodología de aprendizaje y adquisición de conocimiento, y una conciencia por parte de la dirección de la importancia de este tipo de engaños en todos los niveles jerárquicos.

Un arma devastadora

Son muchos los métodos de ataque usados por personas malintencionadas para atentar contra los cuatro pilares básicos de la transmisión y almacenamiento de información; confidencialidad, disponibilidad, integridad y no repudio. Uno de los más habituales es aquel que conocemos como *phishing*.

Existen diferentes definiciones para este término derivado del inglés fishing que significa pescando. En este caso lo que se pretende capturar no es otra cosa que datos privados de forma fraudulenta; nombres de usuario y contraseñas, números de tarjeta de crédito, números de cuentas bancarias y cualquier otro dato privado que el atacante considere de valor.

Una de las definiciones más acuñadas es aquella que liga el término phishing con su procedencia, de esta forma podríamos definirlo como aquel método por el cual un atacante conocido como *phisher* pretende obtener datos privados de un usuario

Phishing: método por el cual un atacante conocido como phisher pretende obtener datos privados de un usuario de banca por Internet suplantando a su banco o caja por medio de un mensaje de correo electrónico.

de banca por Internet suplantando a su banco o caja por medio de un mensaje de correo electrónico.

Entendido en un sentido amplio el término phishing puede utilizarse para referirse a cualquier tipo de engaño que pretenda obtener información privada de forma fraudulenta a través del correo electrónico suplantando a una entidad real. El phishing hace uso de lo que se conoce como *ingeniería social*, que no es otra cosa que el uso de habilidades sociales para manipular a usuarios legítimos con el fin último de obtener algún tipo de información.

El phishing es utilizado en otros métodos de ataque como por ejemplo el *scam*, además surgen multitud de variantes dependiendo del medio que se usa para contactar con la víctima como el *vishing* o el *smishing*.

Kits de phishing

La evolución natural de los sistemas de fraude así como de los procedimientos de ataque es la tendencia a automatizarse. El phishing no es una excepción y podemos encontrar conjuntos de herramientas que nos permiten lanzar un ataque a coste 0 y en un corto lapso de tiempo [1].

Un *kit de phishing* es un conjunto de herramientas que interactúan entre sí para conseguir que un usuario con pocas nociones técnicas sea capaz de lanzar un ataque de phishing.

Un kit de phishing habitualmente incluye herramientas para desarrollar webs que suplanten a las originales manteniendo un nivel de semejanza bastante alto con la entidad que se pretende estafar, software de spamming, que permite automatizar el envío masivo de e-mails y en algunos casos incluso listas de e-mails a los que enviar por correo el spam.

No resulta nada difícil hacerse con uno de estos kits e incluso con las instrucciones para usarlo, basta con una simple búsqueda en google.

Whaling, a la caza de ballenas

Una variante que ha surgido más actualmente de lo que conocemos como phishing es el *whaling* o *caza de ballenas*. El término está relacionado directamente con los destinatarios de este tipo de fraude; los mandatarios y directivos de las empresas. Este tipo de engaño consiste en que el atacante se hace pasar por una organización gubernamental o por qué no, por un banco, instando a uno de los máximos mandatarios de una empresa a que descargue un formulario desde una web. Cuando la persona en cuestión descarga el formulario a su sistema

***Ingeniería Social:* uso de habilidades sociales para manipular a usuarios legítimos con el fin último de obtener algún tipo de información.**

***Kit de Phishing:* conjunto de herramientas que interactúan entre sí para conseguir que un usuario con pocas nociones de informática sea capaz de lanzar un ataque de phishing.**

***Whaling:* El término está relacionado directamente con los destinatarios de este tipo de fraude; los mandatarios y directivos de las empresas.**

y lo abre, se ejecuta un código malicioso adjunto a dicho formulario que intenta recuperar información del ordenador de la víctima [2].

Se dan casos en los que un código malicioso cifra el contenido de ciertos directorios del disco duro del sistema comprometido y exige un rescate a cambio de la clave que los descifra. En un caso reciente, el contenido resulta prácticamente irrecuperable sin dicha clave [3].

La situación actual del phishing

El phishing está creciendo. Gracias a los anteriormente mencionados kits, prácticamente cualquier persona es capaz de lanzar correos de forma masiva y realizar este tipo de fraude.

El informe mensual RSA Online Fraud Report [4] arroja datos reveladores acerca de los países que sufren mayor SPAM o cuales son los que hospedan las páginas fraudulentas en mayor proporción, incluso detallando el número de instituciones que se vieron afectadas por este tipo de fraude. Adjuntos a este texto dispone de algunos de los datos que se desprenden del informe del mes de Junio de 2008.

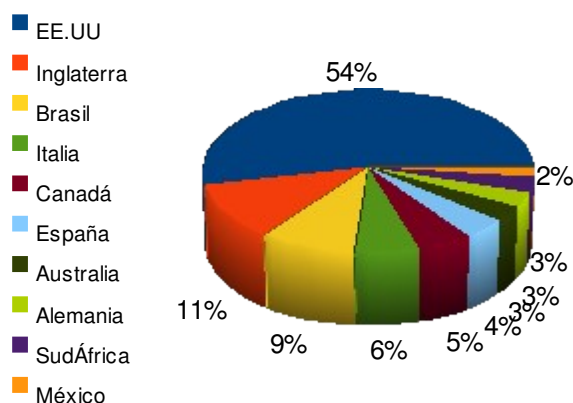


Ilustración 1: Phishing por países; Junio de 2008

Estados Unidos es el país que más ataques sufre aunque poco a poco va perdiendo porcentaje con respecto a otros países como Inglaterra, Brasil o Italia.

En Marzo de 2008 España estaba en la tercera posición con un 5% del total, pero países como Brasil, Italia y Canadá han emergido como objetivos de este tipo de engaño en los últimos meses.

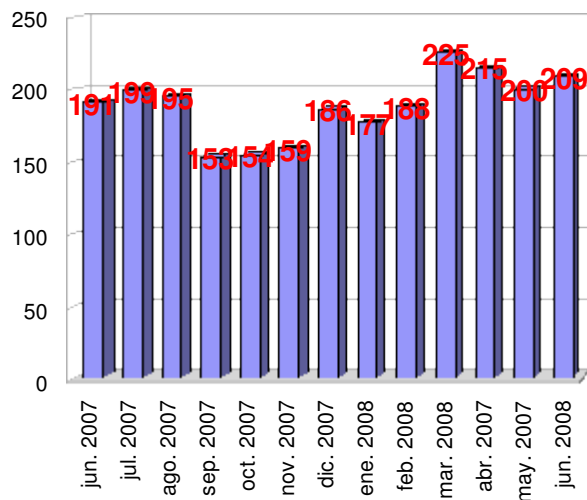
El número de entidades que tratan de ser suplantadas crece año tras año superándose una y otra vez, y mes a mes, los valores de años anteriores. El mes de Marzo de 2008 batió todos los récord con 225 entidades como objetivo de los ataques de

El Phishing crece dada la facilidad con la que se pueden realizar estos tipos de ataques en la actualidad.

Estados Unidos es el país más castigado pero mes tras mes, nacionalidades como Inglaterra le restan porcentaje.

En Marzo de 2008 España estaba en la tercera posición con un 5% del total pero países como Brasil, Italia y Canadá han emergido como objetivos de este tipo de engaño en los últimos meses.

phishing, pero llama especialmente la atención que a partir de dicho mes, en ninguno se ha bajado de las 200 entidades como objetivo de este tipo de fraude.

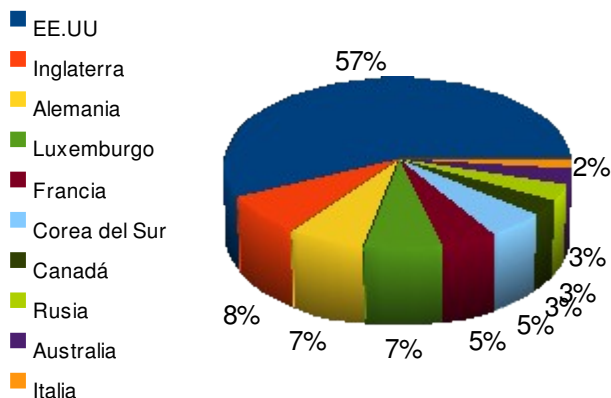


Si tenemos en cuenta la tendencia alcista del mes de Julio del año pasado podemos esperar que Julio de 2008 roce el récord establecido en el mes de marzo.

Ilustración 2: Entidades suplantadas por mes

Si tenemos en cuenta la tendencia alcista del mes de Julio del año pasado podemos esperar que Julio de 2008 roce el récord establecido en el mes de marzo.

A la cabeza de los países que albergan mayor número de páginas suplantando a entidades bancarias se encuentra también Estados Unidos, seguida de Inglaterra y Alemania. China increíblemente se ha caído de esta lista en el mes de Junio tras ocupar la segunda posición en los meses de Abril y Mayo de 2008.



A la cabeza de los países que albergan mayor número de páginas fraudulentas se encuentra también Estados Unidos, seguida de Inglaterra y Alemania.

Ilustración 3: Páginas Fraudulentas; Junio de 2008

En España, un estudio realizado por INTECO [5] a finales de 2007 mostraba información interesante acerca de los casos de phishing recibidos por los internautas de nuestro país y los importes defraudados en los casos de éxito.

El 70,1% de los encuestados afirma no haber sido víctima del phishing mientras que del 29,9% restante, el 27,8% declara no haber sufrido perjuicio económico. Tan sólo el 2,1% resulta en casos de éxito. Podemos pensar que este es un porcentaje bajo pero se ha de tener en cuenta que un phisher puede llegar a enviar miles de correos.

Las cantidades defraudadas no son muy elevadas en un alto porcentaje, de forma que no suelen ser denunciadas. el 75% de los fraudes no supera los 500€ y tan sólo el 4% supera los 5000€.

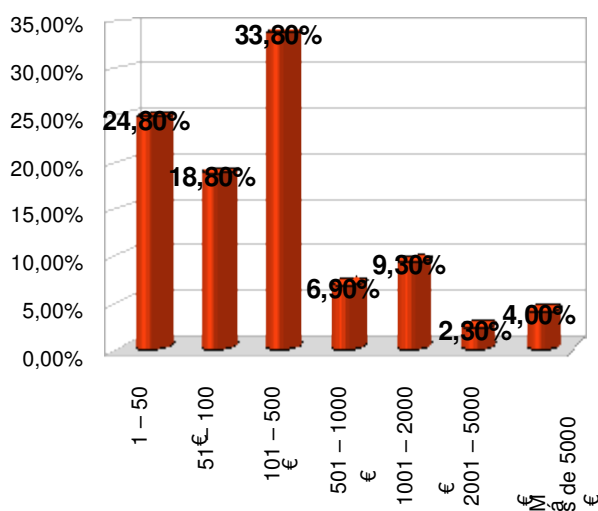


Ilustración 4: % Cantidades Defraudadas

El Phishing desde la perspectiva del Auditor

El phishing atenta directamente contra la confidencialidad de los datos de una forma sutil, induciendo al afectado a que revele información privada.

Está considerado como un ataque activo puesto que exige una iniciativa por parte del atacante con un objetivo claramente definido, existiendo una respuesta por parte de la entidad atacada. Por contra, los ataques pasivos buscan cierta información en distintos medios, como por ejemplo en la red. Dentro de este tipo de ataques podemos encontrar el sniffing o fisgoneo, consistente en recabar información que pasa por la red.

Como tal, el phishing no ataca directamente ningún activo físico ni lógico de la organización, de forma que sus sistemas no están en peligro, a no ser que se use para recabar otro tipo de información no bancaria, pero su peligro podría ser potencialmente mayor, dado que el compromiso de un número de cuenta en el que se reflejan todas las transacciones y el susten-

En España, el 70,1% de los encuestados afirma no haber sido víctima del phishing mientras que del 29,9% restante, el 27,8% declara no haber sufrido perjuicio económico.

Las cantidades defraudadas no son muy elevadas en un alto porcentaje, de forma que no suelen ser denunciadas. el 75% de los fraudes no supera los 500€ y tan sólo el 4% supera los 5000€.

El phishing está considerado como un ataque activo puesto que exige una iniciativa por parte del atacante con un objetivo claramente definido, existiendo una respuesta por parte de la entidad atacada.

to económico de la organización puede dar lugar a infinidad de problemas que pueden ir desde el robo, pasando por la extorsión y llegando en un caso extremo a la caída de la empresa.

Contra el phishing se pueden interponer muchos medios, automatizados o no, en pos de su prevención. Una alternativa cada vez más utilizada son los clientes de correo electrónico que desde hace algún tiempo identifican los correos fraudulentos avisando al usuario. No obstante, sería posible que algún correo pasase los filtros de los lectores y en ese caso, solo nos queda el conocimiento. La mejor solución pasa por que en la empresa se encuentre instaurada una conciencia y un entrenamiento formal en materia de seguridad.

La seguridad real dependerá siempre del personal de la empresa, tanto directivos como empleados, siendo la conciencia en esta materia necesaria en todos los niveles de la organización.

Referencias

- [1] Murcia, Control Y Auditoría, página de noticias.
“¿Kits de Phishing?”
<http://www.seguridadsi.murcia.org/node/12>
- [2] Murcia, Control Y Auditoría, página de noticias.
“Whaling, el spoofing de alto standing”
<http://www.seguridadsi.murcia.org/node/22>
- [3] Murcia, Control Y Auditoría, página de noticias.
Karspersky busca solución al virus que encripta el Disco Duro
<http://www.seguridadsi.murcia.org/node/48>
- [4] RSA Security Division
“Online Fraud Intelligence Report”
http://www.rsa.com/phishing_reports.aspx
- [5] Instituto Nacional de Tecnologías de la Comunicación
“Estudio sobre usuarios y entidades públicas y privadas afectadas por la práctica fraudulenta conocida como phishing”
<http://www.inteco.es/>

La mejor solución pasa por que en la empresa se encuentre instaurada una conciencia y un entrenamiento formal en materia de seguridad.

La seguridad real dependerá siempre del personal de la empresa.