Simulación de un ataque de Ingeniería Social para el robo de credenciales mediante SOCIAL ENGINEER TOOLKIT

Autor: Maíllo Fernández, Juan Andrés.

Director/es: Rodelgo Lacruz, Miguel.

Contacto: jmaifer@et.mde.es, mrodelgo@cud.uvigo.es

Resumen: La ciberdelincuencia gana peso año tras año en el volumen total de infracciones que se cometen, tanto en España como en el resto del mundo. La gran revolución que han supuesto las TIC en el mundo actual en el que vivimos, unido a las facilidades que les han proporcionado a los delincuentes, han creado el caldo de cultivo perfecto para que hoy en día tengamos que ser más precavidos ante un robo en Internet que cuando salimos a la calle.

Y dentro de este escenario, los delitos más comunes son los relacionados con los fraudes informáticos, especialmente aquellos que tienen que ver con los robos de credenciales de los usuarios en los servicios *On-Line*, aquello que denominamos *Phishing*.

Es sumamente importante que tanto los responsables de seguridad como los propios usuarios estén familiarizados con este tipo de ataques, su modus operandi y sus consecuencias, para que sean capaces de detectarlos antes de llegar a ser víctimas de ellos.

A lo largo de este trabajo se abordarán cuestiones relativas a la Ciberseguridad en el ámbito de los ataques mediante Ingeniería Social, proporcionando al lector una visión global del problema que suponen y estudiando el funcionamiento de los mismos mediante una simulación de ataque con *Social Engineer Toolkit*, de modo que consiga adquirir las capacidades necesarias para saber cuándo está siendo objetivo de un intento de fraude.

Palabras clave: Seguridad de la información, Ingeniería Social, robo de credenciales, Social Engineer Toolkit, Phishing

---

1. Introducción

1.1. Motivación y objetivos

La aparición y la gran expansión que han experimentado las TIC en el mundo actual durante los últimos años han producido grandes cambios en nuestra vida diaria, tanto en el ámbito laboral como en el personal. Pero a pesar de habernos aportado grandes ventajas, también han traído consigo bajo el brazo nuevas amenazas a las que debemos hacer frente para salvaguardar nuestra seguridad.

Los delincuentes también han sabido aprovechar las nuevas tecnologías para cometer sus crímenes, y se han adaptado con rapidez a este nuevo paradigma al darse cuenta de las enormes posibilidades que les ofrecían.

Esta circunstancia obliga a empresas y organismos a invertir gran cantidad de recursos en la seguridad de sus sistemas digitales que los hace cada vez más resistentes a posibles acciones malintencionadas. Pero hay un elemento dentro de todo el conjunto que sigue siendo el más débil, y por lo tanto uno de lo más explotados: las personas.

Ante esta situación, se hace tremendamente importante conocer el modo de actuación que siguen los cibercriminales en este tipo de ataques, de modo que tanto los usuarios como los administradores de los sistemas de información sean conscientes de los graves riesgos a los que están expuestos y tengan la capacidad de protegerse.

Para ello, los objetivos que se persiguen en el presente Trabajo Fin de Máster son los siguientes:

- Estudiar la situación actual de la ciberdelincuencia en España, incluyendo los tipos de ataques más habituales que se producen.
- Introducirnos en los ataques de Ingeniería Social, especialmente en aquellos que tienen como propósito el robo de credenciales de usuarios.
- Conocer las capacidades y funcionamiento de la herramienta SET (*Social Engineer Toolkit*), y profundizar en las opciones que ofrece para realizar el tipo de ataques que estamos estudiando.
- Realizar una simulación de un ataque, dentro de un entorno controlado, explicando el proceso del mismo.
- Analizar los resultados obtenidos, extrayendo de los mismos las conclusiones principales que nos aporten.
- Estudiar las posibles aplicaciones que podría tener este trabajo en el entorno del Ministerio de Defensa.

1.2. Situación de la ciberdelincuencia en España

Tal y como puede comprobarse en la Figura 1, el porcentaje que supone los crímenes de tipo cibernético dentro del total de las acciones delictivas cometidas en España aumenta año tras año.

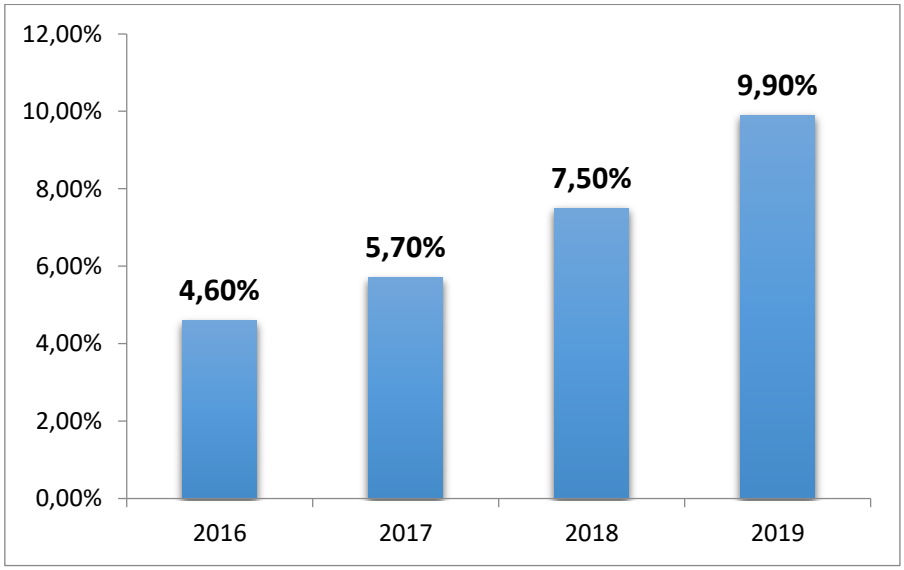

Figura 1 Evolución del porcentaje que representa la cibercriminalidad sobre el total de infracciones penales en España [1]

Y de entre todos ellos, sin lugar a dudas el más común de todos ellos es el fraude informático, que como se puede comprobar en la Figura 2 supuso casi un 90% del total en 2019, experimentando un aumento del 50% respecto al año anterior.

HECHOS CONOCIDOS	2016	2017	2018	2019
ACCESO E INTERCEPTACIÓN ILÍCITA	3.243	3.150	3.384	4.004
AMENAZAS Y COACCIONES	12.036	11.812	12.800	12.782
CONTRA EL HONOR	1.546	1.561	1.448	1.422
CONTRA PROPIEDAD INDUST./INTELEC.	129	121	232	197
DELITOS SEXUALES(*)	1.231	1.392	1.581	1.774
FALSIFICACIÓN INFORMÁTICA	3.017	3.280	3.436	4.275
FRAUDE INFORMÁTICO	70.178	94.792	136.656	192.375
INTERFERENCIA DATOS Y EN SISTEMA	1.336	1.291	1.192	1.473
Total HECHOS CONOCIDOS	**92.716**	**117.399**	**160.729**	**218.302**

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración

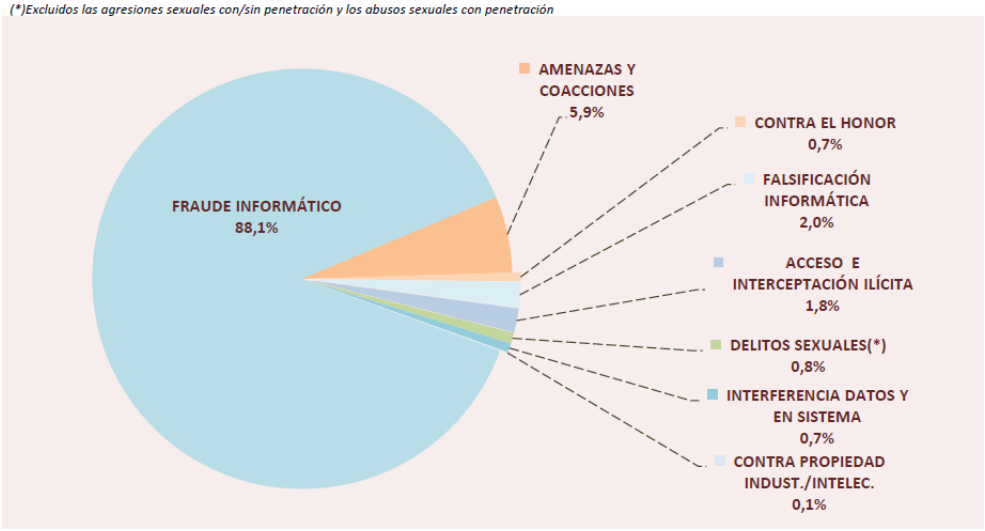

Figura 2 Evolución de hechos conocidos por categorías delictivas. Imagen extraída del Estudio sobre la cibercriminalidad en España de la Secretaría de Estado de Seguridad [1]

Uno de los métodos más extendidos para llevar a cabo este tipo de ataques consiste en el robo de las credenciales de acceso a los sistemas de los usuarios. Y para ello los delincuentes cuentan con una disciplina que les aporta grandes resultados en este sentido: la Ingeniería Social.

1.3. Introducción a la Ingeniería Social

Se puede definir la Ingeniería Social como el arte de obtener información de personas sin que estas sean conscientes de lo que están haciendo, para lo cual se recurre a engaños, técnicas psicológicas y habilidades sociales. Un atacante con buenas dotes para esta disciplina puede obtener gran cantidad de información de un usuario sin que éste sea consciente de lo que está sucediendo en realidad.

El padre de la Ingeniería Social, Kevin Mitnick, enumera cuatro principios básicos innatos al ser humanos en los que se basa cualquier acción de Ingeniería Social para lograr sus objetivos [2]:

- Todos queremos ayudar.
- El primer impulso hacia alguien que no conocemos es de confianza hacia él.
- A nadie le gustar decir no.
- A todos nos gusta que nos adulen.

Para ello se pondrán en práctica diferentes técnicas que actúan sobre el propio comportamiento humano, llevadas a cabo por el propio atacante como el *Pretexting*, el *Quid Pro Quo* o el *Tailgating* (entre otros), o con ayuda de herramientas digitales como sucede en el caso que vamos a estudiar para un ataque de *Phishing* [3].

2. Desarrollo

Para comprobar la eficacia de este tipo de ataques, y comprender mejor el funcionamiento de los mismos, se llevará a cabo una simulación de un robo de credenciales [4], utilizando para ello una plataforma virtualizada mediante VirtualBox [5] donde desplegaremos una máquina virtual con Kali Linux [6] (distribución orientada a pruebas de *Pentesting*) que hará las veces de atacante, y utilizando el sistema anfitrión con Microsoft Windows 10 como víctima.

Dentro de la máquina con Kali Linux, se recurre a la herramienta *Social-Engineer Toolkit* [7], una completa suite desarrollada con Phyton que nos ofrece múltiples funcionalidades para automatizar ataques mediante Ingeniería Social.

En nuestro caso vamos a emplear una opción que nos permitirá llevar a cabo un ataque de *Web Spoofing* de un modo muy sencillo [8] y [9], creando una copia idéntica de una web de *login* a la que haremos llegar a nuestra víctima para que intente acceder al servicio.

Una vez el usuario haya introducido sus credenciales, estas serán recogidas automáticamente en SET dentro de Kali Linux (véase Figura 3) y la víctima será redirigida a la página real que ha sido clonada.

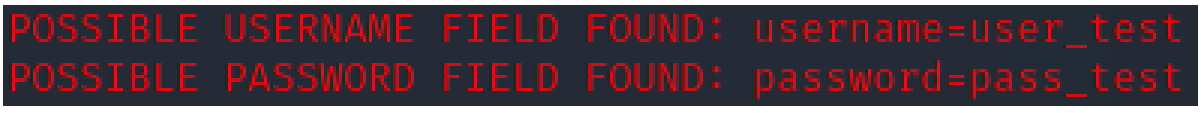

Figura 3 Resultado del robo de credenciales en la simulación del ataque de *Phishing*

De este modo es muy posible que piense que se ha producido un fallo en el proceso de autenticación y vuelva a meter su nombre de usuario y su contraseña, accediendo esta vez sí al servicio y (muy probablemente) sin ser consciente en ningún momento de haber sido víctima de un ataque de *Phishing*.

3. Resultados y discusión

Después de llevar a cabo la simulación, somos conscientes de lo sencillo que puede resultar a un cibercriminal poner en práctica esta técnica para intentar hacerse con las credenciales de acceso de los usuarios de los servicios web. En tan solo unos pasos, y apoyándose en herramientas como SET, se puede crear un clon idéntico del sistema a suplantar para lanzar el ataque.

Afortunadamente para los usuarios, estas herramientas no son perfectas, y si prestamos un poco de atención a los detalles podremos ser capaces de detectar en muchas ocasiones que el sitio web al que nos han enviado no es el real y estamos siendo víctimas de un *Phishing*. Pero de todos modos no debemos bajar la guardia, ya que los atacantes cada vez perfeccionan más sus acciones y resulta más complicado detectarlas.

Métodos como los ataques homográficos para conseguir que la *URL* del sitio clonado se parezca a la real, la incorporación de certificados digitales para implementar la web con protocolo *HTTPS*, o la distribución de enlaces a nuestro *website* malicioso con pretextos bien diseñados y técnicas de suplantación de remitentes, nos dificultarán la labor de detección de este tipo de fraudes.

4. Conclusiones

Las implicaciones que un robo de credenciales puede tener en la seguridad de nuestros sistemas es más que evidente. Si alguien no autorizado consigue tener acceso a un determinado servicio, las consecuencias pueden ir desde un robo en la cuenta de banca *On-Line* de un usuario, hasta la revelación de información clasificada en el caso de los sistemas del Ministerio de Defensa.

Teniendo en cuenta la gran proliferación que existe actualmente de este tipo de ataques, se hace completamente necesario invertir mayores esfuerzos en protegernos contra ellos [10] y [11], para lo cual se establecen las siguientes líneas futuras de trabajo:

- Securización de las aplicaciones, exigiendo la implementación de la autenticación por doble factor, aumentado de este modo la seguridad en los procesos de *login* de los servicios web.
- Despliegue de sistemas contra intrusiones en nuestra infraestructura de red (IDS, IPS y/o SIEM), que dificultarán el acceso de personas no autorizadas a la misma y nos avisará en caso de que llegue a producirse para poder minimizar daños.
- Establecimiento de políticas robustas de cambio de contraseñas, obligando a los usuarios al cambio de las mismas cada cierto tiempo, de modo que si un atacante consigue robar sus credenciales únicamente le sean de utilidad hasta el siguiente cambio.
- Implementar una campaña de información y concienciación entre los usuarios de los sistemas de nuestra organización, dando a conocer los métodos de ataques más habituales y los riesgos que pueden correr en caso de ser víctimas de uno de ellos.

Referencias

1. «Web del Ministerio del Interior,» [En línea]. Available: http://www.interior.gob.es. [Último acceso: 16 de noviembre de 2020]
2. K. Mitnick, El arte de la intrusión, Editorial Ra-Ma, 2017.

3. A. Ramos, C. A. Barbero, D. Marugán e I. González, Hacking con Ingeniería Social. Técnicas para hackear humanos, Editorial Ra-Ma, 2015.
4. P. González, Ethical Hacking. Teoría y práctica para la realización de un pentesting, Editorial 0xWORD, 2015.
5. «Web de Oracle VM Virtual Box,» [En línea]. Available: https://www.virtualbox.org. [Último acceso: 19 de noviembre de 2020]
6. «Web de Kali Linux,» [En línea]. Available: https://www.kali.org. [Último acceso: 19 de noviembre de 2020]
7. «Web de Social Engineering Toolkit,» [En línea]. Available: https://github.com/trustedsec/social-engineer-toolkit. [Último acceso: 24 de noviembre de 2020]
8. P. González, G. Sánchez y J. M. Soriano, Pentesting con Kali 2.0, Editorial 0xWORD, 2015.
9. M. A. Caballero y D. Cilleros, El libro del hacker. Edición 2018, Ediciones Anaya Multimedia, 2018.
10. «Web de la Oficina de Seguridad del Internauta,» [En línea]. Available: https://www.osi.es. [Último acceso: 17 de diciembre de 2020]
11. «Web del Instituto Nacional de Ciberseguridad,» [En línea]. Available: https://www.incibe.es. [Último acceso: 17 de diciembre de 2020]