GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Phishing introduction

Exercises

017 TU AYUDA EN CIBERSEGURIDAD
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDEX

1. Practical Exercises 3
2. Research exercise 7

FIGURE INDEX

Figure 1 Practical exercise – Spear phishing mail 3
Figure 2 Practical exercise – Phishing mail 4
Figure 3 Practical exercise – Phishing website 4
Figure 4 Practical exercise – Real mail 5
Figure 5 Practical exercise – Real SMS 6
Figure 6 Practical exercise – Spim 6
Figure 7 Research exercise – Benign mail 7
Figure 8 Research exercise - Benign Word document 8
Figure 9 Research exercise – Malicious mail 8
Figure 10 Research exercise – Reverse shell 9
Figure 11 Research exercise - VirusTotal 9

1. PRACTICAL EXERCISE

In this exercise, we try to discern between possible benign mailings and phishing.

It analyzes the different elements of phishing, (pretext, sender, URL or attachments), in case of a scam it will be classified among the different types of phishing studied, i.e:

- Generic Phishing,
- Spear phishing,
- Whale Phishing,
- Mailing chain,
- Smishing,
- Spim,
- Vishing.

Once the file has been decompressed, you will find several directories with different cases.

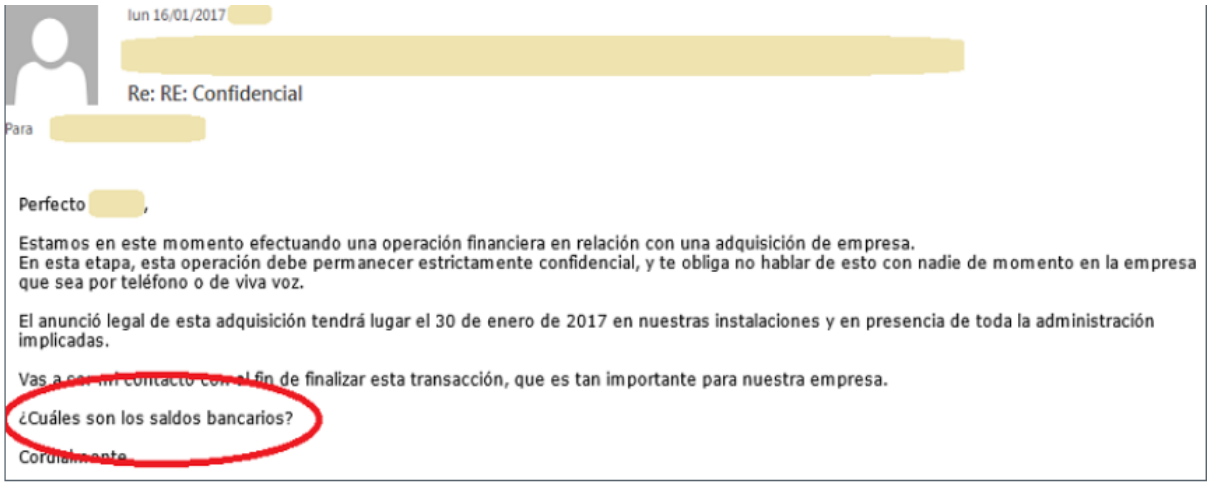
In each case there are different images belonging to possible phishing.

Solution

Case 1

Spear phishing

This can be discerned from the elaboration of the pretext and the requirement of the bank details for a transaction.


lun 16/01/2017

Re: RE: Confidencial

Para

Perfecto ,

Estamos en este momento efectuando una operación financiera en relación con una adquisición de empresa.
En esta etapa, esta operación debe permanecer estrictamente confidencial, y te obliga no hablar de esto con nadie de momento en la empresa que sea por teléfono o de viva voz.

El anunció legal de esta adquisición tendrá lugar el 30 de enero de 2017 en nuestras instalaciones y en presencia de toda la administración implicadas.

Vas a ser mi contacto con el fin de finalizar esta transacción, que es tan importante para nuestra empresa.

¿Cuáles son los saldos bancarios?

Cordialmente

Figure 1 Practical exercise – Spear phishing mail

Case 2

Generic Phishing

In this case it is a generic phishing impersonating the tax office.

Phishing is quite convincing as far as the sender is concerned because the domain is very similar to the real one.

The pretext is a good bait because it promises the victim an amount of money to be returned.

This scam includes a URL that redirects to a cloned agency page for data theft.

Figure 2 Practical exercise – Phishing mail

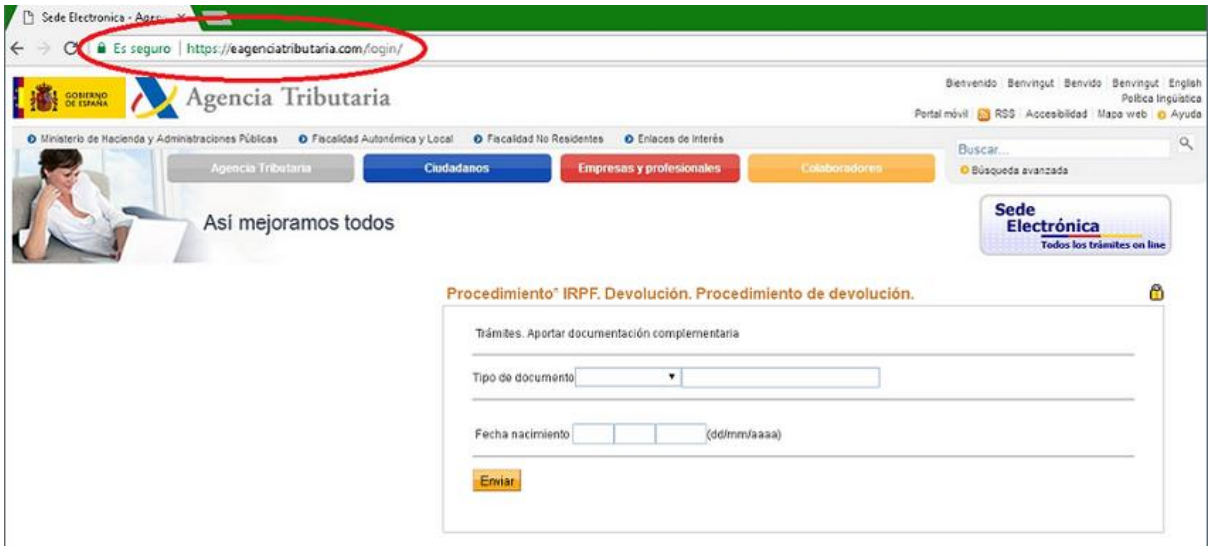


Figure 3 Practical exercise – Phishing website

Case 3

Real Mail

This mail is totally legitimate, the sender coincides with the domain of the bank, it is simply an advertisement.

De: **ING** <ing@ing.es>
Date: mié., 29 ene. 2020 8:30
Subject: Ahora invertir a lo grande es para todos
To: <su[redacted]@gmail.com>

Si no ves correctamente este email, haz clic aquí

ING

Publicidad

Ha llegado la simplicidad al mundo de la inversión.

Hola [redacted]

Puede que hasta ahora pensaras que la forma de acceder a determinados productos de inversión, por su complejidad, estaba reservada a unos pocos.

En ING, simplificamos la fórmula para acercar la inversión a todos. Con **Inversión NARANJA+** ponemos a tu alcance la forma de invertir de los que más saben, desde la cantidad que quieras, con la que podrías sacar partido a tus ahorros.

Los principales mercados del mundo en un solo producto.

A través de **Inversión NARANJA+** inviertes en empresas y gobiernos

Figure 4 Practical exercise – Real mail

Case 4.

Real SMS

This is an advertising SMS from a telecom company, if you check the URL to unlink from the service or call the number provided could be confirmed.

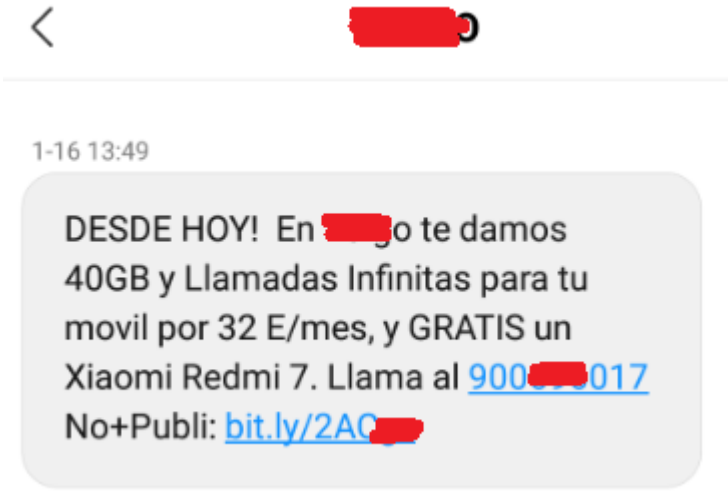


Figure 5 Practical exercise – Real SMS

Case 5

Spim – WhatsApp

This is a phishing via WhatsApp. Even without verifying the URL, it is quite clear, surely this leads the user to download a malicious software for Android, either to obtain the victim's data, install malicious software or some kind of scam.

The pretext tries to make the victim believe that he has won a prize and that he only has to enter his data.

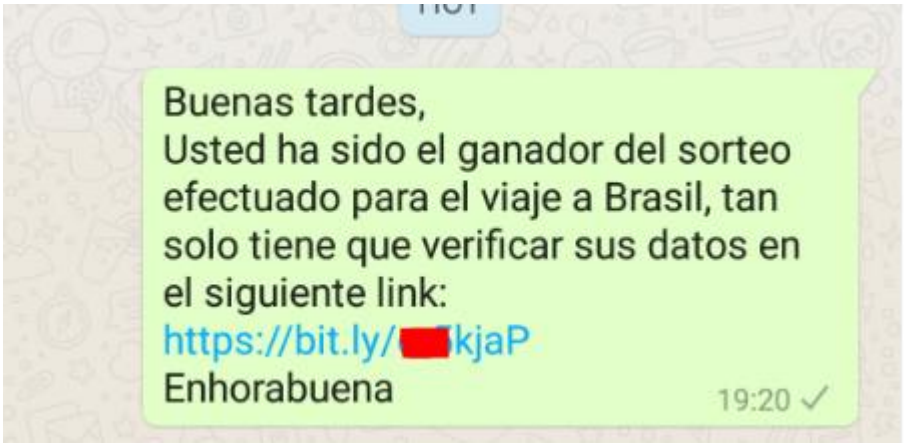


Figure 6 Practical exercise – Spim

2. RESEARCH EXERCISE

The objective of the exercise is to determine the difference between the attachments of two emails that arrived with the same origin, in one case the identity of the sender has been supplanted by the theft of the account, in the other case it is legitimate.

Since the mail sent by the same sender is totally similar, the two attachments are provided for study to verify which of them is the phishing, that is, which is malicious, and which is not.

In the zip file you will find two directories with another zip file containing the image of the email and its extracted attachment

Attachment mail 1 (benign)

The attachment is a Word document containing what appears to be customer information embedded.

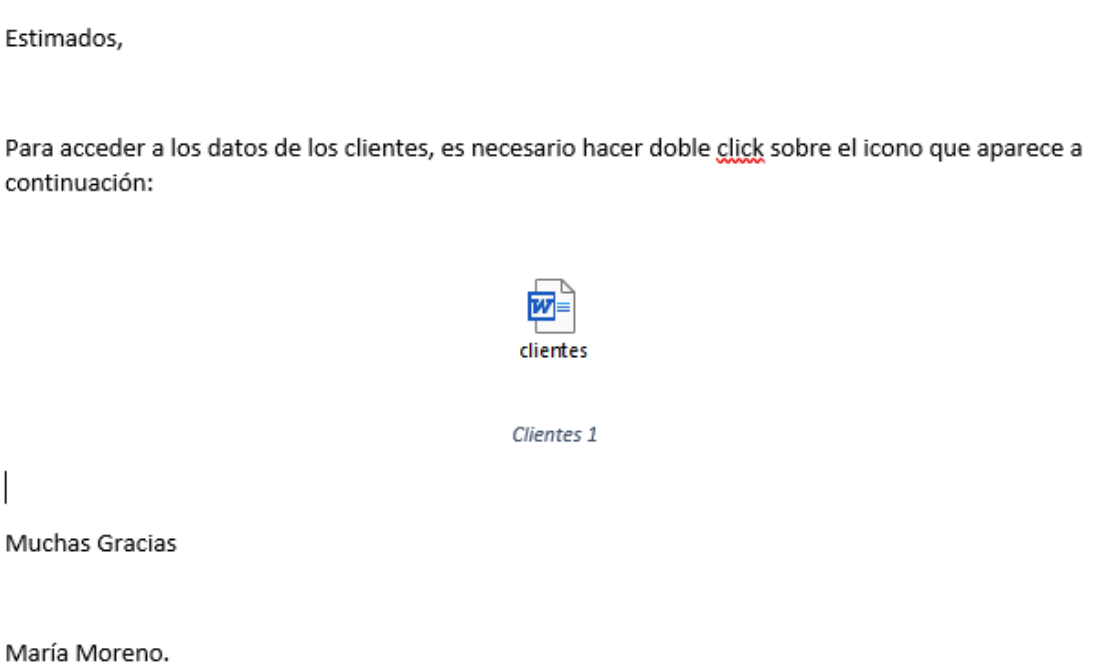


Figure 7 Research exercise – Benign mail

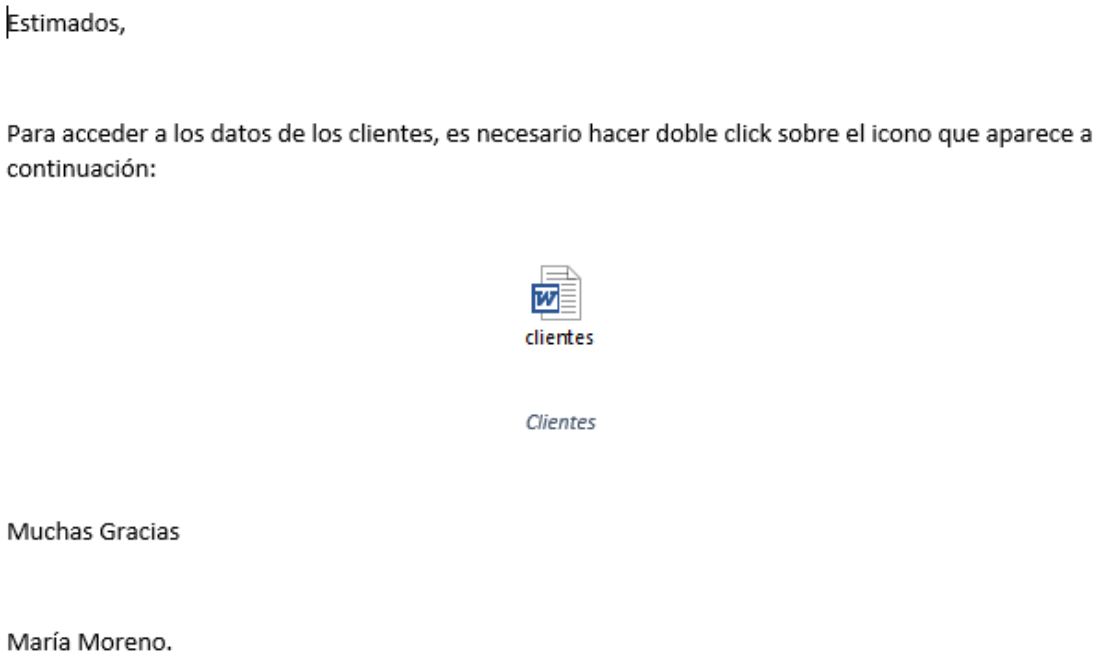
If you double-click on the document, you will see that another Word document containing the following information will open normally:

Clientes Nuevos	Contacto
Ferpozas Sociedad Limitada	Emiliano Diaz
Aerospinada	Andrea Garcia
Motores Fernandez Lopez	Francisco Fernandez

Figure 8 Research exercise - Benign Word document

Attachment mail 2 (malicious)

The attachment file is a Word document containing what appears to be customer information, apparently the same as the previous one.



Estimados,

Para acceder a los datos de los clientes, es necesario hacer doble click sobre el icono que aparece a continuación:

clientes

Clientes

Muchas Gracias

María Moreno.

Figure 9 Research exercise – Malicious mail

The difference occurs when you double-click on the embedded object.

In this case it asks for a security authorization to execute a .bat file, something that seems out of the ordinary, so the user should not accept such execution.

If you allow the execution, a command line window will open that simulates the execution of a reverse shell:

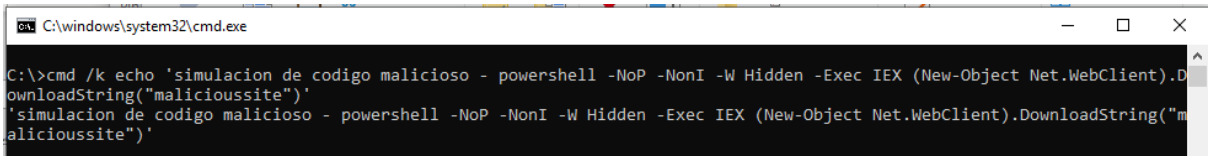


Figure 10 Research exercise – Reverse shell

If the file is uploaded to an online analysis service, such as VirusTotal, it can be seen that although in this case and for study it is not malicious because it simply writes on screen what could be a remote connection, there is some antivirus engine that marks it as malicious for this unusual behavior.

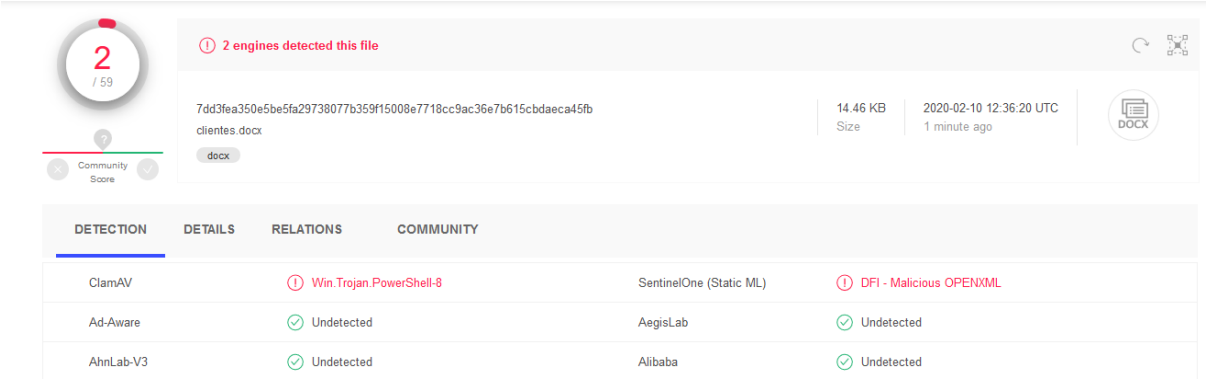


Figure 11 Research exercise - VirusTotal