



PHISHING TO 2FA

Autores de la ponencia

@carol12gory

@martrudix

Marta Barrio Marcos


Security Researcher

> 7 years of experience

CISA, CEH, CSX, OSCP

Speaker at security conferences like NN2019

Teacher in ISACA, TSS, IMF, master UCLM

 <https://es.linkedin.com/in/martabarriomarcos>
 @martrudix





Carolina Gómez Uriarte

Security Analyst

> 2 years of experience

Head of Sh3llCON

Speaker at security conferences like NN2019,
HoneyCON...

 <https://es.linkedin.com/in/carolina-gomez-uriarte>
 @Carol12Gory



#index

Part I: Introduction

- Who are we?
- Disclaimer
- What is phishing?
- How to detect phishing?

Part II: Hands on labs

- Requirements
- GoPhish
- Evilginx2

Part III: How not to be phished

- Countermeasures

Part IV: References

1. Part I

Introduction

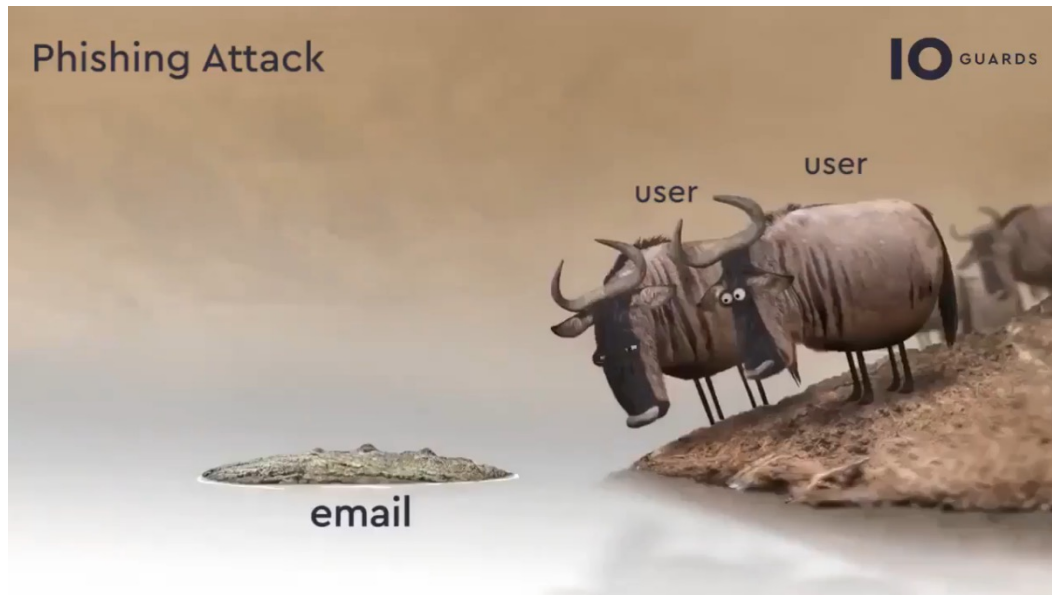
Disclaimer

This workshop is held to raise awareness and teach how cyber criminals carry out phishing attacks.

Everything explained in this workshop has been done in controlled environments and without any evil purpose.

Both speakers are not responsible for any illegitimate use for profit.

What is phishing?



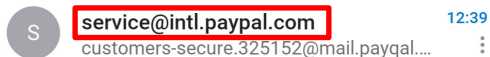
What is phishing?

- **Impersonation** of web pages, e-mails, etc.
- Use of logos, texts, images known by the user to **mislead the user** and make him fall for the trick.
- Target: credentials, malware distribution, subscriptions to spam lists...

How to detect phishing?

- Check the recipient
- Check the grammar of the mail
- Where does the link go?
- Others checks like Mail Headers: IPs, domains, etc.

Phishing examples



01/15/2020 Wednesday, 21:41:55 PM PDT,
Receipt Number: ZE55731931789465.

Hello,

You have sent a payment for \$134.90 USD
to Huawei Cloud, Inc.

Please note this transaction may take a few moments to
appear in your account overview.

[View the details of this transaction online](#)

If it was not you who did this transaction you can dispute the
transaction by clicking [Resolve Now](#)

Seller

Huawei Cloud, Inc.

Instructions for the seller

You have not entered
instructions.

Description	Price	Quantity	Subtotal
Huawei Cloud,	\$134.90	1	\$134.90



01/15/2020 Wednesday, 21:41:55 PM PDT,
Receipt Number: ZE55731931789465.

Hello,

You have sent a payment for \$134.90 USD
to Huawei Cloud, Inc.

Please note this transaction may take a few moments to
appear in your account overview.

<http://minionsuperfasters.id/I0E1aiT?idtrack=31931789>



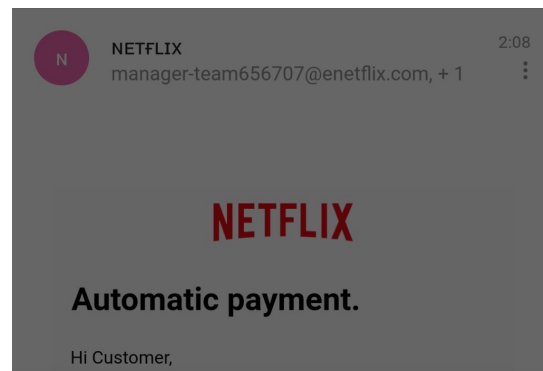
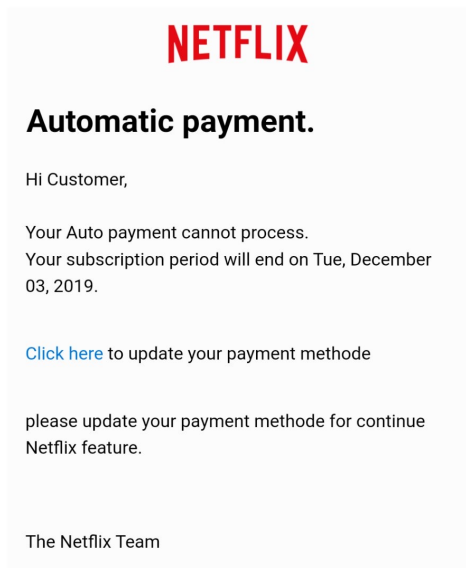
Copiar dirección del vínculo



Abrir en explorador

<https://twitter.com/t31m0/status/1217431423843520518?s=21>

Phishing examples



[http://dkawlsmgherhoafiuirgnam
eoiwwuhgsmaoeirshnnwonassd
.asoapdjw0pup.info/KAOLECNQLYWW2HP8
/OBLDPQTCM9P7SL7L5C6S0DRBBD
/SM6ZKK/KAOLECNQLYWW2HP8?reminder=
KAOLECNQLYWW2HP8](http://dkawlsmgherhoafiuirgnam
eoiwwuhgsmaoeirshnnwonassd
.asoapdjw0pup.info/KAOLECNQLYWW2HP8
/OBLDPQTCM9P7SL7L5C6S0DRBBD
/SM6ZKK/KAOLECNQLYWW2HP8?reminder=
KAOLECNQLYWW2HP8)

<https://twitter.com/t31m0/status/1201809152655405057?s=20>

Phishing examples



Estimado(a) cliente,
¡Bienvenido a Mi Endesa!

¡Notamos que pague la factura al mismo tiempo dos veces. ¿Qué debo hacer? Siga los siguientes pasos:

Importe : 41,82€

Referencia : ENDESA- ES-1028336913

Para confirmar su reembolso

Haga clic aquí

© 2019 Endesa. Reservados todos los derechos.



Estimado(a) cliente,
¡Bienvenido a Mi Endesa!

¡Notamos que pague la factura al mismo tiempo dos veces. ¿Qué debo hacer? Siga los siguientes pasos:

Importe : 41,82€

Referencia : ENDESA- ES-1028336913

Para confirmar su reembolso

Haga clic aquí

© 2019 Endesa. Reservados todos los derechos.

<https://www.rethinkhomeinteriors.com/wp-admin/Endesa/>

<https://twitter.com/t31m0/status/1194543214184808449?s=20>

Phishing examples

De: "correos@correos.com" <corree@i-med.com.au>

Fecha: 22 ene, 2020 1:22 p. m.

Asunto: Información sobre su envío

Para: [redacted]

Cc:



El envío para su pedido CR854800290 está disponible.



CR854800290

Debido Estimado cliente, En breve recibirá en su domicilio el envío CR854800290 remitido.

Para más información, pinche en el nº de envío

[HAGA CLIC AQUÍ](#)

Atentamente, Atención al Cliente Correos S.A.E. Por favor, no responda a este correo electrónico ya que su petición no será atendida.

La Información incluida en el presente correo electrónico es SECRETO PROFESIONAL Y CONFIDENCIAL, siendo para el uso exclusivo del destinatario arriba mencionado.

Si usted no es el destinatario del mensaje o ha recibido esta comunicación por error le informamos que esta totalmente prohibida cualquier divulgación, distribución o reproducción de esta comunicación.

Gracias.



Correos

12:43

Estimado cliente:

Sentimos mucho que no se pudiera entregar el paquete el 4 de noviembre.

La tasa de aduanas de 1 € estaba pendiente <http://trackmail.club/3x8>

<https://twitter.com/t31m0/status/1192408711681204224?s=12>

Phishing examples

De: Liberbank <cliente@liberbank.es>

Fecha: 3 jun. 2019 8:34 p. m.

Asunto: Notificación

Para:

Cc:

Liberbank

Buenos días,

Para evitar el uso fraudulento de tarjetas de crédito en Internet, **liberbank** tiene un nuevo sistema de control de pagos.

Este servicio es completamente gratis.

Nuestro sistema ha detectado que no activa su servicio de **Clave OTP**

Para activar este servicio, simplemente haga clic en el siguiente enlace y siga los pasos provistos :

[Acceso clientes](#)

Saludos ,

Carmen Maria Marchal Basalo.

Este email es resultado de una investigacion liberbank S.A.

<http://nuevadigital.co.vu/?ref=9809C51RO2M5BB3908H8SY1HXTFRLW3D0998D7H897>

2.

Part II

Hands on labs

Requirements

Deployment

- **GoPhish** – Mail sender
- **Evilginx** – Manage the phishing

GoPhish

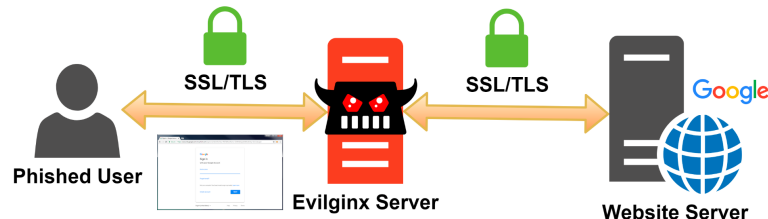
Deployment

- *Config.json* file → IP and certificates config
- Sending Profiles → Config SMTP relay.
- ~~Landing Pages → Web that is shown to the victim when he clicks on the link~~
- Email Templates → Mail received by the victim
- Users & Groups → Destinations
- Campaigns

Evilginx2

Deployment

- **Phishlet** → YAML file where are defined subdomain necessary to do proxy, which strings should be replaced in relayed packets and which cookies should be captured.
- **Lure** → generation of phishing URLs
- **Config** → general configuration
- **Sessions** → sessions and captured tokens with credentials



OMG

DEMO TIME





3. Part III

How not to be phished

Countermeasures

Recommendations for final users

- Check domain in URL bar
- Use U2F devices
- DO NOT use SMS 2FA – SIMJacking
- Common sense



Countermeasures

Recommendations for developers

- Check *window.location*
- Check *window.location* & obfuscate

```
>> window.location
< Location https://www.google.com/
  ▶ assign: function assign()
    hash: ""
    host: "www.google.com"
    hostname: "www.google.com"
    href: "https://www.google.com/"
    origin: "https://www.google.com"
    pathname: "/"
    port: ""
    protocol: "https:"
  ▶ reload: function reload()
  ▶ replace: function replace()
    search: ""
  ▶ toString: function toString()
  ▶ valueOf: function valueOf()
    Symbol(Symbol.toPrimitive): undefined
```

Countermeasures

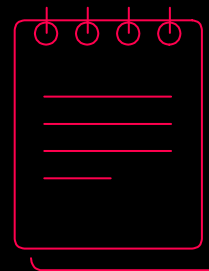
Recommendations for developers

- Check *baseURI* property of DOM items

```
>> $("body").baseURI
```

```
← "https://www.google.com/"
```

- Check headers: *X-Evilginx*



4. References

Documentation and resources

4.1 References

- <https://breakdev.org/evilginx-2-3-phishermans-dream/>
- <https://www.youtube.com/watch?v=QRyinxNY0fk>
- <https://docs.getgophish.com/user-guide/>
- <https://medium.com/@valeriyshevchenko/how-to-perform-phishing-attack-with-2fa-e9d633c66383>
- <https://www.cyberpunk.rs/evilginx-phishing-examples-v2-x-linkedin-facebook-custom>
- <https://breakdev.org/evilginx-2-next-generation-of-phishing-2fa-tokens/>



Thanks!

Any questions?

You can find us at [@martrudix](#) & [@Carol12Gory](#)