CIBERSEGURIDAD

2FA: PHISHING

Universidad de Alcalá

Alain Arsene, 11/05/2022

Universidad de Alcalá

SIE

ÍNDICE

Universidad de Alcalá

SIE

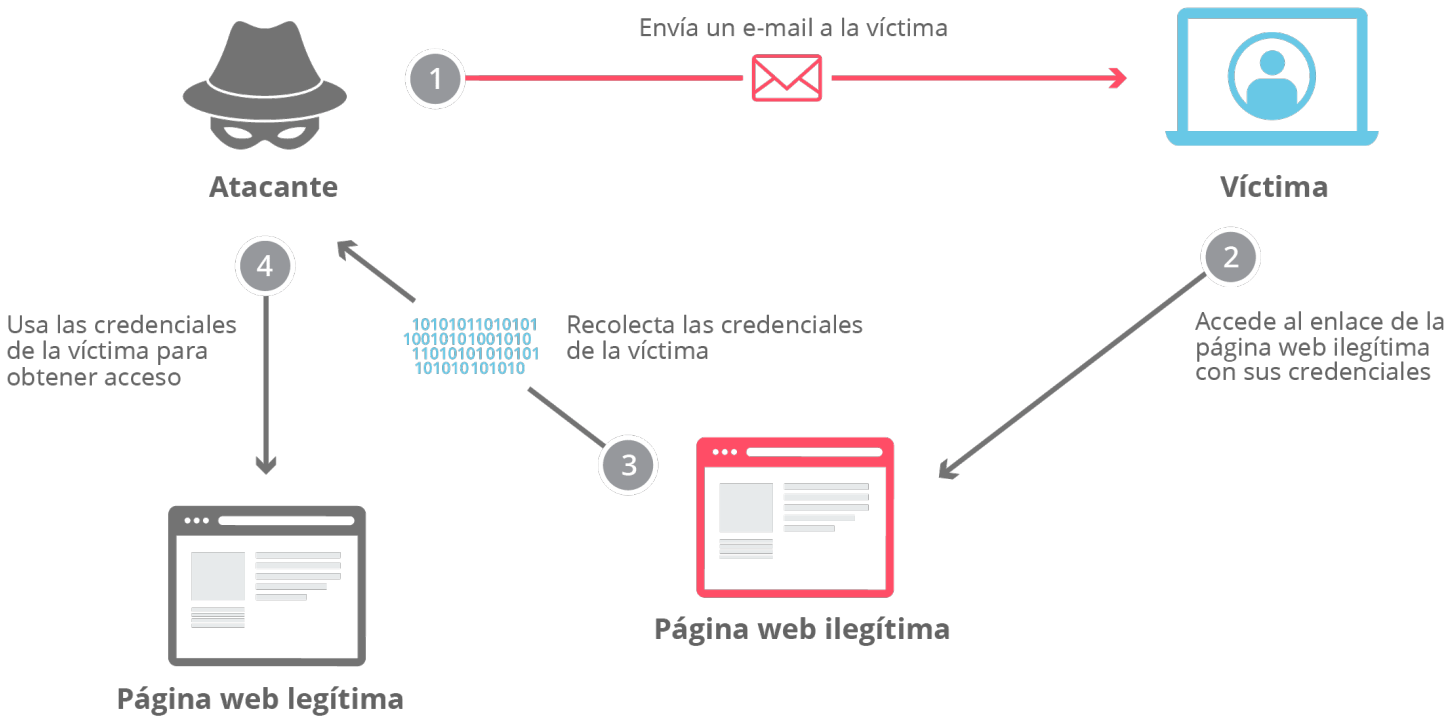
SECCIÓN I

Aviso informativo

- El propósito de esta presentación es única y exclusivamente educativo.
- Todos los conceptos explicados en esta presentación fueron probados en entornos controlados y sin intenciones maliciosas.
- Ni el ponente ni ninguna organización de las presentes en este evento se harán responsables del posible uso indebido de esta presentación o de sus contenidos por parte de otros usuarios.

SECCIÓN I

¿Qué es el phishing?



Universidad de Alcalá

SIE

SECCIÓN I

¿Qué es el phishing?

- Duplicación de páginas webs, e-mails, sms, etc.
- Uso de textos, logos e imágenes conocidas por el usuario para aumentar la confianza y hacerle caer en la trampa.
- Objetivos: datos personales, credenciales, distribución de software malicioso…

Universidad de Alcalá

SIE

SECCIÓN I

¿Cómo detectar el phishing?

- Comprobar el remitente
- Comprobar la gramática de los e-mails/sms
- Comprobar los enlaces
- Otras comprobaciones: cabeceras, IP's, dominios, etc.

Universidad de Alcalá

SIE

SECCIÓN I

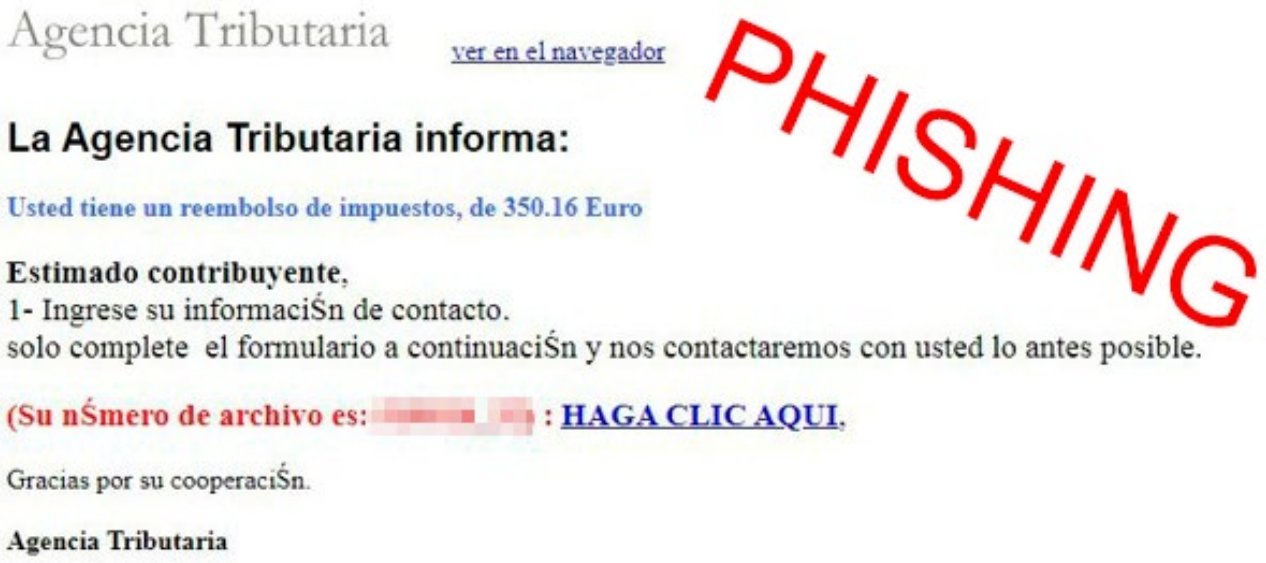
¿Cómo detectar el phishing?

Universidad de Alcalá

SIE

SECCIÓN I

¿Cómo detectar el phishing?



SECCIÓN II

Laboratorio

- GoPhish → Remitente de correos
- Evilginx2 → Gestiona la suplantación de identidad

SECCIÓN II

GoPhish

Set Templates & Targets

Gophish makes it easy to create or import pixel-perfect phishing templates.

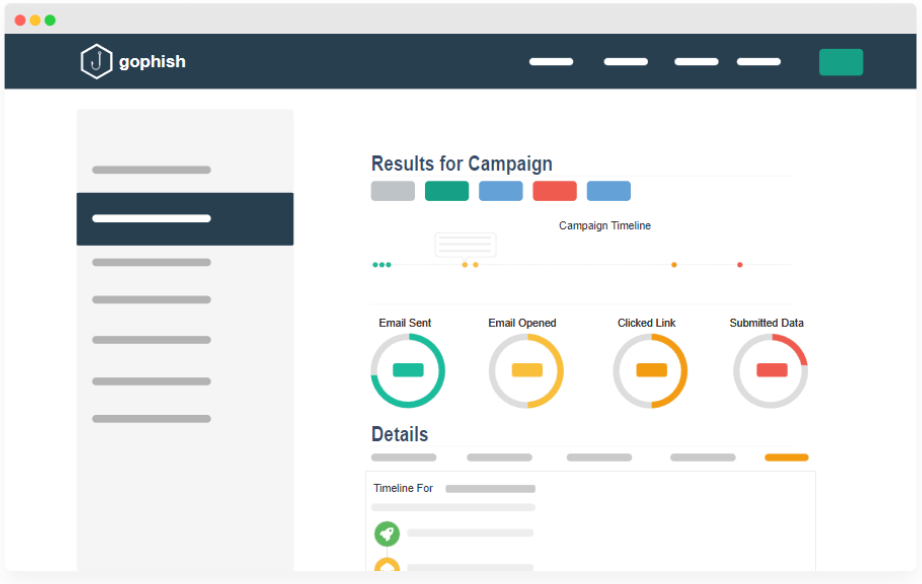
Our web UI includes a full HTML editor, making it easy to customize your templates right in your browser.

Launch the Campaign

Launch the campaign and phishing emails are sent in the background. You can also schedule campaigns to launch whenever you'd like.

Track Results

Detailed results are delivered in near real-time. Results can be exported for use in reports.



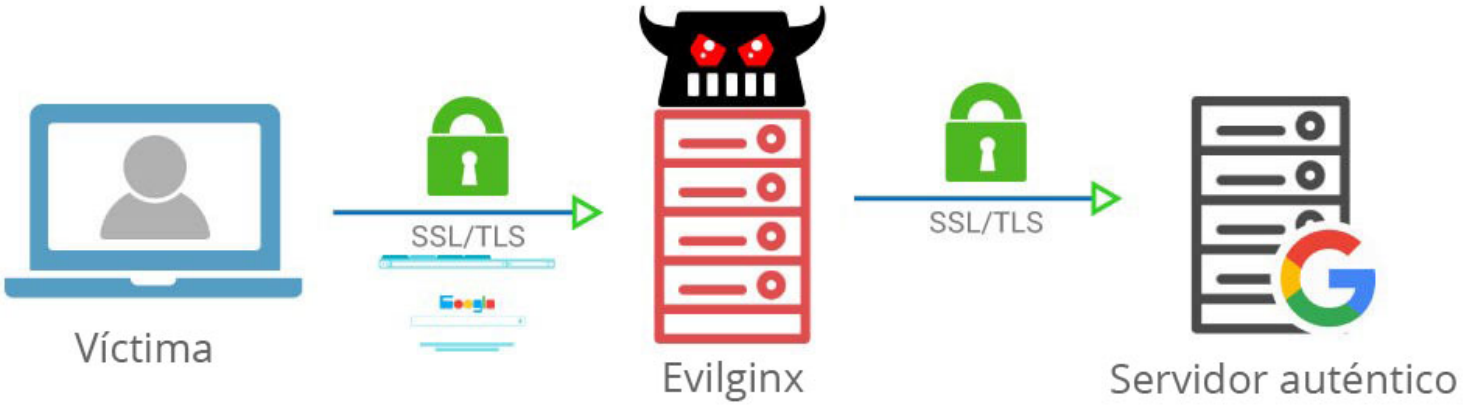
SECCIÓN II

GoPhish

- Users & Groups → Destinatarios (víctimas)
- Email Templates → Correo enviado a la víctima
- Landing Pages → Página web ilegítima
- Sending Profiles → Servidor de correos
- Campaigns → Campañas de phishing

SECCIÓN II

Evilginx2



SECCIÓN II

Evilginx2

- Config → Configuración general de la IP y el dominio
- Phishlet → Archivos de configuración en texto plano
- Lures → Creación de páginas webs ilegítimas
- Sessions → Sesiones capturadas

SECCIÓN III

Contramedidas

- Comprobar los dominios y los subdominios
- No usar SMS como 2º factor de autenticación
- Utilizar dispositivos de autenticación universal (U2F)
- Usar el sentido común

SECCIÓN III

Contramedidas

- Comprobar las cabeceras:

```
Return-Path: <alainjre@gmail.com>
Received: from kali [redacted]
        by smtp.gmail.com with ESMTPSA id [redacted]
        for <alainjre@gmail.com>
        (version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256 bits=128/128);
        Wed, 27 Apr 2022 04:36:35 -0700 (PDT)
From: Google Security <alainjre@gmail.com>
X-Google-Original-From: "Google Security" <security@googIe.es>
Mime-Version: 1.0
Date: Wed, 27 Apr 2022 07:36:34 -0400
X-Mailer: gophish
Message-Id: <[redacted]@kali>
Subject: Alerta de seguridad
To: alain arsene <alainjre@gmail.com>
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: quoted-printable
```

SECCIÓN IV

¿Has sido víctima de un phishing?

- Informar a la entidad afectada
- Modificar los datos de acceso
- Recopilar toda la información posible: e-mails, documentos, etc.
- Denunciar

Universidad de Alcalá

SIE

SECCIÓN IV

¿Has sido víctima de un phishing?

Contactar con:

- La entidad afectada
- Las Fuerzas y Cuerpos de Seguridad del Estado (FFCCSE)
- Servicios online: Instituto Nacional de Ciberseguridad (INCIBE)

SECCIÓN V

Referencias

Gracias por vuestra atención

Universidad de Alcalá

SIE

[LinkedIn] linkedin.com/in/alain-arsene