Phishing

El **Phishing** consiste en enviar un correo electrónico con intenciones maliciosas, para obligar a los destinatarios a revelar información, descargar archivos maliciosos, transferir dinero, revelar información o completar una acción que normalmente no harían, explotando el factor humano a través de técnicas de ingeniería social.

Aunque el phishing se basa principalmente en el correo electrónico, existen otros ataques que utilizan llamadas de voz (**Vishing**) y SMS o mensajes de texto (**SMiShing**).

El phishing es la ruta principal de compromiso muy por encima de los demás métodos, como la explotación de vulnerabilidades; y cuanto más sofisticadas sean las tecnologías empleadas para proteger la información, más centrados estarán los ataques en explotar las debilidades del personal.

Estructura de un email

Los emails están formados por una cabecera (*header*) y un cuerpo (*body*)

Cabecera (Header)

Se trata de un conjunto de líneas con información sobre el transporte del mensaje, como la dirección del remitente y del destinatario, las marcas temporales que indican cuándo el mensaje fue procesado por servidores intermedios, el asunto del mensaje, ... Esta información aparece recogida en campos (*header fields*):

- **From**: indica la dirección del remitente.
- **To**: indica la dirección del destinatario.
- **Date**: indica la fecha de envío del email.

A mayores es posible encontrar otros campos opcionales como:

- **Subject**: indica el asunto del email.
- **Reply-To**: indica la dirección a la que enviar la respuesta.
- **Received**: indica información sobre servidores intermedios y la fecha en la que procesaron el email.
- **message-ID**: identificador único del email.
- **Cabeceras X-Headers**: cabeceras personalizables que proporcionan información adicional como X-SPAM-STATUS, X-Originating-IP, X-Mailer, ...

```
Received: from PAXP194MB1470.EURP194.PROD.OUTLOOK.COM (2603:10a6:102:1a0::8)
 by AM0P194MB0322.EURP194.PROD.OUTLOOK.COM with HTTPS; Wed, 12 Jan 2022
 23:03:51 +0000
Received: from DM3PR03CA0015.namprd03.prod.outlook.com (2603:10b6:0:50::25) by
 PAXP194MB1470.EURP194.PROD.OUTLOOK.COM (2603:10a6:102:1a0::8) with Microsoft
 SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.4888.10; Wed, 12 Jan 2022 23:03:50 +0000
Received: from X-Sender-IP: 149.72.46.179DM6NAM11FT056.eop-nam11.prod.protection.outlook.com
 (2603:10b6:0:50:cafe::d1) by DM3PR03CA0015.outlook.office365.com
 (2603:10b6:0:50::25) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.4888.9 via Frontend
 Transport; Wed, 12 Jan 2022 23:03:50 +0000
Authentication-Results: spf=pass (sender IP is 149.72.46.179)
 smtp.mailfrom=em9899.maxmind.com; dkim=pass (signature was verified)
 header.d=maxmind.com;dmarc=pass action=none
 header.from=maxmind.com;compauth=pass reason=100
Received-SPF:    PX-Sender-IP:    149.72.46.179ass    (protection.outlook.com:    domain    of
em9899.maxmind.com
 designates 149.72.46.179 as permitted sender)
```

```
 receiver=protection.outlook.com; client-ip=149.72.46.179;
 helo=o1.ptr9166.maxmind.com;
Received: from o1.ptr9166.maxmind.com (149.72.46.179) by
 DM6NAM11FT056.mail.protection.outlook.com (10.13.173.99) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.4888.9 via Frontend Transport; Wed, 12 Jan 2022 23:03:49 +0000
Received: from queue-processor-us-east-1.localdomain (unknown)
      by geopod-ismtpd-6-3 (SG) with ESMTP id _xuZsWigTPK9JDePyM-0ZQ
      for <subnetting@hotmail.com>; Wed, 12 Jan 202`2 23:03:49.128 +0000 (UTC)
Received: from localhost (localhost.localdomain [127.0.0.1])
      by queue-processor-us-east-1.localdomain (Postfix) with UTF8SMTP id 10CE113B04A
      for <subnetting@hotmail.com>; Wed, 12 Jan 2022 23:03:49 +0000 (UTC)
Date: Wed, 12 Jan 2022 23:03:49 +0000 (UTC)
From: support@maxmind.com
Subject: Welcome To MaxMind
X-Sender: mm_website
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html; charset=us-ascii
Message-Id: <20220112230349.10CE113B04A@queue-processor-us-east-1.localdomain>
To: subnetting@hotmail.com
X-Entity-ID: dypfiwxJY3nRwSXslc4zjg==
X-Sender-IP: 149.72.46.179
Return-Path: bounces+22608499-b268-subnetting=hotmail.com@em9899.maxmind.com
```

Cuerpo (Body)

El cuerpo del mensaje contiene la información bien en texto plano o formateado en html.

```
Content-Type: text/html; charset=us-ascii
<!DOCTYPE html><html><head>
<meta http-equiv=3D"Type" content=3D"text/html; charset=3Dus-ascii"=
>
    <title>Welcome To MaxMind</title>
  </head>
  <body>
    <p>Dear sub,</p>
   =20
    <p>Thank you for creating an account.</p>
...
```

Es habitual que en los emails aparezca contenido codificado en base64 si tiene ficheros adjuntos como imágenes, pdf, ..., o usa muchas etiquetas html. En el siguiente ejemplo las cabeceras indican que el documento adjunto es un pdf codificado en base64:

- Content-Type: application/pdf
- Content-Disposition: attachment
- Content-Transfer-Encoding: base64

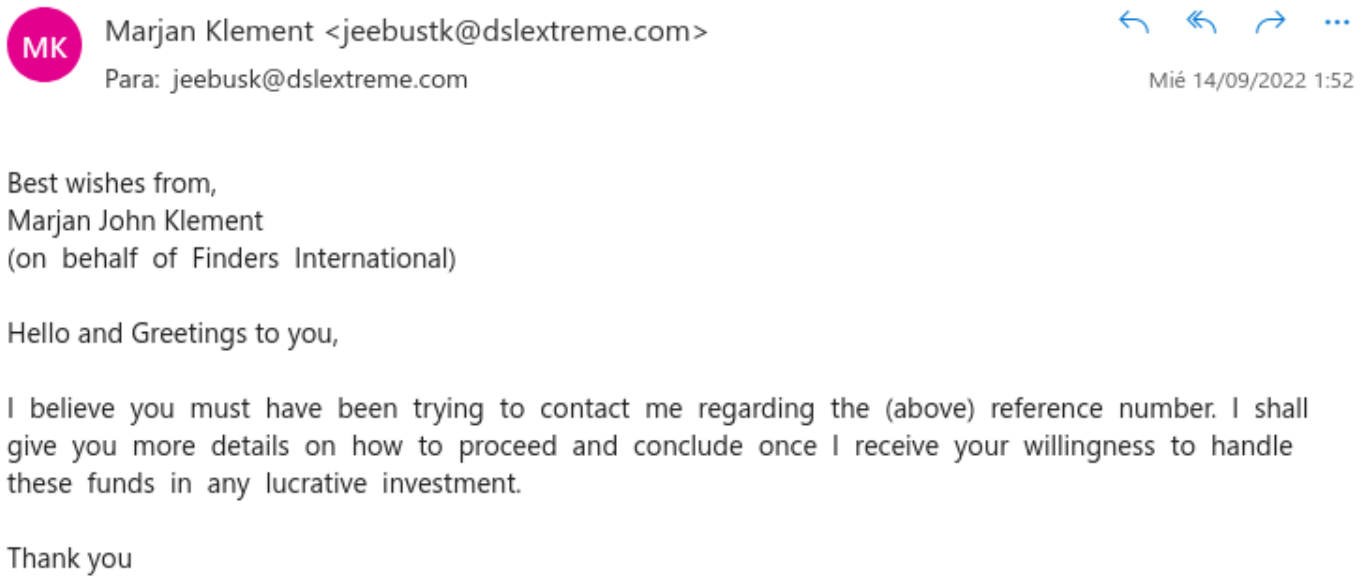
```
----==_mimepart_61b86519468fa_72842b081a96993c54771
Content-Type: application/pdf;
 filename=PentesterLab_PRO_Invoice.pdf
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
 filename=PentesterLab_PRO_Invoice.pdf
Content-ID: <61b8651948966_72842b081a96993c550b2@ip-172-31-60-188.ec2.internal.mail>

JVBERi0xLjQKJf////8KMSAwIG9iago8PCAvQ3JlYXRvciA8ZmVmZjAwNTAwMDcyMDA2MTAwNzcw
MDZlPgovUHJvZHVjZXIgPGZlZmYwMDUwMDA3MjAwNjEwMDc3MDA2ZT4KPj4KZW5kb2JqCjIgMCBv
YmoKPDwgL1R5cGUgL0NhdGFsb2cKL1BhZ2VzIDMgMCBSCj4+IGVuZG9iagozIDAgb2JqCjw8IC9U
...
```

Tipos de phishing

Los emails usados en phishing pueden clasificarse principalmente como:

- **Reconocimiento**: el objetivo de estos emails es obtener una respuesta del destinatario para saber si la cuenta de correo está en uso. Se usan técnicas como:
  - mensajes con texto al azar que en caso de recibir un mensaje de error del servidor de correo, permite determinar el estado del buzón de correo.
  - mensajes con algún tipo de técnica de ingeniería social que provoque la respuesta del destinatario.
  - mensajes con *tracking pixels*. [1]



- **Recopilación de credenciales** (***credential harvester***): mensajes que buscan que el destinatario proporcione sus credenciales. Habitualmente se encuentran:
  - mensajes formateados para parecer que proceden de compañías legítimas como Amazon, Netflix, Outlook, ..., con enlaces o botones que conducen a portales falsos.
  - mensajes que llevan a sitios web maliciosos que simulan portales de autenticación de la organización de la víctima.phishing

1 Tracking pixels: típicamente son imágenes no visibles pero que se cargan al leer el mensaje permitiendo al adversario saber que el mensaje fue abierto, indicando que la cuenta de email está activa. El cargar la imagen le puede proporcionar al adversario información adicional como sistema operativo usado, versión del cliente de correo o navegador web usado para abrir el email, fecha en la que se abrió el mensaje, dirección IP, ...

- **Spear phishing**: se trata de un mensaje phishing especialmente preparado para la víctima, en base a información previamente recopilada por el adversario. Recopilando y analizando información sobre el trabajo del la víctima, gustos, hobbies, familiares, sitios web que visita habitualmente, ..., el atacante diseña

un email más convincente y con mayores probabilidades de que la víctima ejecute la acción deseada.

- **Whaling**: similar al spear phishing, pero dirigido específicamente a personas de alto nivel o C-Level (CEO, CFO, etc.).
- **BEC (Business Email Compromise)**: se vigila a la empresa objetivo para saber con que empresas y proveedores trabaja. Una vez localizada una relación entre el objetivo y un proveedor, se comprometerá una cuenta de correo electrónico de un empleado de alto nivel o se suplantará la dirección para que parezca legítima; y se ordenará a los empleados pertinentes que transfieran dinero a una cuenta bancaria diferente que esté bajo control del actor malicioso.

Técnicas

En los mensajes de phishing es habitual encontrar algunas de las siguientes técnicas:

- **Spear Phishing**.
- **Tracking pixels.**
- **Email spoofing**: se falsifica el nombre y/o la dirección del remitente.
- **Suplantación**: el adversario envía el email haciéndose pasar por otra persona como un amigo, compañero de trabajo o alguien en un nivel superior en la jerarquía de la organización.
- **Error tipográfico** (***Typo squatting***): se trata de suplantar un nombre de dominio usando un error tipográfico. Por ejemplo, en vez de iessanclemente.net: iesanclemente.net, iessancllemente.net, ...
- **Palabras Homógrafas**: se basa en que caracteres que son semejantes en apariencia para el ser humano, son considerados diferentes por los ordenadores (distintos caracters unicode); por ejemplo, la 'o' Latina y la 'o' griega. Los adversarios 'abusan' de los IDN (Internationalized Domain Name) que permiten usar nombres de dominio con caracteres no latinos (cirílico, chino, árabe, ...) creando nombres de dominio que simulan ser otros gracias a su parecido.
- **Estilo HTML**: el cuerpo del mensaje trata de imitar la apariencia de mensajes legítimos tratando de engañar a las víctimas.
- **Adjuntos**: en las campañas de phishing se suelen adjuntar:
  - archivos maliciosos como documentos de Office con macros maliciosas.
  - archivos no maliciosos con enlaces maliciosos; por ejemplo, documentos pdf con enlaces a sitios web o ficheros maliciosos.
  - archivos no maliciosos usados con técnicas de ingeniería social; por ejemplo, facturas o formularios de recogida de datos.

De DHL Servicio.

Asunto **Importante: Su paquete está esperando la entrega. Confirme el pago (1,99 EUR)**

A

Estimado cliente,

Su paquete está esperando la entrega. Confirme el pago (1,99 EUR) utilizando el siguiente enlace. La revisión en línea debe llevarse a cabo dentro de los próximos 14 días antes del vencimiento:

Sigue mi paquete

Condiciones de entrega complicadas debido a la situación excepcional del Covid-19
Hay dificultades de entrega en esta comunidad.
Sin embargo, estamos trabajando para entregarle el pedido lo antes posible. Gracias por tu paciencia

Saludos,
El equipo de DHL

- **Servicios legítimos**: tratando de superar medidas de seguridad automatizadas y/o la confianza del usuario, hay adversarios que usan servicios legítimos ampliamente usados como:
  - servicios de email: usan direcciones de servicios como Gmail o Outlook, ampliamente usadas por la gente y normalmente no bloqueadas por los filtros de correo electrónico.
  - servicios de almacenamiento: como Dropbox o Google Drive donde se alojan ficheros maliciosos o se crean documentos con enlaces a sitios web o archivos maliciosos.
- **Enlaces**: usados por el adversario para dirigir a la víctima a sitios web para robo de credenciales o descarga de archivos maliciosos.

```
<p>Tuvimos que suspender tu cuenta temporaImente, Detectamos un comportamiento irregular en tus operaciones. </p>

<p><strong>Para mas informacion y reactivar tu cuenta ingresa en: </strong><a href="http://www.wellnessprofi.cz/www.banregio.com1.php">https://banregio.com/activacion#</a></p>
```

Tuvimos que suspender tu cuenta temporalmente, Detectamos un comportamiento irregular en tus operaciones.

Para mas informacion y reactivar tu cuenta ingresa en: https://banregio.com/activacion#

- **Acortadores de URL** (**URL shorteners**): transforman URLs largas en URLs cortas. La URL corta generada redirige a los visitantes al destino real de la URL a través de una redirección http. Este tipo de URL cortas ocultan el destino real final.