IES Zaidín-Vergeles

Correos electrónicos.

25 de mayo de 2021

Tabla de contenidos

CAPÍTULO 1

Introducción

Los protocolos primarios y más extendidos, utilizados en el sistema de correo electrónico carecen caracteristicas de seguridad para: a) privacidad del remitente, b) autenticación del remitente, c) integridad del mensaje de correo electrónico, d) no repudio del remitente, y e-mail. Estos lapsos de seguridad permiten falsificar el correo electrónico forjando sus encabezados o enviándolo de forma anónima.

Desde el punto de vista del análisis forense se pueden distinguir dos clasificaciones diferentes para is correos electrónicos:

1. Enviados o recibidos: A nivel forense existe gran diferencia a la hora de poder certificar la autenticidad y la procedencia de los correos electrónicos enviados frente a los correos recibidos. Por un lado, sabemos que los correos electrónicos recibidos pueden permanecer almacenados en las servidores de correo una vez descargados, facilitándonos su proceso de autentificación. Incluso el caso de que estos servidores estén configurados para borrar los correos tras ser descargados se podrá realizar un análisis de las cabeceras de estos correos. Este análisis nos permitirá establecer una azabilidad de los servidores de correo por los que éste ha pasado, desde el momento en el que fue enviado hasta el servidor final de entrega.
2. La segunda clasificación depende del tipo de servidor donde se almacenan los correos electrónicos:
    a) Servidores de correo locales: son servidores que han podido ser accesibles de forma fisica por lo que se recomienda realizar un análisis forense para comprobar que no hayan sido manipulados intencionadamente.
    b) Servidores de correo de terceras empresas: En este caso podriamos fiarnos de la autenticidad de la información de los servidores en el caso que estas empresas cumplan con las regulaciones y estándares nacionales e internacionales en materia de seguridad y en el tratamiento de la información (Ley LOPD y Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico).
    c) Servidores de correo en la nube (GMAIL, YAHOO...): en estos casos no será posible acceder directamente a los servidores para extraer la información, por

lo que tendremos que valernos de herramientas:

a) Las que permitan obtener certificados con sello de tiempo de correos electrónicos como eGarante o Safe Stamper.

b) Aquellos proveedores que permiten descargar una copia de contenido de la cuenta, por ejemplo Google a través de la siguiente url: https://myaccount.google.com/privacy

c) Si el caso es un Exchange en cualquiera de sus configuraciones, nos podemos valer de la Power Shell para realizar esta tarea.

CAPÍTULO 2

Técnicas para la investigación de correo electrónico

El análisis forense del correo electrónico se refiere al estudio de la fuente y el contenido del correo electrónico como evidencia para identificar el remitente y destinatario real de un mensaje, datos, tiempo de transmisión, registro detallado de la transacción de correo electrónico, intención del remitente, etc. El análisis forense de un mensaje de correo electrónico tiene como objetivo descubrir la historia de un mensaje y la identidad de todas las entidades involucradas. El análisis de correo electrónico comienza en el buzón del destinatario que contiene el mensaje de correo electrónico. El mensaje se analiza para determinar la fuente (origen y autor). El análisis implica la investigación tanto de la información de control (encabezado) como del cuerpo del mensaje. Las diferentes técnicas que se implementan para realizar una investigación de correo electrónico eficaz y transparente son las siguientes:

1. Análisis de encabezados, cuerpo y metadatos del correo electrónico

El análisis de encabezado se realiza con el fin de extraer la información relativa al remitente del correo y también la ruta a través de la cual se ha transmitido el correo electrónico. Normalmente, los metadatos de los correos electrónicos se almacenan en los encabezados. A veces, estos encabezados pueden ser manipulados con el fin de ocultar la verdadera identidad del remitente.

2. Extracción de correos del servidor

La investigación del servidor es útil cuando los correos electrónicos que residen en los extremos del remitente y del receptor han sido eliminados permanentemente. Dado que los servidores mantienen un registro de los correos electrónicos enviados y recibidos, la investigación del registro generará todos los correos electrónicos eliminados. Además, los registros pueden dar la información de la fuente donde los correos se han generado. La investigación del servidor no significa que se puedan extraer todos los correos electrónicos eliminados. Esto se debe a que después de un cierto período de retención, los correos electrónicos se eliminan permanentemente de un servidor.

3. Investigación de Fuentes de Red

Esta investigación se elige, cuando los registros del servidor no logran generar la información requerida. Además, si los Proveedores de Servicios de Internet no dan acceso al servidor, se elige la investigación de las fuentes de red. Los registros generados por los IDS, concentradores, enrutadores, firewalls, etc. proporcionan información sobre el origen del mensaje de correo electrónico.

4. Tácticas de cebo

Es el proceso para rastrear la dirección IP del remitente de un correo en particular bajo investigación. En esta técnica, se envía un correo que contiene una etiqueta http: «<S It; img src» (siendo src la ruta a una imagen en un servidor bajo nuestro control) a la dirección de correo desde la que se ha recibido el correo. Cuando se abre el correo, un registro que contiene la dirección IP del destinatario es capturado por el servidor de que aloja la imagen y se rastrea al destinatario. En caso de que el destinatario esté utilizando un servidor proxy, la dirección del servidor proxy se registra.

5. Comparación de datos

Tanto el análisis de toda la información obtenida como su correlación buscando posibles datos incoherentes (fechas, direcciones, destinatarios, etc) pueden clarificar la autenticidad o no de los correos electrónicos analizados.

Algunas aplicaciones de correo electrónico almacenan un back up de emails. Para abrir este tipo de ficheros, normalmente es necesaria la aplicación nativa. Si se dispone de esta información también se puede utilizar para hacer comparaciones con los correos originales.

CAPÍTULO 3

Análisis de cabeceras

Cuando se envía un correo electrónico, el mensaje se enruta de servidor a servidor hasta llegar al servidor de correo electrónico del receptor. El mensaje se envía al servidor del correo electrónico MTA (Mail Transport Agent) que tiene la tarea de transportarlos hacia el MTA del destinatario. En Internet, los MTA se comunican entre si usando el protocolo SMTP.

Posteriormente, el MTA del destinatario entrega el correo electrónico al servidor del correo entrante MDA (Mail Delivery Agent) que almacena el correo electrónico a la espera de que el usuario lo acepte. Existen dos protocolos principales utilizados para recuperar I correo electrónico de un MDA:

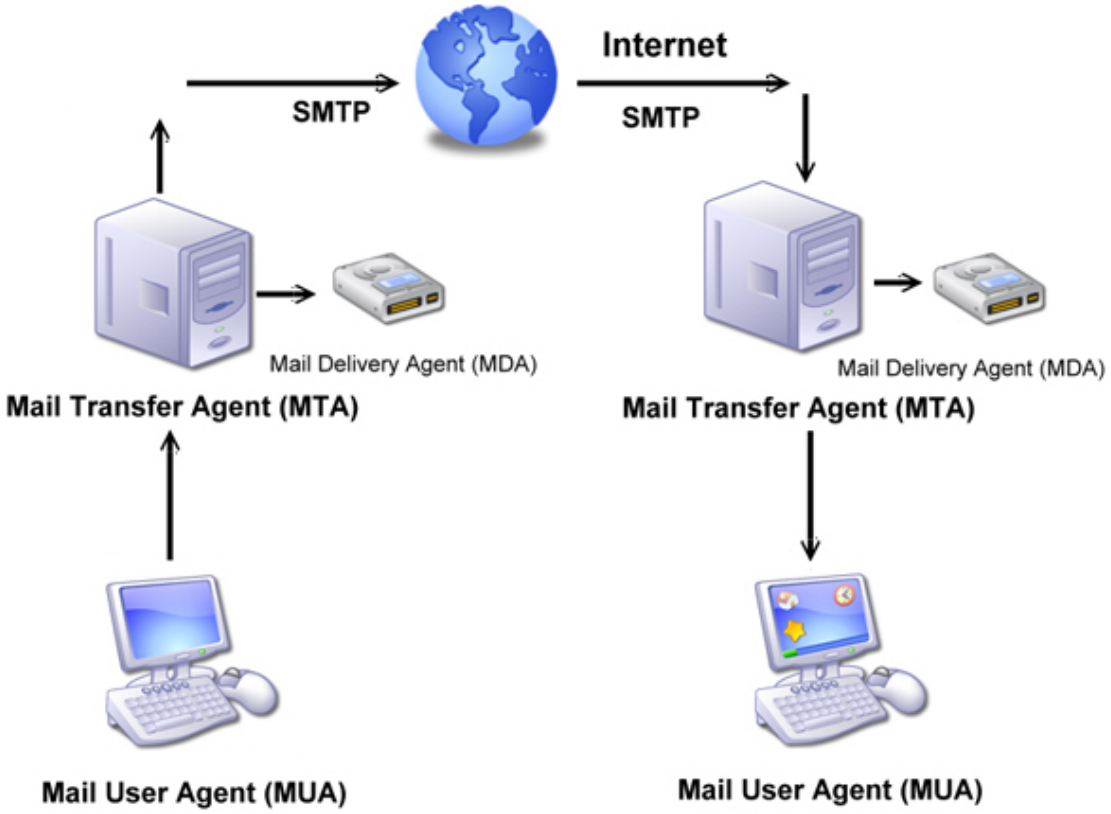
a) **POP3 (Post Office Protocol)**, se usa para recuperar el correo electrónico y, en algunos casos, dejar una copia en el servidor.

b) **IMAP (Internet Message Access Protocol)**, se usa para coordinar el estado de los correos electrónicos (leído, eliminado, movido) a través de múltiples clientes de correo electrónico. Con IMAP, se guarda una copia de cada mensaje en el servidor, de manera que esta tarea de sincronización se pueda completar.

Por esta razón, los servidores de correo entrante se llaman servidores POP o servidores IMAP, según el protocolo usado.

Por supuesto, el MDA está protegido por un nombre de usuario llamado registro y una contraseña.

La obtención del correo se logra a través de un programa de software llamado MUA (Mail User Agent). Cuando el MUA es un programa instalado en el sistema del usuario, se Hama cliente de correo electronico (Thunderbird, Outllok, Eudora, Incredimail o Lotus Notes)



Las cabeceras de correo electrónico determinan a dónde se envía un mensaje y registran la ruta específica que sigue el correo a medida que pasa por cada servidor a través de la red, aunque en la mayoría de los clientes de correo esta información permanece oculta.

Existen herramientas que facilitan la lectura de las cabeceras de los mensajes como, por ejemplo, https://toolbox.googleapps.com/apps/messageheader/.

Si se desea leer la cabecera de un mensaje manualmente, se debe seguir la ruta del mensaje en orden cronológico desde el final de la cabecera hasta el principio.

A continuación, se describen algunos de los campos más importantes de un encabezado:

a) El encabezado X-Apparently-To es relevante cuando se ha enviado el correo como un BCC o para los destinatarios de alguna lista de correo. Este campo en la mayoría de los casos contiene la dirección como en el campo A. Pero si el correo se ha enviado a un destinatario del BCC o una lista de correo, X-Apparently-To es diferente del campo TO. Algunos pueden mostrar el TO mientras que otros no pueden mostrarlo. Así, X-Apparently-To mostrará siempre en el correo electrónico la dirección del destinatario, independientemente de si el correo se ha enviado utilizando TO, BCC, CC direcciones o mediante el uso de alguna lista de correo.

b) El encabezado Return-Path es la dirección de correo electrónico del buzón especificado por el remitente en el comando MailFrom. Esta dirección también puede ser falsificada, no es posible determinar autenticidad del encabezado Return-Path sólo a través del análisis de encabezado.

c) El valor del encabezado Received-SPF especifica si el correo proviene de un dominio que tiene un registro SPF o aún no es un emisor autorizado designado.

d) La puntuación de spam calculada por el software de filtrado de spam del servidor receptor o MUA está contenido en el campo X-Spam-Ratio. Si esta relación exce-

de determinado umbral predefinido, el correo electrónico serán clasificados como spam. Diferentes servidores receptores y MUA's utilizados diferentes campos X-Header para indicar la puntuación de spam y la decisión de clasificación tomada con respecto al mensaje actual. Éstos incluyen X-Spam-Flag, X-SpamChecker-Version, X-Spam-Level, X-Spam-Status, etc.

e) X-Originating-IP especifica la dirección IP del último MTA del SMTP de envio Server, que ha entregado el e-mail al servidor de foo@bar.com. Esta dirección también está contenida en el campo de encabezado Recibido.

f) El encabezado X-Sieve especifica el nombre y la versión del sistema de filtrado de mensajes. Esta se refiere al lenguaje de secuencias de comandos utilizado para especificar las condiciones para el filtrado de mensajes y manejo.

g) El encabezado X-Spam-Charsets especifica el conjunto de caracteres utilizado para filtrar mensajes.

h) La dirección X-Resolved-To es la dirección de correo electrónico del buzón al que se ha enviado el correo ha sido entregado por MDA del servidor de «bar». En la mayoría de los casos, es lo mismo que el campo XDelivered-To.

i) X-Delivered-To es la dirección del buzón al que este mail ha sido enviado.

j) El encabezado X-Mail-From especifica la dirección de e-mail del buzón especificado por el remitente.

A continuación, se muestra un ejemplo de cabecera de un mensaje de correo electrónico que empleado1@proveedorcorreo.com ha enviado a empleado2@gmail.com:

```
Delivered-To: empleado2@gmail.com

Received: by 10.36.81.3 with SMTP id e3cs239nzb; Tue, 29 Mar␣
↪2017 15:11:47 -0800 (PST)

Return-Path:

Received: from correo.proveedorcorreo.com (correo.
↪proveedorcorreo.com [111.111.11.111]) by mx.gmail.com with␣
↪SMTP id h19si826631rnb.2017.03.29.15.11.46; Tue, 29 Mar 2017␣
↪15:11:47 -0800 (PST)

Message-ID: <20050329231145.62086.correo@correo.proveedorcorreo.
↪com>

Received: from [11.11.111.111] by correo.proveedorcorreo.com␣
↪via HTTP; Tue, 29 Mar 2017 15:11:45 PST

Date: Tue, 29 Mar 2017 15:11:45 -0800 (PST)

From: Señor Empleado 1

Subject: Hola

To: Señor Empleado 2
```

En el ejemplo, las cabeceras se añaden al mensaje tres veces:

1. Cuando el señor Empleado 1 redacta el mensaje:

```
Date: Tue, 29 Mar 2017 15:11:45 -0800 (PST) From: Señor␣
↪Empleado 1

Subject: Hola

To: Señor Empleado 2
```

2. Cuando el mensaje se envía a través de los servidores del proveedor de correo electrónico del señor Empleado 1, correo.proveedorcorreo.com:

```
Message-ID: <20050329231145.62086.correo@correo.proveedorcorreo.
↪com>

Received: from [11.11.111.111] by correo.proveedorcorreo.com␣
↪via HTTP; Tue, 29 Mar 2017 15:11:45 PST
```

3. Cuando el mensaje se transfiere desde el proveedor de correo electrónico del señor Empleado 1 a la dirección de Gmail del señor Empleado 2.

```
Delivered-To: Empleado2@gmail.com

Received: by 10.36.81.3 with SMTP id e3cs239nzb; Tue, 29 Mar␣
↪2017 15:11:47 -0800 (PST) Return-Path:␣
↪Empleado1@proveedorcorreo.com

Received: from correo.proveedorcorreo.com (correo.
↪proveedorcorreo.com [111.111.11.111D) by mx.gmail.com with␣
↪SMTP id h19si82663 1rnb; Tue, 29 Mar 2017 15:11:47 -0800 (PST)
```

A continuación, se incluye una descripción de cada sección de la cabecera de un correo electrónico:

```
Delivered-To: Empleado2@gmail.com
```

La dirección de correo electrónico a la que se enviará el mensaje.

```
Received: by 10.36.81.3 with SMTP id e3cs239nzb;

Tue, 29 Mar 2017 15:11:47 -0800 (PST)
```

La hora a la que se recibió el mensaje en los servidores de Gmail.

```
Return-Path:
```

La dirección desde la que se envió el mensaje.

```
Received: from correo.proveedorcorreo.com

(correo proveedorcorreo.com [111.111.11.111])
```

(continué en la próxima página)

(proviene de la página anterior)

```
by mx.gmail.com with SMTP id h19si82663 Irnb.2017.03.29.15.11.
↪46;

Tue, 29 Mar 2017 15:11:47 -0800 (PST)
```

Un servidor de Gmail recibió el mensaje desde correo.servidorcorreo.com el 29 de marzo de 2017 a las 15:00 aproximadamente.

```
Message-ID: 20050329231145.62086.correo@correo.proveedorcorreo.
↪com
```

Un numero único asignado por correo proveedorcorreo.com para identificar el mensaje.

```
Tue, 29 Mar 2017 15:11:45 PST

Received: from [11.11.111.1111 by correo proveedorcorreo.com␣
↪via HTTP:
```

El señor Empleado 1 utilizó un programa de correo electrónico para escribir el mensaje, que se recibió posteriormente en los servidores de correo electrónico de correo.proveedorcorreo.com.

```
Date: Tue, 29 Mar 2017 15:11:45 -0800 (PST)

From: Señor Empleado 1

Subject: Hola

To: Señor Empleado 2
```

La fecha, el remitente, el asunto y el destino: el señor Empleado 1 incluyó esta información cuando redactó el correo electrónico, a excepción de la fecha.