

# **Análisis de ataques a un sistema de correo electrónico por medio de mensajes que incluyen contenido alterado de forma maliciosa**

## **POR**

Egdares Futch Higueros  
Catedrático UNITEC  
efutch@gmail.com

## **RESUMEN**

La investigación se realiza con el propósito de evaluar la vulnerabilidad de los sistemas de comunicación por correo electrónico de Internet, para determinar la facilidad de explotación de un ataque por medio de mensajes que incluyen contenido creado con fines maliciosos, con el objeto de diseñar y preparar medidas de mitigación de riesgos y educación de los usuarios.

Se describe el análisis realizado sobre la capacidad de crear mensajes de correo electrónico de Internet, que incluyen código HTML diseñado maliciosamente para hacer creer al receptor que proviene de una entidad o persona de confianza, y hacerle creer que está interactuando con ella, sin que sea detectado por el sistema de correo electrónico o paquetería de filtrado y seguridad, como antivirus y antispam.

Se considera como un ataque de ingeniería social (“social engineering”) hacia los usuarios de los sistemas de correo electrónico, que aprovecha de debilidades en los paquetes de correo electrónico (“Mail User Agents – MUAs”) y sistemas de filtrado de correo y virus disponibles comercialmente. El término utilizado comúnmente para este tipo de ataques se denomina *phishing*.

La prueba de concepto se realiza sobre software disponible comercialmente y de uso generalizado entre las personas que se comunican a través de correo electrónico de Internet.

## INTRODUCCIÓN

De acuerdo a Tomlinson, la comunicación por correo electrónico tal y como se conoce actualmente, fue derivado de los primeros experimentos de comunicación en la red ARPANet en 1971, y fue transmitido entre dos computadores conectados lado a lado en los laboratorios de Bolt, Beranek & Newman, contratistas del Departamento de la Defensa de Estados Unidos. Esta transmisión hizo uso del famoso signo de arroba (@), que en inglés refleja el concepto de “lugar” (*at*) para distinguir una comunicación local (sin signo de @), de una comunicación remota (con signo de @).

La mayoría de los primeros protocolos de comunicaciones fueron diseñados para ser usados en redes de acceso limitado: solamente aquellas entidades que formaban parte de un club muy selecto y tecnológicamente avanzado, eran quienes formaban parte de esos sistemas de comunicación. En los primeros años del Internet fueron las universidades, el Departamento de Defensa de Estados Unidos y algunos laboratorios de investigación quienes intercambiaban información.

Por lo anterior, Anderson (2001) indica que los primeros protocolos como Telnet, FTP, DNS y SMTP se ejecutaban en un entorno de servidores autónomos, sin consideraciones relevantes de seguridad, ya que asumían un entorno confiable, basado en estaciones de trabajo interconectadas por medio de redes locales con administración distribuida, pero dentro de algunas pocas organizaciones autónomas.

De las condiciones que se asumieron inicialmente para el funcionamiento del Internet, muy pocas son aplicables todavía, incluso de forma parcial. Sin embargo, la gran mayoría ya no son funcionales, debido a que el Internet ahora consiste en millones de computadoras conectadas, a millones de redes locales y de área amplia

## DESARROLLO

### **A) Ingeniería social automatizada: mensajes de correo electrónico maliciosos**

El concepto de Ingeniería Social es aplicado a aquellas técnicas de extracción o manipulación de información de terceros a través de interacciones personales, que se aprovechan de relaciones de confianza.

Como un ejemplo de Ingeniería Social, basado en el expuesto en Crume (2000), puede plantearse el siguiente: un adversario malicioso quiere infiltrarse en la computadora personal del gerente general de una compañía. Para lograrlo, llama al PBX de la empresa y pide hablar con el gerente. Cuando su secretaria le responde, en vez de comunicarse con la persona el atacante le solicita que le traslade al departamento de Sistemas.

El departamento de Sistemas recibe la llamada de la secretaria del gerente general: “Hola, ¿que tal? Le paso una llamada”. Esto ya establece una relación de confianza que la persona externa puede explotar: “Buenos días, habla el Gerente. Necesito que me cambien mi clave en el sistema por favor, porque tengo que entregar las proyecciones de noviembre”. En un entorno corporativo normal, esta solicitud será

atendida rápidamente, por los requerimientos de negocios, logrando que la persona que llamó obtenga una cuenta de sistema. Este ejemplo tiene muchas simplificaciones, y solamente sirve para ilustrar el concepto.

En el caso de esta investigación, se estudia cómo lograr explotar una relación de confianza en forma automatizada, por medio de mensajes de correo electrónico que suplantan ser de una entidad de confianza, operando en conjunto con un sitio Web falso, copiado del servidor original en otro equipo, controlado por un grupo malicioso.

La práctica de atraer personas a sitios maliciosos por medio de ingeniería social automatizada en mensajes de correo electrónico se ha llamado *phishing*, término que deriva de la palabra *fishing*, que significa pescar en inglés, sustituyendo la F por PH, según la usanza de los piratas informáticos.

## **B) Prueba de concepto**

### **B.1) Instalación del ambiente de pruebas**

El ambiente de pruebas para verificar la factibilidad de insertar código malicioso en un mensaje de correo electrónico requiere de dos componentes: un servidor de páginas Web falsas (*servidor phish*) que suplantaría al verdadero sitio que se está atacando, y al que el mensaje *phish* trataría de dirigir al usuario para capturar su palabra clave; el segundo componente es un cliente de correo que pudiera usarse para componer un mensaje de correo *phish* e insertarle código incorrecto.

El servidor *phish* fue instalado con la siguiente configuración:

- Sistema operativo Red Hat Advanced Server 4 (Linux), corriendo dentro de una máquina virtual VMware Workstation 4.5.
- Software Apache HTTPD, como servidor de Web.
- Software Dovecot, como servidor de IMAP y POP3
- Software Sendmail, como servidor de SMTP

Este servidor estará suplantado al sitio Web original <http://www.bancovirtual.hn>.

Los clientes de correo que serán probados son:

- Outlook Express, como cliente de correo *standalone*.
- Squirrelmail, como cliente de correo Web.
- GMail, como servicio público de correo Web.
- Yahoo! Mail, como servicio público de correo Web.

Los servicios de correo Web dependen de un componente adicional de seguridad en el navegador de Internet, quien será el que deberá interpretar el código HTML que se reciba.

### **B.2) Copia y modificación del sitio Web a suplantar (servidor phish)**

La copia que se hizo fue de los archivos y programas para manejar un sitio Web de banca en línea, que una institución local tenía disponibles públicamente. Esto es posible hacerlo con cualquier herramienta básica de manejo de sitios Web.

En este caso, se hizo por medio del software *wget* directamente desde el servidor *phish* de pruebas; se hizo una copia del sitio Web de una institución financiera en el servidor local. Este software cuenta con opciones especiales que le permiten crear una copia fiel de un sitio remoto, de tal manera que las referencias a servidores externos sean cambiadas de forma tal que se conviertan en referencias locales.

Al haber hecho la copia del sitio, se eliminaron las referencias al nombre de la institución original, y se modificó la página principal para ejecutar una acción diferente a la normal cuando el usuario ingresara su clave. Para el propósito de esta prueba, se hizo que desplegara un mensaje advirtiendo que era un sitio modificado junto con la clave recién ingresada. Es importante notar que en un sitio realmente alterado por piratas informáticos, en vez de mostrar un mensaje, se podría redirigir silenciosamente al sitio original sin que el usuario se diera cuenta.

El código original es:

```
// Fragmento del código original de la página copiada

1  function logear()
2  {
3    if(validarClaves()){
4      boolean=encriptar(document.logeo.Pv_clave.value);
5
6      rndsid = seed;
7      document.logeo.Pv_SID.value = rndsid;
8      document.logeo.submit();
9      clockProgress = setTimeout("setStatus();",1000);
10     deshabilitarCajaLogin();
11   }
12 }
13
14 <font color="#003366">Usuario&nbsp;&nbsp;&nbsp;</font></b></font></div> </td>
15 <td width=229>
16 <input type=text ID=login name="Pv_login" size=16 TITLE="Introduzca username.">
17 </td> </tr> <tr> <td width=167> <div align=right>
18 <font face="Arial, Helvetica, sans-serif" size=2><b>
19   <font   color="#003366">Clave&nbsp;&nbsp;&nbsp;</font></b></font></div>   </td>   <td
width=229>   20   <input   ID=clave   type=password   name="Pv_clave"   size=16
onkeypress="loginEnter();"
21 TITLE="Introduzca clave."> </td> </tr> <tr> <td colspan=2> <br> <div align=center>
22 
```

Este código muestra que cuando se ingresa la clave se llama a una función llamada *logear()* [líneas 1-12] escrita en Javascript directamente dentro de la página, que ejecuta un proceso de cifrado de la clave del usuario, la cual se recibe como un parámetro de dos formas: por medio de presionar la tecla ENTER [línea 20] o haciendo clic sobre un botón [línea 22].

Conociendo este código, es posible ahora interceptar la palabra clave del usuario, y se está en la capacidad de guardarla en el servidor *phish* para usarla posteriormente. Un servidor malicioso tiene algunas opciones ahora:

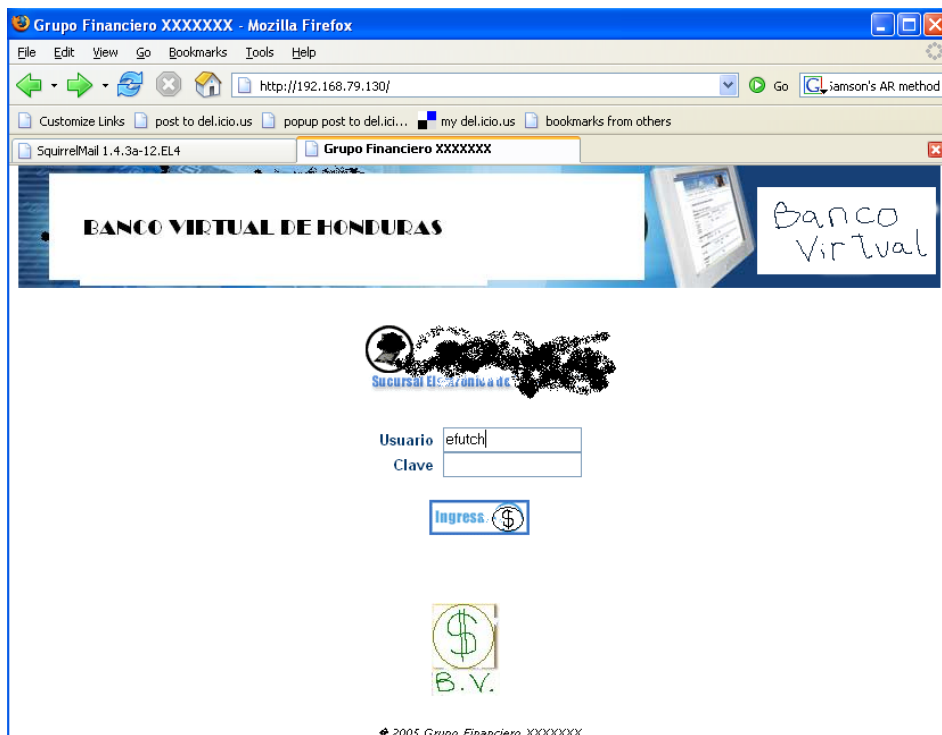
1. Guardar la clave del usuario, e informarle que ha habido un error. Luego de mostrar el error, se le puede redirigir al sitio original para que el usuario abandone el servidor *phish*.
2. Redirigir transparentemente al usuario que fue engañado, y colocar los valores de identificación y clave automáticamente para que la persona no se dé cuenta que tuvo una interacción con un servidor falso.

La modificación realizada al código fue la siguiente:

```
// Fragmento del código modificado
1  function logear()
2  {
3    document.write('<H1>ALERTA!!! USTED HA SIDO VICTIMA DE UN PHISH!!!<P>');
4    document.write('Su password es : ' + documento.logeo.Pv_clave.value);
5  }
```

Esta modificación intercepta el código de la función logear(), la cual en el código de la página original envía la clave en forma cifrada del usuario al servidor. Para la prueba de concepto, el código modificado intercepta la clave del usuario y se despliega en el navegador [líneas 1-5].

Al estar lista la modificación, el sitio Web se puso en línea en el servidor *phish* que se había preparado anteriormente, con una copia del sitio Web de Banco Virtual. A continuación se muestra la página de ingreso, contando con artes y textos modificados:



Es interesante notar que esta es la única modificación necesaria para capturar la clave del usuario, y está disponible en código públicamente accesible. Si un atacante modificara el servidor Web original y cambiara esta función, la institución sería víctima de una fuga de seguridad a gran escala.

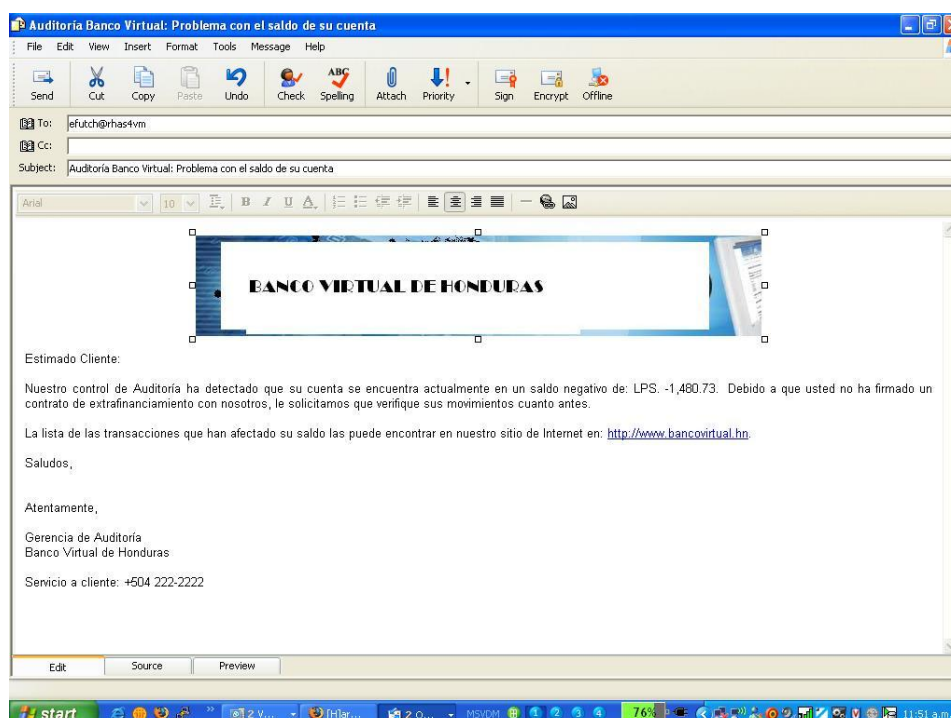
### B.3) Creación del mensaje con código malicioso (mensaje phish)

Al tener ya disponible el sitio Web alterado, se preparó un mensaje de correo electrónico que tuviera la apariencia de ser una comunicación oficial de la institución atacada.

Este mensaje debería contar con los siguientes elementos:

- Gráficos formales de la marca o sitio que se está atacando, para mejorar la apariencia oficial del mensaje.
- Enlaces directos y destacados visiblemente al sitio Web falso (sitio phish).
- Contenido que induzca un sentido de urgencia en el receptor para que se conecte lo antes posible al sitio que se está atacando.
- Código HTML y formateo que se aproveche de fallas en el software cliente de correo.

La combinación de los elementos anteriores provee el componente de ingeniería social deseado para atraer víctimas de esta técnica. Se compuso el mensaje en Outlook Express directamente, incorporando elementos gráficos del sitio Web, con contenido apropiado para un usuario de una institución financiera. El mensaje se muestra a continuación:



Con este texto, se pretende impresionar a la persona, y hacerle que se interese en hacer clic en el enlace al sitio *phish* de [www.bancovirtual.hn](http://www.bancovirtual.hn). Se incluyeron los elementos gráficos del sitio Web, y un número telefónico que pretendería ser el verdadero.

El código HTML malicioso se insertó en la pantalla de edición del código fuente HTML que presenta Outlook Express, en el tab Source.

El código fuente original era el siguiente:

```
1 <BODY bgColor=#ffffff onLoad="scrollit(100)">
2 <DIV align=center><FONT face=Arial size=2><IMG alt="Banco Virtual de Honduras"
3 hspace=0 src="C:\Temp\images\frame-sup-izq.jpg" align=baseline
4 border=0></FONT></DIV>
5 <DIV align=center><FONT face=Arial size=2></FONT>&nbsp;</DIV>
6 <DIV align=justify><FONT face=Arial size=2>Estimado Cliente:<BR><BR>Nuestro
7 control de Auditoría ha detectado que su cuenta se encuentra actualmente en un
8 saldo negativo de: LPS. -1,480.73.&nbsp;   Debido a que usted no ha firmado un
```



Cliente de correo	Presentación del correo	Ofuscación del URL	Nivel de riesgo
Microsoft Outlook Express	El mensaje contenía todos los elementos gráficos y de formato.	Al hacer clic sobre el URL, se llegaba al sitio phish. La línea de estado del navegador mostró la dirección del servidor <i>phish</i> .	Alto
Squirrel Mail	El mensaje no desplegó correctamente.	Al hacer clic sobre el URL, se llegaba al sitio original. La línea de estado del navegador mostró la dirección del servidor original.	Bajo
GMail	Las gráficas del mensaje se mostraron bien Al hacer clic sobre el URL, se redirigió al sitio phish.	Al hacer clic sobre el URL, se llegaba al sitio phish. La línea de estado del navegador mostró la dirección del servidor <i>phish</i> .	Alto
Yahoo! Mail	El mensaje no desplegó correctamente, pero había una opción para mostrar las gráficas. Se recibió en el folder de correo basura (Junk Mail o Spam).	Al hacer clic sobre el URL, se llegaba al sitio phish. La línea de estado del navegador mostró la dirección del servidor <i>phish</i> .	Medio

La efectividad de las medidas de código malicioso se evaluó haciendo un cruce del número de clientes de correo vulnerables respecto a cada una de las características del código, asumiendo que el usuario será inducido a seguir el enlace *phish* el 100% de las veces:

Medida	Efecto	Riesgo
Actualizar la barra de estado del navegador con información falsa	Esconder la dirección falsa.	0%
Esconder en HTML la dirección del servidor <i>phish</i> dentro de un HREF	Mostrar en pantalla una dirección URL diferente a la que navegará, si es seleccionada.	75%
Cambiar el texto de la barra de estado del navegador con información falsa cuando se hace clic o se pasa el apuntador del ratón sobre el URL.	Esconder la dirección falsa.	0%

Con base a los resultados anteriores, se establece una matriz de análisis de riesgos y controles, para minimizar el impacto de este tipo de ataques, desde el punto de vista del receptor de los mensajes. En cambio, el sitio atacado tiene mayores problemas de seguridad, pero que no son analizados en este documento:

Escenario de riesgo	Riesgo base	Control	Riesgo residual
Código dentro de un mensaje que actualiza la barra de estado del navegador con información falsa.	0%	Asegurarse que el navegador de Internet esté actualizado con los últimos parches de seguridad, y contar con software antivirus y antispam actualizado.	0%
Mensaje alterado de tal forma que esconde en HTML la dirección del servidor <i>phish</i> dentro de un HREF.	75%	Entrenamiento a los usuarios para reconocer mensajes fraudulentos; campañas de información y prevención; contar con software antivirus y antispam actualizado.	Bajo
Código dentro de un mensaje que cambia el texto de la barra de estado del navegador con información falsa cuando se hace clic o se pasa el apuntador del ratón sobre el URL.	0%	Asegurarse que el navegador de Internet esté actualizado con los últimos parches de seguridad, y contar con software antivirus y antispam actualizado.	0%

Debe notarse que los dos ataques con riesgo 0% fueron explotados activamente hasta que los fabricantes o diseñadores del software crearon los parches de seguridad apropiados, lo que muestra la importancia de mantenerse al día en actualizaciones de seguridad, ya que con software moderno, como el que se probó, no se tuvo incidencia de estos riesgos.

## D) Otros posibles ataques conocidos

Otra técnica usada en mensajes *phish* se denomina ofuscación de direcciones (*URL obfuscation*), la cual trataba de presentar direcciones Web falsas aprovechándose de una característica poco utilizada de formateo de claves para ingresar a sitios FTP. El formato utilizado era el siguiente:

`http://usuario:clave@sitiowebatacado`

Siguiendo ese formato, una opción adicional para falsificar direcciones en nuestro caso podría mostrarse como:

`http://www.bancovirtual.hn:DKSADUGnas8432o25n5sodoirdi4@hackers.phish.net`

Es posible que este tipo de direcciones sea más efectivo para engañar al receptor de mensajes phish, ya que esconden de una forma más efectiva, y sin necesidad de programación al sitio phish ya que en el ejemplo mostrado, la parte que dice [www.bancovirtual.hn](http://www.bancovirtual.hn) es solamente un identificador de usuario, y no una dirección de sitio.

Debido a que esta vulnerabilidad fue considerada crítica, ya fue corregida por Microsoft y otros proveedores de navegadores de Internet, y ha sido incluida en las firmas de detección de algunos programas antivirus y antispam.

## CONCLUSIONES

- Es posible crear la infraestructura básica de un sitio malicioso similar a de cualquier empresa, de forma muy sencilla y rápida de manera que se puede adaptar el código disponible públicamente para realizar acciones no esperadas.
- Es posible manipular directamente código HTML de mensajes de correo electrónico con características que permiten explotar vulnerabilidades en clientes de correo y navegadores Web.
- Es importante mantenerse al día en actualizaciones de seguridad, tanto para los clientes de correo electrónico, como los servidores.
- Para evitar problemas en los mensajes de correo electrónico, es necesario activar características para que los clientes de correo no interpreten código dentro de los mensajes recibidos; adicionalmente, el software antivirus y antispam requiere de un proceso más exhaustivo de revisión del código HTML, posiblemente a través de análisis heurístico.
- La educación a los usuarios puede ser un método efectivo de mitigación de riesgos informáticos, ya que las técnicas de ingeniería social basan su éxito en engañar a las personas, y no a infiltrarse por medio de vulnerabilidades de sistemas.

## BIBLIOGRAFÍA

- Anderson, R. (2001). Security engineering: A guide to building dependable distributed systems. New York, New York: John Wiley & Sons.
- Cheswick, W. R., Bellovin, S. M. (1994). Firewalls and Internet security: Repelling the wily hacker. Reading, Massachussets: Addison-Wesley.
- Crume, J. (2000). Inside Internet Security: What hackers don't want you to know. Edimburgo, Gran Bretaña: Pearson Education.
- Gundavaram, S. (1996). CGI programming on the World Wide Web. Sebastopol, California: O'Reilly & Associates.
- McClure, S., Scambray, J. & Kurtz, G. (1999). Hacking exposed: Network security secrets and solutions. New York, New York: McGraw-Hill.
- Tomlinson, R. The first e-mail. En *Ray's page* (Frequently asked questions). Recuperada el 15 de noviembre de 2005, de <http://openmap.bbn.com/~tomlinso/ray/firstemailframe.html>.