Estos correos intentan engañar al usuario diciéndole que ha sido ganador de algún premio: viaje, dinero en efectivo, autos, etcétera.

- Supuestos boletines informativos de una institución pública o privada.

  Los intrusos que utilizan este tipo de temas invitan al usuario al usuario a descargar un archivo o visitar una página que supuestamente contiene un "boletín" o archivo elaborado por alguna institución reconocida y de confianza para la sociedad.

Ejemplo de un correo electrónico de pharming

El usuario recibe un correo electrónico con el siguiente tema: ¡Has recibido una tarjeta de Gusanito.com! y podría provenir de una dirección aparentemente válida como cards@cards.gusanito.com.

El correo electrónico usualmente contiene un vínculo para que se descargue un archivo ejecutable, el cual realiza la modificación en el archivo hosts de tu sistema para redireccionar tu navegador de Internet a páginas Web falsas.

¿Cuál es la diferencia entre phishing y pharming?

atacado. Ahora bien, en el Pharming el ataque ocurre cuando se envía el correo electrónico y se concreta cuando el usuario abre su contenido. En el caso de Phishing lo podemos observar cuando el intruso crea el sitio falso y completa su ataque cuando la víctima introduce sus datos personales.

Si deseas conocer más sobre phishing te recomendamos el siguiente documento:

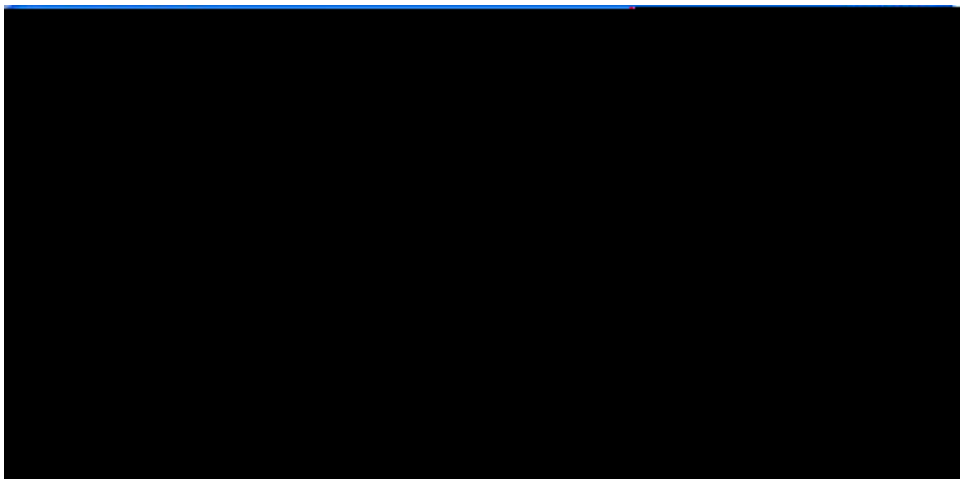
http://www.seguridad.unam.mx/usuario-casero/secciones/phishing.dscs

¿Cómo puedo identificar si he sido víctima de un ataque de pharming?

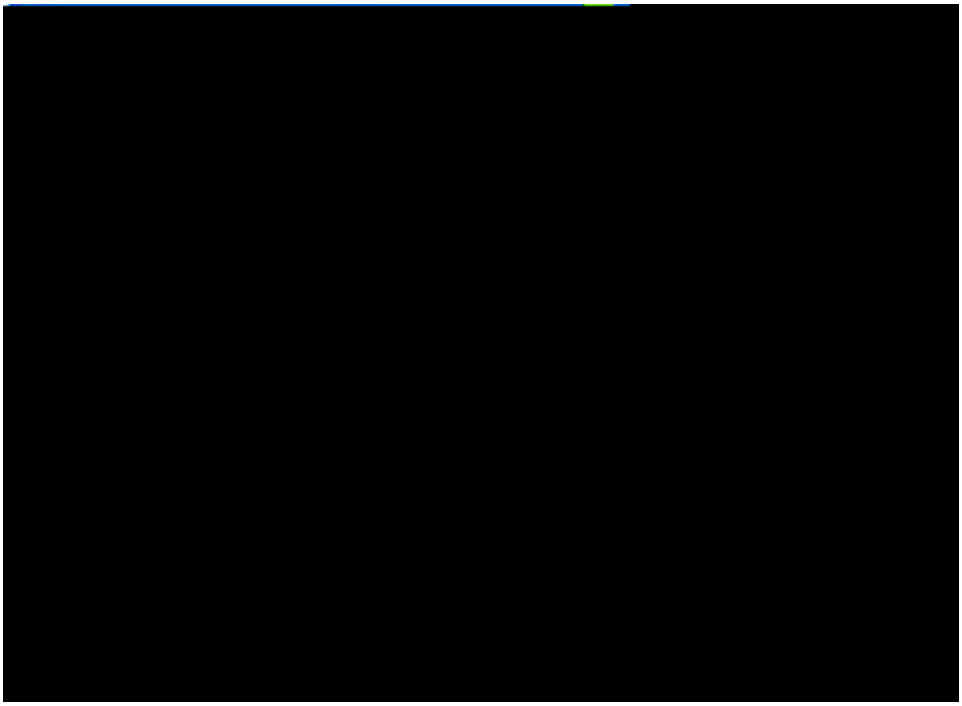
Si sospechas que has sido víctima de un ataque pharming puedes verificar el contenido del archivo hosts (sin extensión) ubicado en la carpeta:

- C:\Winnt\system32\drivers\etc (en sistemas Windows 2000) ó
- C:\WINDOWS\system32\drivers\etc (en sistemas Windows XP y Windows Server 2003)

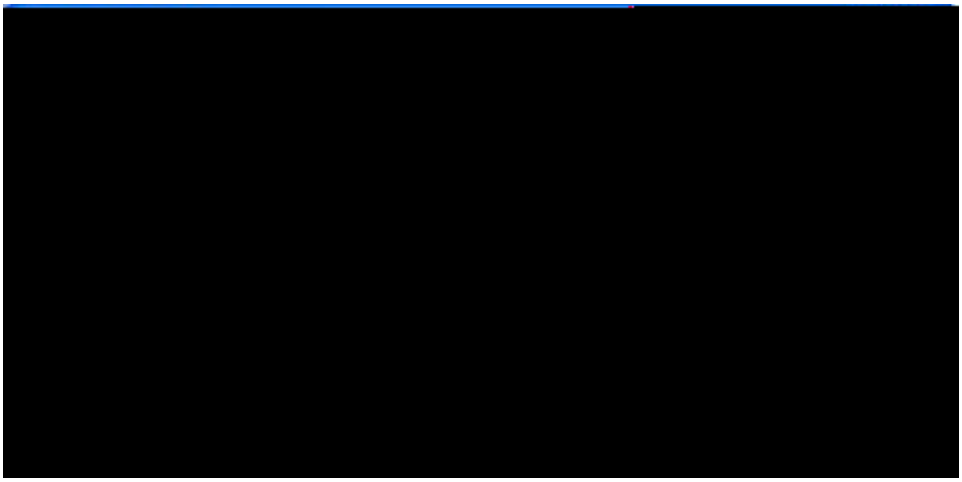
La estructura de un archivo hosts con un contenido normal se muestra a continuación:



Como puede observarse, existen distintas direcciones IP agregadas al archivo hosts que redireccionarán a tu



3. Haz doble clic sobre el archivo hosts y ábrelo con el Bloc de Notas.
4. Elimina todas las entradas distintas a 127.0.0.1 localhost y a continuación haz clic en el men EaArchivo y después en Guardar.



6. Otra posible solución es copiar el archivo hosts de un equipo del que estés completamente seguro que no ha sufrido ningún ataque al equipo comprometido.

¿Cómo me puedo proteger del pharming?

Para prevenirte de este tipo de ataques te damos las siguientes recomendaciones:

- No abras correos electrónicos de desconocidos.
- No proporciones información sensible (usuarios, contraseñas, datos de tarjetas de crédito) por correo electrónico o a través de enlaces a sitios Web contenidos en mensajes de correo electrónico no solicitado.
- No descargues archivos a través de enlaces contenidos en un correo electrónico no solicitado.
- Instala y/o actualiza software antivirus y software antispyware.
- Reporta los correos sospechosos a

  phishing at seguridad dot unam dot mx o incidentes at seguridad dot unam dot mx.

Revisión histórica

- Liberación original: 28 de agosto de 2005
- Última revisión: octubre de 2009

El Departamento de Seguridad en Computo/UNAhate Seguridad en CoRTTj radecos de poyocorr soelaboal: 28 de ytu