

Protocolo de Segu-Info para denunciar casos de Phishing

*Durante los 11 años de existencia de **Segu-Info** hemos puesto énfasis en colaborar con la comunidad y las fuerzas del orden en la denuncia y persecución de casos de Phishing y malware y, durante este tiempo, hemos creado un **Protocolo interno para el seguimiento y baja de casos**.*

El objetivo del presente es exponer dicho Protocolo para:

- *Identificar el carácter del correo o sitio denunciado para verificar si es procedente investigarlo*
- *Identificar abuso de recursos en Internet, para reportarlo a sus responsables*
- *Denunciar sitios falsos o malware propagado para prevenir y evitar que el engaño, fraude o estafa continúe activo*
- *Notificar a la comunidad la modalidad del engaño y las formas de mantenerse alerta*

Autor: Cristian Borghello y Raúl Batista – Segu-Info

Versión: 1.0 (20110401)

Introducción

El Protocolo creado por **Segu-Info** para denunciar y dar de baja sitios falsos en Internet se divide en 10 etapas, algunas obligatorias y otras opcionales y está pensado e ideado para lograr la mayor reacción y velocidad posible ante una denuncia y lograr la baja del sitio falso en el menor tiempo posible, incluso por debajo de los 5 (cinco) minutos después de recibida la primera denuncia. Además también asegura la detección de archivos dañinos que puedan ser recibidos en dichas denuncias.

Inicialmente **Segu-Info** recibe las denuncias anónimas de sus usuarios, mediante dos alternativas:

- Ingresar a www.segu-info.com.ar/denuncia y enviar la denuncia deseada
- Enviar un correo a [phishing\[arroba\]segu-info.com.ar](mailto:phishing[arroba]segu-info.com.ar) adjuntando o reenviando el correo falso que se desea denunciar

A continuación se aplica el Protocolo creado por **Segu-Info** para analizar, denunciar y lograr la baja de sitios dañinos. Una vez recolectada la información pertinente de cada caso, se publica su análisis en: www.segu-info.com/phis

1. Clasificación de los correos recibidos

Al recibir el correo denunciado, inicialmente, el mismo puede clasificarse en:

- **Phishing:** correo con vínculo a sitio web falso que solicita datos personales y/o credenciales de acceso del usuario y que generalmente está relacionado con alguna entidad bancaria o financiera reconocida en el mercado.
- **Scam:** correo sin adjunto ni enlaces pero que realiza un pedido de información privada o comercial al destinatario y la misma debe ser enviada a una cuenta de correo.
- **Malspam:** correo con vínculo o adjunto que al final llevan a la infección de la PC.
- **Marketing:** correos pobremente diseñados que se confunden con alguno de los casos anteriores por su redacción y/o por vínculos a dominios que simulan ser marcas y empresas reconocidas.
- **Spam, boletines de información o publicidad:** correos “normales” que no son una amenaza pero que son reportados erróneamente o por desconocimiento de quien lo hace.

Si bien existen otros tipos de correos fraudulentos, en Segu-Info se analizan los descriptos anteriormente debido a su masividad y a lo común de las denuncias recibidas.

2. Verificación sobre un caso real de Phishing/Scam/Malspam

Luego de la clasificación inicial, se lee el correo y se comienza su análisis para evaluar que acción ofrece el delincuente al destinatario:

- Hacer clic en un texto o imagen que tiene un vínculo a una página web (Phishing). Dicha página ha sido creada por el delincuente y puede estar alojada en un servidor gratuito, en un servidor vulnerado previamente o en un Blog.



Imagen 1 – Phishing que apunta a un sitio falso

- Pedido de respuesta al mensaje con cierta información sensible o personal (Scam)

Si le interesa saber más sobre la posibilidad de cobrar ganancias merecidas por su trabajo le pedimos enviar sus datos de contacto al siguiente correo:

`info@hiring-[ELIMINADO].com` [Por favor, borra los espacios antes de enviar el correo]

1. Nombre, apellido;
2. Edad;
3. País de residencia;
4. Teléfonos de contacto. (el numero de telefono en el formato enternacional)

Imagen 2 – Scam que solicita el envío de datos a un correo

- Publicidad no deseada

BASE DE DATOS DE EMAILS DE ARGENTINA

SEGMENTADOS POR RUBROS - 8 MILLONES DE EMAILS

RECOPIACION DE EMAILS DE LOS ULTIMOS 10 AÑOS

Permite realizar estrategias de marketing mucho más precisas y definidas, descubrir nuevos mercados, etc. Es una herramienta imprescindible de decisión. La información que se obtiene pe gestión comercial de cualquier empresa, dado que cuenta con la más completa información disponible.

Imagen 3 - Publicidad

- Abrir un archivo adjunto o descargar el mismo desde un enlace (Malware)

Bradesco S/A

Caro cliente, [REDACTED] ;
A instituição, **Bradesco** vem através deste aviso notificar que a partir da **Lei 000529/2010** será obrigatória realizar a **atualização cadastral do seu Cartão Chaves de Segurança**.

Utilize o botão abaixo para efetuar a atualização:

Atualizar

[http://www.color\[REDACTED\].com/plugins/syst...lizacao.com](http://www.color[REDACTED].com/plugins/syst...lizacao.com)

Imagen 4 – Phishing que descarga un archivo dañino (.COM)

Esta verificación es fundamental para responder a quien haya realizado la denuncia sobre la veracidad del caso y también para confirmar que no se trata de un correo original que se malinterpretó como falso. Posteriormente esta verificación también es la que se tiene en cuenta en caso de denunciar el caso a la entidad afectada.

3. Datos de las cabeceras del correo

Debido a que el [protocolo SMTP](#) usado para enviar correo electrónico carece de los medios para evitar falsificaciones, los datos de dirección tales como los campos *Sender*, *From*, *Reply-to*, *To*; no deben ser tomados como auténticos, podrían ser falsificados y de hecho lo son cuando están involucrados ataques como los mencionados anteriormente.

```
Delivered-To: [REDACTED]@gmail.com
Received: by 10.231.173.130 with SMTP id p2cs1143ibz;
      Wed, 23 Mar 2011 00:53:53 -0700 (PDT)
Received: by 10.150.94.19 with SMTP id r19mr6202799ybb.310.1300866833417;
      Wed, 23 Mar 2011 00:53:53 -0700 (PDT)
Return-Path: <Debian-exim@espoir[REDACTED].com>
Received: from SRV1023-MIA.server[REDACTED].com (srv1023-mia.server[REDACTED].com [38.117.1.254])
      by mx.google.com with ESMTP id p5si9873542ybk.63.2011.03.23.00.53.53;
      Wed, 23 Mar 2011 00:53:53 -0700 (PDT)
Received-SPF: neutral (google.com: 38.117.1.254 is neither permitted nor denied by best
Authentication-Results: mx.google.com; spf=neutral (google.com: 38.117.1.254 is neither
Received: from mail.espoir[REDACTED].com ([REDACTED] 20.228.161])
      by SRV1023-MIA.server[REDACTED].com (Post.Office MTA v3.5.3
      release 223 ID# 0-53968U100L100S0V35) with ESMTP id com
      for <[REDACTED]@gmail.com>; Wed, 23 Mar 2011 01:29:27 -0400
Received: from Debian-exim by mail.espoir[REDACTED].com with local (Exim 4.69)
      (envelope-from <Debian-exim@espoir[REDACTED].com>)
      id 1Q2G13-0003SD-3R
      for [REDACTED]@gmail.com; Wed, 23 Mar 2011 01:37:25 -0400
To: [REDACTED]@gmail.com
Subject: TARJETA INACTIVA!!
From: BBVA@Atencion-seguridad.net
Content-Type: text/html
Message-Id: <E1Q2G13-0003SD-3R@mail.espoir[REDACTED].com>
Date: Wed, 23 Mar 2011 01:37:25 -0400
```

Imagen 5 – Cabecera de un correo de Phishing

Analizar el servidor desde donde se originó el correo (su dominio e IP) puede ser de utilidad para identificar un origen malicioso, pero no necesariamente concluyente. En esta etapa puede identificarse un servidor válido y auténtico como remitente, y aun así es necesario completar el análisis del cuerpo del mensaje. En casos espurios pueden aparecer datos interesantes o novedosos respecto de la modalidad usada por el delincuente o el atacante.

Las direcciones IP desde donde se reciben ataques de delincuentes pueden ser: redes bot (constituidas por PC zombies infectadas conectadas a banda ancha), servidores de correo configurados en forma incorrecta y que permiten el envío de correos falsos, servidores de correo alojados en ISP poco responsables o servicios abusados tales como los de email marketing. En este caso también se puede analizar el [registro PTR](#) de la IP en cuestión.

En este aspecto es interesante el análisis automatizado que realiza [SpamCop](#) en el que es necesario estar registrado pero que se puede usar de forma gratuita. Al reportar el correo se puede marcar “*Show technical details*” para obtener y visualizar el análisis del correo involucrado. El mismo sistema prepara la notificación a cada uno de los responsables de las redes, sitios web y servicios involucrados que automáticamente el sistema pueda determinar. SpamCop además alimenta una [RBL \(Black List\)](#) que luego puede ser utilizada como referencia para casos futuros.

4. Análisis del cuerpo del mensaje

Si el mensaje esgrime motivos de re-empadronamiento, o alerta de bloqueo de cuentas, tarjetas, o servicio, habilitación de *e-token* o un nuevo mecanismo de seguridad, en esos casos es casi seguro que se trata de un engaño de Phishing o Malspam. Si bien esos son los casos más usuales, existen otros casos que en general apuntan a seducir al receptor para que haga clic, abra un adjunto o responda el correo enviando cierta información.

Comúnmente, en el correo se encuentra una imagen o una dirección web con un enlace que conduce a un sitio dañino.

5. Análisis de enlaces y descargas

Una vez determinado cuál es el enlace dañino, se puede realizar **un análisis activo o pasivo** del mismo.

5.1 En el **análisis activo** se procede a visitar el enlace sospechoso en **condiciones de laboratorio** y se verifica a que resultado conduce. Estas condiciones involucran que quien realiza el análisis debe tener un conocimiento técnico importante y utilizar herramientas que aseguren que no se verá involucrada información personal o equipos de computación personal.

El procedimiento recomendado a seguir es el siguiente:

- a) Aislar el sistema operativo y navegador de las posibles consecuencias que podría generar navegar en un sitio dañino.
- b) Utilizar una máquina virtual para ejecutar las acciones y, al finalizar el análisis, descartar cualquier cambio realizado sobre la misma.
- c) Utilizar alguna herramienta que provea un ambiente aislado para el proceso del navegador, por ejemplo [Sandboxie](#) o el modo *Sandbox* del [Firewall gratuito Comodo](#).
- d) Utilizar herramientas de detección de amenazas tales como las ofrecidas por cualquier *Firewall* y/o antivirus.
- e) Realizar un análisis detallado de las acciones, páginas visitadas y archivos descargados por el sitio sospechoso. En este caso se puede utilizar cualquier navegador que admita extensiones tales como [HTTP-Watch](#), [HTTP-Fox](#) o [No-Script](#), [ShowIP](#) y los complementos como [WOT](#), y [Webutation](#).

En este análisis cada persona desarrolla sus preferencias en cuanto a cómo realizarlo y probablemente se deberá realizar varias veces para conseguir y buscar la siguiente información:

- Tráfico HTTP, sitios y recursos utilizados (HTTP-Watch y HTTP-Fox)
- Detección por parte del navegador FireFox/Chrome ([SafeBrowsing de Google](#)), Internet Explorer (SmartScreen) y de las herramientas de reputación web como [Site Advisor de McAfee](#), [WOT](#) y [Webutation](#).

Si el sitio dañino sigue activo se pueden encontrar varias formas elegidas por los delincuentes para alojarlos y engañar a la mayor cantidad de víctimas posibles.

a) Sitio web que copia en forma casi idéntica al sitio original y tiene campos donde se piden datos sensibles, como usuario, contraseña, PIN, código secreto, datos de la tarjeta de crédito o de la tarjeta de coordenadas, lugar y fecha de nacimiento y cualquier otro dato sensible. En este caso se está frente a un caso de Phishing tradicional.

En este caso se podrá comprobar la dirección en donde termina la navegación y desde dónde se visualiza el formulario de datos, cuidando de no ser engañados por los gráficos o los *scripts* tomados del sitio original afectado (tal es la práctica de muchos delincuentes para que el sitio falso luzca semejante al original).

Por ejemplo en la siguiente imagen puede apreciarse que existen redirecciones de un sitio a otro y que finalmente la página del engaño se encuentra en un tercer dominio:

```
E:\>wget -Oa.txt http://www.wildand[REDACTED].co.uk/site/cache.php
--19:58:51-- http://www.wildand[REDACTED].co.uk:80/site/cache.php
=> 'a.txt'
Connecting to www.wildand[REDACTED].co.uk:80... connected!
HTTP request sent, awaiting response... 302 Found
Location: http://goo.gl/Cq[REDACTED] [following]
--19:58:52-- http://goo.gl:80/C[REDACTED]
=> 'a.txt'
Connecting to goo.gl:80... connected!
HTTP request sent, awaiting response...
Location: http://www.iphone4[REDACTED].org/media/ssl/en-linea.colmena.com.co/icol/control/ [following]
--19:58:52-- http://www.iphone4[REDACTED].org:80/media/ssl/en-linea.colmena.com.co/icol/control/
=> 'a.txt'
Connecting to www.iphone4[REDACTED].org:80... connected!
HTTP request sent, awaiting response... 200 OK
Length: 1,573 [text/html]
```

Imagen 6 – Seguimiento de sitios web dañinos

Con la información recogida, posteriormente ya se puede realizar las denuncias pertinentes de todos los dominios involucrados.

b) Página web alojada en un sitio gratuito o Blog (Blogger, Wordpress, etc.). En este caso generalmente se intenta engañar al usuario para que ingrese información personal referida a algún tipo de premio y es alojada en Blogs gratuitos por la dificultad que ofrecen estos para dar de baja una página alojada allí.

Por ejemplo la siguiente página alojada en Blogger y que ofrece supuestos premios de compañías telefónicas:



Imagen 7 – Sitio con promociones falsas alojado en Blogger

c) Descarga de un archivo (ejecutable o de otro tipo) esgrimiendo distintos motivos como ser actualización de seguridad, *codec* para visualizar un video y muchos otros. En caso de Malspam, se descarga el archivo dañino (sin ejecutarlo) y se procede a su análisis y reporte. Es recomendable que la carpeta de descarga no sea analizada en forma automática por un antivirus, debido a que si el mismo es detectado, podría ser eliminado y lo que se desea es conservarlo para su análisis.

Finalmente, en esta etapa se analizan las distintas carpetas públicas del servidor que aloja el sitio falso, con el fin de hallar y analizar cualquier tipo de información adicional sobre el caso, como podría ser:

- Carpetas sospechosas con otros casos similares de Phishing o malware.
- Archivos con información del atacante, como puede ser su correo electrónico.
- Archivos comprimidos conteniendo todos los archivos del caso (es común que “delincuentes sin experiencia” cometan este error).

- Base de datos o archivos de texto con la información robada a las víctimas.
- Contadores o estadísticas de ingreso de las víctimas.



Name	Last modified	Size	Desc
Parent Directory		-	
AJUDA.txt	13-Mar-2010 14:30	933	
ERRO.php	28-Mar-2011 22:57	5.1K	
Encerramento.php	28-Mar-2011 22:58	5.0K	
Scripts/	04-Jan-2011 22:58	-	
VRFSENHA.php	28-Mar-2011 22:57	43K	
VRFSENHA1UAL.php	28-Mar-2011 22:57	127K	
enviauto.js	14-Mar-2010 02:40	76	
finaliza.php	29-Mar-2011 06:07	8.3K	
imagens/	04-Jan-2011 21:36	-	

Apache/2.2.11 (Ubuntu) PHP/5.2.6-3ubuntu4.6 with Suhosin

Imagen 8 – Archivos dañinos almacenados en un servidor vulnerable

Cualquier tipo de información que se encuentre es útil para continuar con la denuncia del caso o comenzar con uno nuevo.

5.2 En el **análisis pasivo** se analiza el dominio y páginas involucradas en el enlace. Hay que tener en cuenta que el dominio involucrado puede ser un dominio benigno que aloja, en ese momento y sin conocimiento de sus administradores, un sitio malicioso, “plantado” por el delincuente mediante vulnerabilidades en el servidor y sus aplicaciones o bien puede contener un archivo que redirige a otro sitio malicioso. Por ejemplo se puede utilizar:

www.sitio-no-daño.com/nombre_banco/homebanking

En este caso el administrador de “sitio-no-daño.com” desconoce que alguien subió un contenido dañino a su sitio y que engaña a usuarios para que ingresen a él.

Puede ocurrir que el dominio y el sitio dañino hayan sido registrados por el mismo delincuente y el dominio utilizado podría ser un nombre similar al sitio blanco del engaño. Por ejemplo:

www.BANC0-REAL.com donde la letra “O” en realidad es el número cero (0).

Y, también puede darse el caso ya explicado de que el sitio falso se encuentre alojado en un Blog gratuito: <http://promociones.blogspot.com/ganadores-del-mes>

El **análisis pasivo** correctamente realizado no implica ningún riesgo al realizarlo pero este análisis tampoco es suficiente en todos los casos. Esto se debe a dos prácticas conocidas y frecuentemente utilizadas en los enlaces de los correos de Phishing/Malspam:

- El enlace puede ser a un sitio benigno recientemente abusado y desde ese sitio se redirige a la víctima a otro sitio controlado por el delincuente. En este caso se obtiene información del sitio a donde sería redirigida la víctima, o sea, el sitio donde finalmente la víctima brindaría su información o sería infectada.
- El enlace conduce a un acortador de URL como las provistas por Bit.ly, Goo.gl, Ow.ly y muchos otros. En este caso es posible continuar analizando el sitio destino.

A continuación se detallan los pasos de este análisis:

- a) Verificar el dominio involucrado y comprobar que no se trata de ningún dominio real relacionado con la marca que se intenta afectar.
- b) Usar un servicio Whois para verificar la fecha de creación, identidad y país de la entidad registrante (posible delincuente con nombre falso):
 - Fecha de creación: si es muy próxima a la fecha actual es altamente sospechosa, pero no concluyente.
 - Datos del registrante: los registros anónimos o evidentemente falsos son sospechosos, pero no concluyentes.
 - Países de registro: en caso del sudeste asiático o Europa del Este pueden ser sospechosos, aunque generalmente este dato depende del contexto y del caso analizado.

Ante cualquier duda, o como confirmación, de un dominio malicioso se puede realizar una o más de las siguientes comprobaciones.

- a) Analizar la reputación del dominio. Se puede utilizar [WOT](#), [Webutation](#) ya que ambos son de utilidad y fácilmente utilizables por cualquier usuario. Estas herramientas pueden utilizarse como extensiones del navegador o visitar y usar en línea con registro previo. Existen muchos otros similares y con los mismos objetivos.
- b) Analizar si el vínculo fue reportado previamente a [PhishTank](#).
- c) Si el vínculo es una dirección IP, es casi seguro que se trata de un sitio montado por delincuentes y por lo tanto es una identificación positiva de Phishing o Malspam.

Nota: en caso de dominios benignos abusados, **Segu-Info** sólo realiza el análisis en busca de información de contacto con el objeto de reportar el abuso al propietario o administrador del sitio afectado a fin de que el mismo pueda proceder de la forma en que lo considere adecuado.

6. Análisis de acortadores de URL

Actualmente es muy común que los delincuentes utilicen acortadores de URL para lograr un mayor nivel de éxito en los correos y engaños creados. En este caso se puede seguir el siguiente procedimiento según el acortador involucrado:

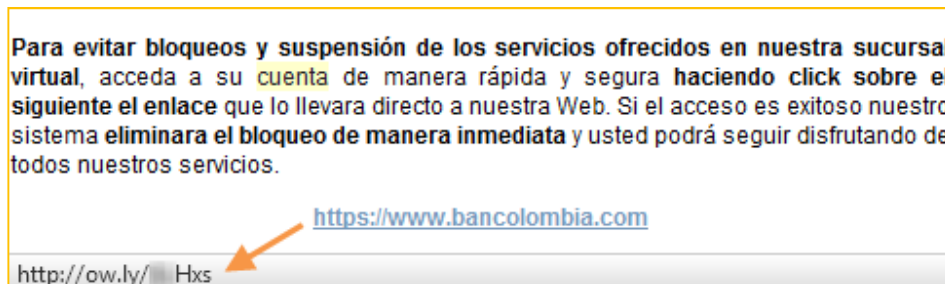


Imagen 9 – Phishing que utiliza un acortador de URL

- [Bit.ly](http://bit.ly) y j.mp → Report Abuse. En este caso agregando “+” al final de la URL involucrada, se obtiene la página destino con la dirección real y las estadísticas del mismo. Por ejemplo <http://bit.ly/segu+>, como se ve a continuación:



Imagen 10 – Datos de una URL acortada

- Goo.gl → Report spam. También se puede utilizar “+”.
- www.tinyurl.com por correo a support@tinyurl.com.
- Utilizar LongUrl y/o [URL Void](http://URLVoid) para conocer la URL destino o bien existen extensiones del navegador que realizan el mismo trabajo (por ejemplo LongURLPlease).
- En [este artículo](#) se explica cómo denunciar en otros acortadores de URL conocidos.

7. Denunciar el abuso al propietario del sitio benigno

Para llevar adelante esta acción se puede visitar la página inicial del sitio y buscar información de contacto ya sea un formulario web o una dirección de correo que figure allí.

En el reporte se explica muy brevemente qué es **Segu-Info**, cuáles son sus objetivos (no comerciales) y nuestra especialidad en Seguridad de la Información. Posteriormente se informa de las vulnerabilidades y del abuso del sitio y se solicita que lo corrijan, destacando la importancia que se haga revisar la seguridad por profesionales capacitados en dichas tareas.

8. Denuncia de Phishing

En este caso se realizan una serie de acciones, que aseguren la baja del sitio dañino a la brevedad posible:

- Denunciar el caso a la entidad afectada a fin de que pueda informar a tiempo a sus clientes y pueda tomar las acciones legales o técnicas que crea necesaria. **Segu-Info** en este caso brinda toda la información de la que disponga y deja que la entidad continúe con sus propios procesos.
- Denunciar la dirección del sitio falso contenida en el correo y las posibles redirecciones involucradas. Cada una de estas direcciones es denunciada a [PhishTank](#), sitio [operado por OpenDNS](#), y que comparte información con el sitio [APWG](#) (AntiPhishing Working Group). Estos sitios requieren estar registrados y que otros miembros voten la denuncia para transformarla en efectiva.
- Denunciar en [WOT](#) con su calificación y un comentario que exprese la naturaleza del sitio dañino. Requiere estar registrado.
- Denunciar en Firefox mediante el menú Ayuda → Informar sitio fraudulento. Es anónimo.
- Denunciar en Internet Explorer mediante el menú Herramientas → Filtro SmartScreen → Notificar sitio web no seguro. La denuncia también es anónima.
- Si el sitio está alojado en un hosting gratuito o pago, y el mismo puede ser identificado, se realiza el mismo tipo de denuncia y se repite el procedimiento con los DNS involucrados.

El procedimiento indicado se hace para cada sitio o redirección detectada en el engaño.

9. Denunciar casos de Malspam y Malware

En estos casos se procede a denunciar los sitios que contengan la página del engaño tal y como ya se realiza para el caso del Phishing. Si el archivo dañino se encuentra alojado en un sitio abusado, también se informa al propietario de dicho sitio.

- a) Se sube el archivo al servicio [VirusTotal](https://www.virustotal.com) y se realiza un comentario apropiado sobre el origen del mismo. Para esta última acción es conveniente estar registrado (aunque no es obligatorio).
- b) Se envía la muestra dañina comprimida con contraseña y por correo electrónico a los siguientes fabricantes de antivirus:
 - virus_doctor@trendmicro.com
 - samples@eset-la.com
 - virus@avast.com
 - virus@avg.com
 - virus_research@avertlabs.com
 - samples@sophos.com
 - Otros...

10. Seguimiento, bloqueo y baja del sitio dañino

Finalmente se realiza el seguimiento del caso por el tiempo que sea necesario hasta lograr el bloqueo o la baja definitiva del sitio dañino. Este trabajo puede involucrar desde varios días en el caso de sitios dañinos complicados o en los cuales están involucradas varias empresas y/o países, o pocos minutos luego de la denuncia recibida, que es lo deseado porque significa una alta tasa de éxito.

Conclusiones

Si bien en muchos casos no es posible determinar quién es el responsable de la baja del sitio falso o de la detección del malware (**Segu-Info**, la entidad afectada, otras empresas, etc.), lo realmente importante es que se logre dicho bloqueo o baja.

Independientemente de las herramientas y los procedimientos utilizados, en la mayoría de los casos las bajas logradas por **Segu-Info** no superan los pocos minutos desde la recepción de la primera denuncia, lo que confirma la efectividad y eficiencia del Protocolo descrito, el cual ha sido utilizado para lograr la baja de centenas de sitios falsos.

Anexo

Sitios de comprobación de reputación de un sitio o dominio

SafeBrowsing de Google: http://www.google.com/safebrowsing/report_phish/?tpl

WOT: <http://www.mywot.com/es>

Webutation: <http://www.webutation.net/>

Site Safety de TrendMicro: <http://global.sitesafety.trendmicro.com/>

Symantec: <http://safeweb.norton.com/>

Site Advisor de McAfee: <http://www.siteadvisor.com/>

Extensiones de Mozilla Firefox

WOT: <http://www.mywot.com/es>

Webutation: <http://www.webutation.net/>

Bitdefender: <http://trafficlight.bitdefender.com/>

ShowIP: <https://addons.mozilla.org/es-ES/firefox/addon/showip/?id=590>

HTTP-Watch: <http://www.httpwatch.com/>

HTTP-Fox: <https://addons.mozilla.org/en-US/firefox/addon/httpfox/>

No-Script: <https://addons.mozilla.org/es-ES/firefox/addon/noscript/>

LongURL: <http://longurl.org/tools>

LongURL Please: <https://addons.mozilla.org/es-ES/firefox/addon/long-url-please/>

Reputación de dirección IP o dominio

Robtex: www.robtx.com

ToolBox: www.mx.toolbox.com

Whois

Domain Tools: <http://www.domaintools.com/>

Software Pointers: <http://www.software-pointers.com/en-whois.html>

Reputación IP, dominio, email

SpamCop: <http://www.spamcop.net/>

Sender Base: <http://www.senderbase.org/>

Reputation Score: <http://www.reputation-score.com/>

McAfee: <http://www.mcafee.com/us/mcafee-labs/threat-intelligence.aspx>

Barracuda: <http://www.barracudacentral.org/lookups>

URLVoid: <http://www.urlvoid.com/>

Denuncias de Phishing

Phishtank: <http://www.phishtank.com/>

SafeBrowsing de Google: http://www.google.com/safebrowsing/report_phish/?tpl

APWG: http://www.antiphishing.org/report_phishing.html

GMail Mail: Menú Responder → Denunciar suplantación de identidad

Hotmail: Menú Marcar como → Correo de suplantación de identidad (phishing)

Firefox: Menú Ayuda → Informar de sitio web fraudulento

Internet Explorer: Menú Filtro de suplantación de identidad (phishing) → Notificar a Microsoft de este sitio web

Opera: presionar sobre el botón “?” a la izquierda de la barra de direcciones → Protección antifraude

Acortadores de URL

LongURL: <http://longurl.org/tools>

LongURL Please: <https://addons.mozilla.org/es-ES/firefox/addon/long-url-please/>

URL Void: <http://www.urlvoid.com/extract-url/>

Información adicional: <http://security.thejoshmeister.com/2009/04/how-to-preview-shortened-urls-tinyurl.html>

Análisis de malware

VirusTotal: <http://www.virustotal.com>

URL Void: <http://www.urlvoid.com/extract-url/>