Reporte de incidentes

Fraude (Phishing)

Tipo de Documento:	Guía
Fecha de Publicación:	04 de diciembre de 2015
Clasificación:	Acceso Libre

Presentado a:	Público General
Autores:	Alan Rodríguez
Versión:	1.2
Estado:	Final

CONTROL DE VERSIÓN

PREPARADO POR: Alan Rodríguez

APROBADO POR: Silvia Batista

FECHA DE INICIO: 18 de junio de 2015

ESTADO DEL DOCUMENTO: Final

HISTORIA DE CAMBIOS:

Fecha	Cambios	Autores	Versión
18/junio/2015	Borrador inicial	Alan Rodríguez	0.1
13/julio/2015	Cambios en redacción	Silvia Batista, Alan Rodríguez	1.0
04/diciembre/2015	Adaptación a formato	Alan Rodríguez	1.1
26/enero/2016	Ediciones	Mario Góngora, Alan Rodríguez	1.2

Contenido

1. Objetivos 4
1.1. Objetivo general 4
1.2. Objetivo específico 4
2. Guía de recolección de evidencia 4
3. Información de contacto: 6

Centro Nacional de Respuesta a Incidentes Informáticos - CSIRT Panamá | Autoridad Nacional para la Innovación Gubernamental
| Edificio Balboa 757, Corregimiento Ancón, Ciudad de Panamá
| Tel: +507 520-CERT (2378) | Fax: +507 517-9500 | E-Mail: info@cert.pa | Twitter: @CSIRTPanama

1. Objetivos

1.1. Objetivo general

Documento de guía rápida de referencia para la recolección de información que sirva de evidencia a compartir con el *CSIRT Panamá* para el análisis en caso de incidentes informáticos en el Estado Panameño.

1.2. Objetivo específico

Ofrecer algunos comandos en sistemas *Linux* y *Windows* para la obtención de información que sirva de evidencia en el análisis de incidentes relacionados con fraude electrónico (*phishing*).

2. Guía de recolección de evidencia

Reportando fraude (*phishing*)

Importante: **recolectar la evidencia** a compartir con el equipo *CSIRT Panamá* **antes de realizar algún cambio interno.**

Comprimir los archivos con la contraseña: Evidencia-CSIRT

Agregar en archivo comprimido y **cifrado con la llave pública del *CSIRT Panamá***:

En caso de suplantación de identidad de página *web* enviar la siguiente información:

- Dirección *URL* fraudulenta.
- Dirección *URL* oficial de la víctima del fraude.
- Código fuente y captura de pantalla de la *URL* fraudulenta.
- Código fuente y captura de pantalla de *URL* oficial.

Centro Nacional de Respuesta a Incidentes Informáticos - CSIRT Panamá | Autoridad Nacional para la Innovación Gubernamental
| Edificio Balboa 757, Corregimiento Ancón, Ciudad de Panamá
| Tel: +507 520-CERT (2378) | Fax: +507 517-9500 | E-Mail: info@cert.pa | Twitter: @CSIRTPanama

En caso de fraude (*phishing*) por correo electrónico enviar la siguiente información:

- Copia de correo fraudulento.
- Captura de pantalla del correo fraudulento y guardar como archivo *.png*.
- Registros del filtro de correo (en caso de tener uno).
- Encabezados (*headers*) del correo fraudulento.
  - Desde *Zimbra*

Hacer *click* con el botón secundario (usualmente botón derecho) al correo de interés y se selecciona “Mostrar original” en la lista desplegable que aparece. Ver Imagen 1.

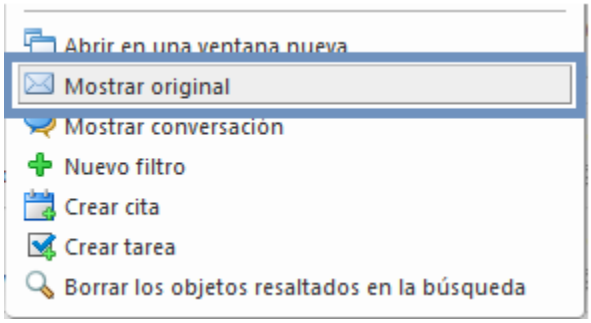

Imagen 1. Opción secundaria sobre correo no deseado.

- Desde *Outlook*

Se selecciona el correo de interés, hacer doble *click* para abrir en una ventana aparte, y en esta pulsar Archivo > Propiedades. Ver Imagen 2.

Imagen 2. Obtención de encabezado de correo en *Outlook*

Centro Nacional de Respuesta a Incidentes Informáticos - CSIRT Panamá | Autoridad Nacional para la Innovación Gubernamental
| Edificio Balboa 757, Corregimiento Ancón, Ciudad de Panamá
| Tel: +507 520-CERT (2378) | Fax: +507 517-9500 | E-Mail: info@cert.pa | Twitter: @CSIRTPanama

Luego se despliega una ventana emergente con los encabezados, se debe copiar y pegar todo el texto mostrado y grabar en un archivo de texto bajo el nombre **Institución_encabezado.txt.**

Presentar en formato comprimido (*zip, rar, tar, bz2*) y cifrar **con llave pública del *CSIRT Panamá*** que se encuentra a continuación en la sección "Información de contacto". Ver guías "CERT-306 – Compresión de archivos (Linux)", "CERT-307 – Compresión de archivos (Windows)" y "CERT-252 - Guía de firma y cifrado de archivos utilizando PGP".
Enviar evidencia a la dirección info@cert.pa colocando en el asunto del correo: **Institución – Fraude (*Phishing*)**.

3. Información de contacto:

CSIRT PANAMA

Computer Security Incident Response Team
Autoridad Nacional para la Innovación Gubernamental
E-Mail: info@cert.pa
Phone: +507 520-CERT (2378)
Web: http://www.cert.pa
Twitter: @CSIRTPanama
Facebook: http://www.facebook.com/CSIRTPanama
Key ID: 16F2B124