OWASP LatamTour
Chile 2011

The OWASP Foundation
http://www.owasp.org

# OWASP Chile

# Delitos Informáticos

Felipe Sánchez Fabre
Perito Informático – Especialista en Delitos Informáticos
e Informática Forense

fsanchez@peritajesinformaticos.cl
fsanchez@fci.cl
Móvil 9228 6839

## Temario

- Antecedentes del relator
- Realidad Internacional y Nacional
- Legislación – Ejemplos prácticos
- Informática Forense
- Sitio del Suceso Computacional

# Antecedentes del Relator

**Felipe Sánchez Fabre**

- Ingeniería de Ejecución en Computación e Informática – Universidad de Santiago de Chile.
- Diplomado en Peritaje Informático – Universidad de Santiago de Chile.
- Diplomado en Criminalística y Metodología Forense – Universidad de Valparaíso.
- Perito Judicial Informático – Ilustres Cortes de Apelaciones de Santiago, Valparaíso, San Miguel y Rancagua.
- Profesor Universidad de Santiago de Chile Diplomado en Peritaje Informático. Cursos: "Peritaje Informático Avanzado" e "Informática Forense".
- Diplomado en Control, Seguridad y Auditoria Computacional – Universidad de Santiago de Chile.
- Diplomado en Seguridad Integral de Empresas – Academia de Ciencias Policiales, Carabineros de Chile.
- Socio de Forensic & Cybercrime Investigation Prevención, Detección e Investigación de Delitos Informáticos.

3

# Realidad Internacional

White Paper

McAfee

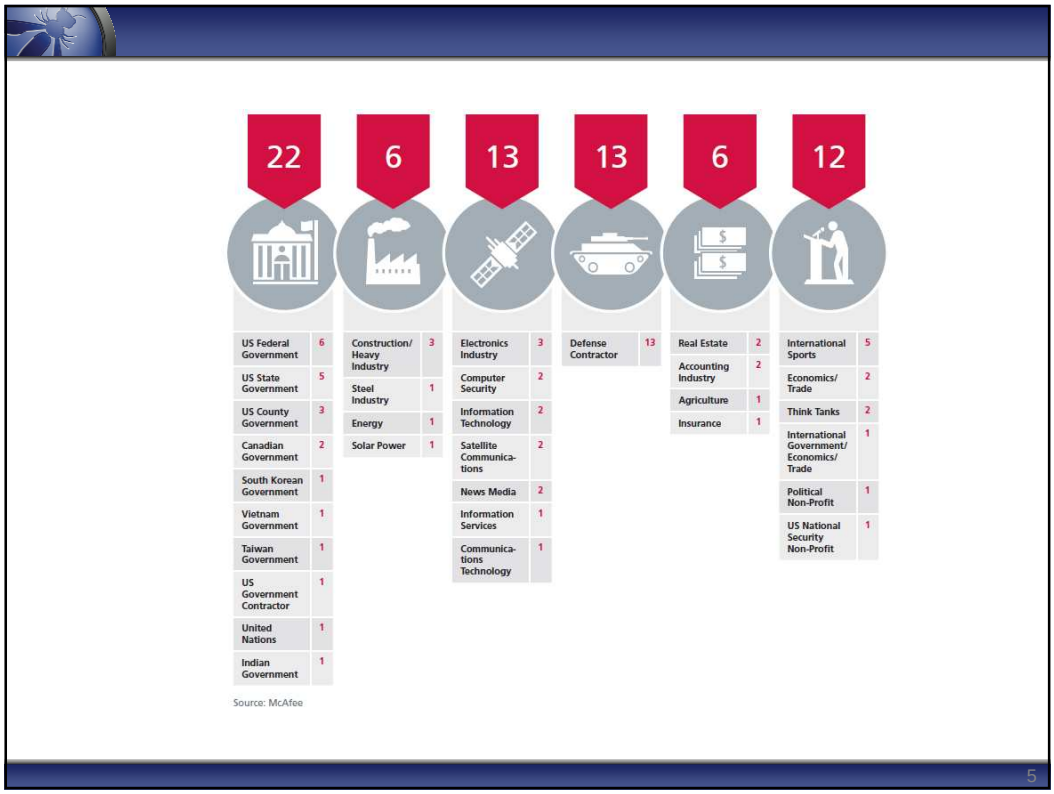
Revealed: Operation Shady RAT

By Dmitri Alperovitch, Vice President, Threat Research, McAfee

An investigation of targeted intrusions into more than 70 global companies, governments, and non-profit organizations during the last five years

Publicación: 2 de Agosto de 2011

4


22
US Federal Government 6
US State Government 5
US County Government 3
Canadian Government 2
South Korean Government 1
Vietnam Government 1
Taiwan Government 1
US Government Contractor 1
United Nations 1
Indian Government 1
6
Construction/ Heavy Industry 3
Steel Industry 1
Energy 1
Solar Power 1
13
Electronics Industry 3
Computer Security 2
Information Technology 2
Satellite Communica-tions 2
News Media 2
Information Services 1
Communica-tions Technology 1
13
Defense Contractor 13
6
Real Estate 2
Accounting Industry 2
Agriculture 1
Insurance 1
12
International Sports 5
Economics/ Trade 2
Think Tanks 2
International Government/ Economics/ Trade 1
Political Non-Profit 1
US National Security Non-Profit 1
Source: McAfee
5


4
49
2
1
1
2
1
1
1
3
2
1
1
3
1
1
Victim's Country of Origin | Victim Count
USA 49
Canada 4
South Korea 3
Taiwan 3
Japan 2
Switzerland 2
United Kingdom 2
Victim's Country of Origin | Victim Count
Indonesia 1
Vietnam 1
Denmark 1
Singapore 1
Hong Kong 1
Germany 1
India 1
Source: McAfee
6

# Realidad Nacional

8 LA TERCERA Miércoles 30 de marzo de 2011

## Formalizan a ingeniero por hurto de base de datos de 400 mil clientes

▶ Camilo Sánchez habría pedido más de un millón de pesos por el archivo.

***Sebastián Labrín***

El pasado jueves, representantes de la empresa [redacted] dependiente del grupo [redacted] se percataron de que, a través de una página web, estaba a la venta la base de datos de sus clientes. A primera hora del viernes, abogados de la firma presentaron una denuncia en el Ministerio Público por espionaje informático, que derivó en que efectivos del Cibercrimen de la PDI indagaran el hecho.

Luego de contactar al presunto vendedor, la policía efectuó una compra simulada entre un representante de la empresa y el sospechoso, "mientras realizábamos una vigilancia discreta, y cuando se realizó la transacción, procedimos a su detención", contó el subcomisario Cristián González.

En el procedimiento se detuvo a Camilo Sánchez Alfaro (26), egresado de Ingeniería In formática que trabajaba para una empresa externa de cobranzas que apoyaba a [redacted] Según la policía, el profesional pidió $ 1,5 millón por el archivo que contenía datos personales (direcciones, RUT y teléfonos) de 400 mil clientes y que fue avaluado por la empresa en $ 800 millones. Según la PDI, Sánchez confesó la venta de una base de datos de [redacted], lo que es indagado por la Fiscalía Centro Norte. El hombre fue formalizado por hurto y espionaje informático. Por este delito,} Sánchez Alfaro arriesga hasta tres años y un día de cárcel.

La abogada del Instituto chileno de Derecho y Tecnologías, Lorena Donoso, dijo que "la mayoría de las veces la gente no tiene idea de la información que se transa a su respecto, ni cómo se transa, ni qué se hace de ella". Por eso pidió endurecer las penas.●

7

10 LA TERCERA Martes 26 de julio de 2011

País

▸▸ El subsecretario del ramo pidió indagar otros eventuales delitos. FOTO: MIRKO ALCOS

## Subsecretaría para las FF.AA. se querella por sabotaje informático

▶ Vulneración afectó al sistema de datos de funcionarios pensionados. **Archivos no fueron alterados.**

▶ Desde la cartera, **el tema fue calificado como "sensible"** ante un eventual nuevo ataque.


***Sebastián Labrín***
*Santiago*

Un ataque "al sistema documental" de la Subsecretaría para las Fuerzas Armadas motivó que el titular del ramo, Alfonso Vargas Lyng, presentara, el 22 de junio pasado, una querella ante el 17° Juzgado de Garantía de Santiago, por el delito de sabotaje informático.

En el libelo se explica que el ataque se llevó a cabo el 29 de marzo, entre las 0.30 y la 1.05, pero los funcionarios sólo se habrían percatado a eso de las 8.00, cuando símbolos y figuras geométricas daban la bienvenida al sitio web, según detallaron fuentes de la cartera.

Los responsables de vulnerar la seguridad de la página se identificaron con los seudónimos de "JaCKal" y "Mafia Hacking Team". No conforme con ello, publicaron su "hazaña" en el sitio web www.zone-h.org, dedicado a publicitar este tipo de ataques en la red.

**"Tema sensible"**

En la querella se revela que el hecho afectó al "sistema de tratamiento de información de la ex Subsecretaría de Guerra, donde se encuentra alojado parte del sistema documental de la Subsecretaría para las Fuerzas Armadas".

Desde la cartera explicaron que en dicho sistema interno -al cual no tienen acceso terceros- existen antecedentes relativos a pensiones de ex funcionarios, jubilaciones anticipadas y asignaciones familiares, los cuales no habrían sido adulterados ni destruidos por los intrusos.

Desde el interior de la subsecretaría y por la vulnerabilidad que demostró la seguridad del sitio, el tema fue calificado como "sensible". Ello, por la relevancia de los antecedentes que allí se manejan y la eventualidad de ser víctimas de un nuevo ataque a documentos en red.

Para despejar dudas, el subsecretario Alfonso Vargas pidió, a través de la querella, que el fiscal de delitos económicos, Mauricio Vergara, indague "todos aquellos delitos que se acrediten durante el curso de la investigación".

Junto con ello, instruyó a la coordinadora de la Unidad Jurídica de esa cartera, Susana Belmar, a "seguir de cerca" la indagatoria del Ministerio Público, para mantenerse informado de sus avances.

Desde la Fiscalía Centro Norte explicaron que los antecedentes se encuentran en poder de la Brigada Investigadora del Cibercrimen de la PDI, a la cual se le instruyó recabar los antecedentes para determinar si el ataque se produjo dentro o fuera del país.●

### Investigaciones por el delito crecen 40%

Un informe realizado por la Brigada Investigadora del Cibercrimen sostiene que, entre 2009 y 2010, las investigaciones por sabotaje y espionaje informático se han incrementado en 40%.

De acuerdo con el reporte, en 2009 se registraron 325 casos, mientras que, en 2010, llegaron a 456. Hasta junio de 2011 se han iniciado 275 investigaciones policiales relacionadas con este tipo de ilícitos.

De ese total, el 56%, es decir, 810 casos, ha terminado con resultados como la detención del responsable y su formalización. El otro 46% de las investigaciones no ha tenido resultados satisfactorios para las indagatorias.

El subcomisario del Cibercrimen, Javier Rodríguez, explica que este tipo de delitos ha registrado "una tendencia al alza". A ello añade que "las personas que cometen este tipo de delitos cada día están más especializadas y saben, a veces, cómo ocultar sus datos".

Debido a este incremento, la PDI realizó un perfil de los responsables de este tipo de delitos: se trata de profesionales con conocimientos en el área informática, o los denominados "nativos digitales", cuya motivación es el lucro, hacer daño a una entidad o demostrar sus habilidades frente a sus pares.

Según el policía, los objetivos de ingresar a una página de forma clandestina son "modificar, destruir o extraer" su información sensible.●

**EL SABOTAJE**

**Las consecuencias del ataque**

Por cerca de 14 horas se mantuvo inutilizable el sitio de la ex Subsecretaría de Guerra. Si bien el ataque se perpetró a eso de las 0.30 del 29 de marzo, sólo a las 14.00 del mismo día pudo volver a funcionar. En ese sitio -explicaron desde la cartera- se manejaban antecedentes de ex funcionarios pensionados.

**Orden para indagar otros delitos**

Debido a la vulnerabilidad que demostró el sitio, que actualmente depende de la Subsecretaría para las Fuerzas Armadas, el titular del ramo, Alfonso Vargas, pidió a la Fiscalía Centro Norte y a la PDI que indaguen otros delitos que, eventualmente, se cometieron antes de que se descubriera el acceso de desconocidos.

8

72 TENDENCIAS

LA TERCERA Domingo 9 de septiembre de 2007

LA TERCERA Domingo 9 de septiembre de 2007

**Delincuentes realizan robo de datos y otras acciones** en sitios de casinos y remates

# Hackers cambian de perfil y se especializan en fraudes y estafas

AIDA WORTHINGTON

**► Hoy ya no buscan fama ni encontrar el lado vulnerable de un sitio, sino que se organizan para amenazar a empresas con interrumpir sus redes, si no están dispuestas a pagarles las sumas que solicitan.**

Hace 25 años, Rich Skrenta, un chico de 15 años, creó el primer virus de computador. Se llamó Elk Cloner y se autorreplicaba e infectaba discos floppy, aquellos antiguos diskets flexibles de 5,2 pulgadas. Según ha declarado, lo hizo como broma para sus amigos.

Pero hoy con la penetración de internet, la cantidad de datos que circulan por la red y las transacciones que se realizan a diario, los *hackers* y creadores de virus no buscan reírse de alguien o ser conocidos, porque encontraron alguna vulnerabilidad en un sitio web:

**Extorsión**

Según el informe de Criminología de la empresa de seguridad informática McAfee, esta acción la realizan principalmente bandas cibernéticas y consiste en amenazas a empresas con la interrupción de sus redes o desconfiguración de sus sitios a cambio de un pago. También el criminal encripta los datos de un usuario y luego solicita dinero a cambio del envío de la clave para desbloquearlos.

**Lavado de dinero**

Fetzner explica que casinos y servicios financieros en internet están siendo usados para lavar dinero. Esto se realiza con transacciones aparentemente legítimas como apuestas, en que una persona apuesta mucho dinero y pierde, mientras otra apuesta poco y gana grandes cantidades.

En esta acción se usan mucho los cómplices, consumidores de estos sitios que según McAfee son reclutados y luego reciben dinero del ciberdelincuente. La suma se transfiere a una cuenta en el extranjero y el cómplice mantiene un porcentaje como honorario.

**Ataques BotNet**

Son redes de computadores que pueden ser controladas remotamente por otro PC. Estos *bots* son usados para ejecutar delitos, como mandar correo basura (*spam*), ejecutar estafas vía *phishing*, robar identidades o ejecutar ataques de denegación de servicio, en los que se satura una red enviando información que satura el ancho de banda. Fetzner menciona el ataque que recibió en abril Estonia, país que quedó sin sus principales sitios de internet por una semana debido a un ataque BotNet.

**Robo de identidad**

Los criminales cibernéticos extraen información personal de tarjetas de crédito, claves bancarias o bases de datos de una empresa, lo que luego es vendida, publicada o usada para realizar estafas. En Chile, según datos de la Brigada Investigadora del Ciber Crimen (Bricrib), durante 2007 este fraude representa el 8% de los delitos investigados, o sea el doble que en 2006.



**LOS PELIGROS** *que circulan en internet evolucionan constantemente y hoy se concentran en acciones como robo de identidad y lavado de dinero.*

## Nuevos delincuentes en internet

Según el informe Criminología McAfee 2007, este año han surgido nuevos perfiles de delincuentes cibernéticos:

►**Cybermules**: Sirven como "palos blancos" y reciben dinero obtenido en un fraude por internet y se lo transfieren a sus jefes *hackers*, a cambio de una pequeña recompensa.

►**Carders**: Se concentran en el robo de tarjetas de crédito. Tienen comunidades de chat privadas y encriptadas.

►**Cyberpunks**: Usan sus habilidades para entrar a sistemas y redes computacionales. No siempre persiguen dinero y muchos realizan cibergraffitis, que consisten en alterar sitios web.

EMAILS DE INSTITUCIONES FALSAS

## El phishing sigue siendo efectivo

Aunque ya es conocido, sigue dando resultados. Cada mes el Antiphishing Working Group recibe más de 24 mil reportes de fraudes de este tipo. Se trata de emails que provienen de una institución falsa, pero que tienen el aspecto de ser de parte de una empresa financiera real.

Este delito se ha vuelto cada vez más sofisticado y usa técnicas sicológicas como anunciar que la cuenta ha sido suspendida y pedir claves de usuario para reactivarla. También, añade Marlon Fetzner, se está usando para instalar troyanos en el PC. Esto haciendo que el usuario baje una nueva versión de un programa como messenger, pero derivándolo a una página falsa e instalando un programa que le roba información. Pese a que existen varios *softwares* en el mercado, lo primordial es que ser cuidadoso al abrir un sitio y no confiar en un mail que solicite claves privadas.

## Ley 19.223
## Tipifica figuras penales relativas a la Informática

**Análisis de la Ley**
- Sujeto activo
- Parte Subjetiva
- Parte Objetiva
- Figuras Penales

1.-El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento.

2.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de información, lo intercepte, interfiera o acceda a él.

3.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

4.- El que maliciosamente revele o difunda los datos contenidos en un sistema de tratamiento de información. Si quien incurre en estas conductas es el responsable del sistema de tratamiento de información se aumenta un grado.

**Sabotaje**

**Espionaje**

# Delitos Informáticos y Delitos Informatizados

**Delitos Informáticos:**

➢Son los delitos donde el bien jurídico protegido son los sistemas de tratamiento de la información, que se encuentran tipificados en la Ley 19.223.

**Delitos Informatizados:**

➢ Son delitos en donde el bien jurídico protegido NO son los sistemas de tratamiento de la información, pero que fueron cometidos con apoyo de tecnologías de la información. Ejemplos: Propiedad Intelectual, Falsificación de Documento Publico y Privado, Estafas vía Internet, etc.

## Defacement

Detalle de la información | Suscríbete

**Justicia determina pena de presidio remitido para "crackers" chilenos**

**Tras acreditarse su responsabilidad en la intervención de sitios web estatales y privados, un tribunal de Santiago condenó a Carlos Amigo León y Leonardo Hernández, a tres años de presidio remitido por su implicancia en el delito reiterado de sabotaje informático.** 15.05.2007, 16:55

**Mouse / Agencias**.- Por infracción al artículo primero de la Ley de Delitos Informáticos, el Tercer Tribunal Oral de Santiago condenó a tres años de presidio remitido a dos piratas, que formando parte del "Byond Hackers Team" intervinieron cerca de 8 mil sitios, incluido el de la agencia espacial estadounidense (NASA).

El tribunal presidido por jueza Anaclaudia Gatica determinó que Carlos Amigo León (37) y Leonardo Hernández (25) efectivamente participaban desde hace varios años en el "defacement" de sitios. Sin embargo, debido a la baja pena de los delitos asignados, se les concedió la libertad con firma mensual en Gendarmería.

El tribunal acogió también la demanda del canal de televisión "Mega", cuyo portal fue uno de los afectados, por lo que Amigo deberá pagar 2 millones de pesos como indemnización por perjuicios.

"SSH2" y "Nettoxic", nicks utilizados por Amigo y Hernández, atacaban sitios desde la localidad de Buin junto a dos gemelos menores de edad, que sólo quedaron a disposición de un tribunal de familia.

Al término de la audiencia, ambos condenados consideraron injustos los cargos imputados, convencidos de que no causaron daño a nadie y que sólo demostraron públicamente sus conocimientos en esta área.

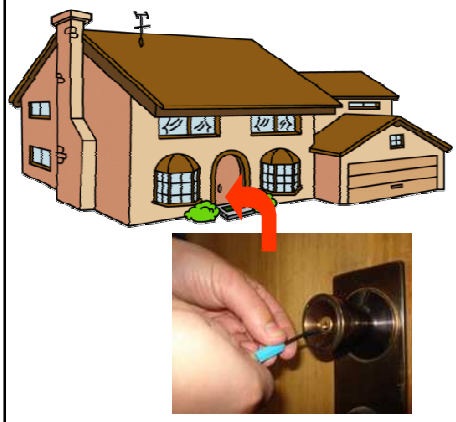
Agrega tu comentario

Fuente: www.mouse.cl ( http://www.mouse.cl/detail.asp?story=2007/05/15/16/55/06 )

es una palabra inglesa que significa desfiguración y es **un término usado en informática para hacer referencia a la deformación o cambio producido de manera intencionada en una página web por un atacante** que haya obtenido algún tipo de acceso a ella, bien por algún error de programación de la página, por algún bug en el propio servidor o por una mala administración de este.

Fuente : http://es.wikipedia.org/wiki/Defacement

**Mundo real**



**Mundo virtual**


# Phishing (I)

C 14 NACIONAL EL MERCURIO DOMINGO 21 DE NOVIEMBRE DE 2010

## Estafadores intervenían cuentas bancarias con la ayuda de *hacker* peruano

Por una serie de estafas a través de correos electrónicos —usando la técnica llamada *phishing*— fueron detenidos por el OS-9 de Carabineros tres presuntos estafadores. Se trata de Ernesto José Mardones Díaz (21), Franco Jacobo Hermosilla Céspesdes (20) y Camila Andrea Lara Hernández (19). Éstos enviaban *e-mails* a sus víctimas simulando operaciones bancarias para conseguir sus datos personales y utilizar sus cuentas para transferir el dinero. Carabineros estableció que el líder de la organización era un *hacker* de nacionalidad peruana. Según la policía, Mardones reclutó a Hermosilla y a Lara para que recibieran las remesas. Su aprehensión, ocurrida el viernes, se originó luego que la víctima J.R.C.D. (41) denunciara que habían sustraído $1 millón 600 mil desde su cuenta. Los detenidos devolvieron voluntariamente $911 mil.

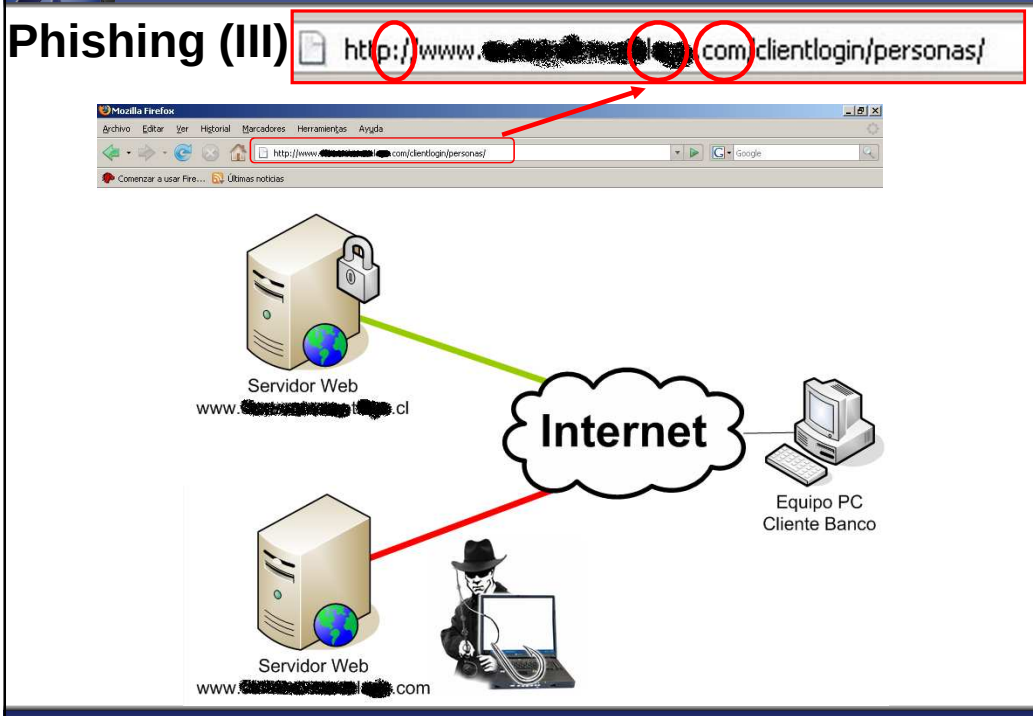
# Phishing (II)

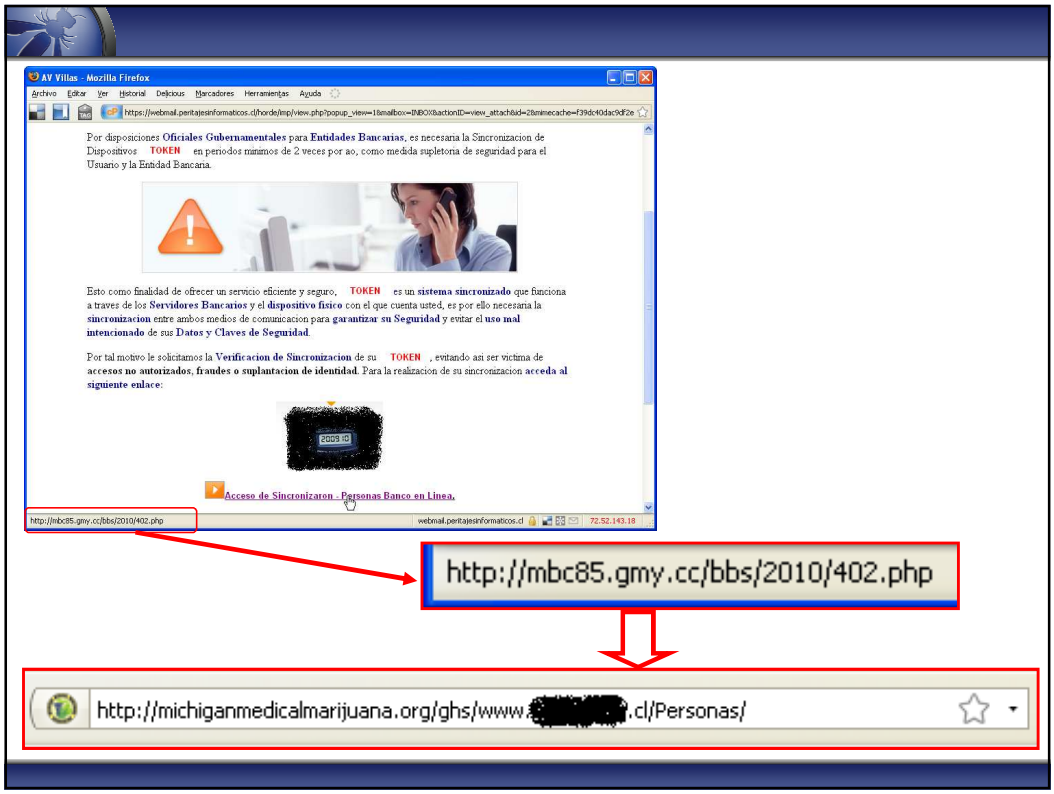
From: soporte@XYZ.cl

ESTIMADO CLIENTE BANCO XYZ
Durante nuestro mantenimiento regular y procesos de verificación, hemos detectado un error en la información que tenemos registrada de su cuenta. Esto se debe a algunos de estos factores:
1. Un cambio reciente en su información personal (cambio de dirección, etc.)
2. Que usted haya proveído información invalida durante su proceso inicial de registro para bancanet o que usted aun no haya realizado dicho registro.
3. Accesos a su cuenta a través de Banca en Linea que han sido realizados desde diferentes direcciones IP. Esto seguramente se debe a que la direccion IP de su PC es dinámica y varía constantemente, o debido a que usted ha utilizado mas de un computador para acceder a su cuenta.
Para verificar la actividad de la misma y omitir el proceso de baja, debe ingresar a su cuenta a través de Banca en Linea haciendo click en el enlace que corresponda a su tipo de cuenta:
Para Personas: https://www.xyz.cl/login.asp?yes=pers
http://www.xys.com/clientlogin/personas
Para Empreas: https://www.xyz.cl/login.asp?yes=emp
http://www.xys.com/canales/empresas/
:
SI la información en su cuenta no se actualiza en las siguientes 12 horas, algunos servicios en el uso y acceso a su cuenta serán restringidos hasta que esta información sea verificada y actualizada.

_____
Todos los Derechos Reservados 1998-2006 Grupo XYZ

# Phishing (III)





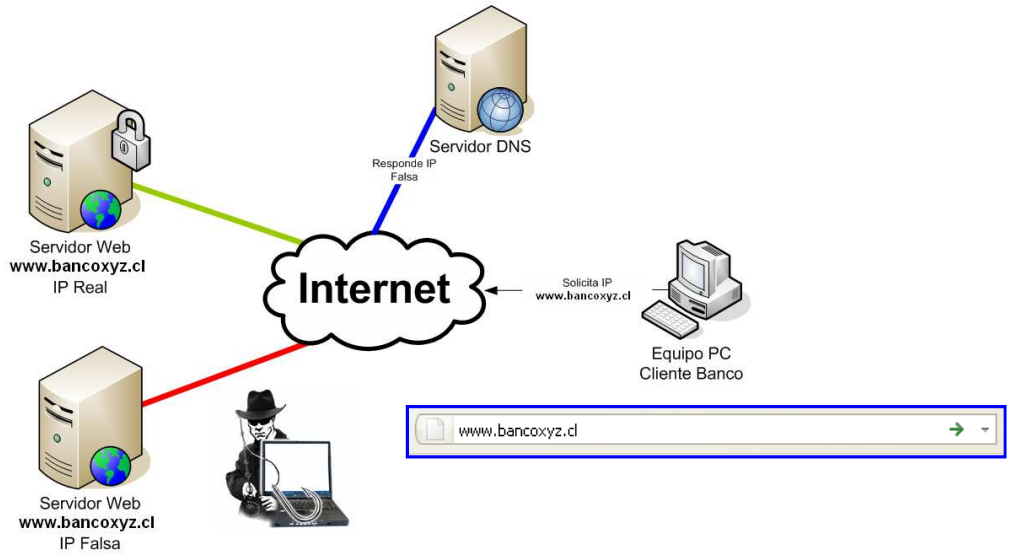

# Herramientas OWASP

Permiten aplicar buenas prácticas que mitigan el riesgo.

**Guias**

- Libros en Codificación Segura y Revisión de Código.

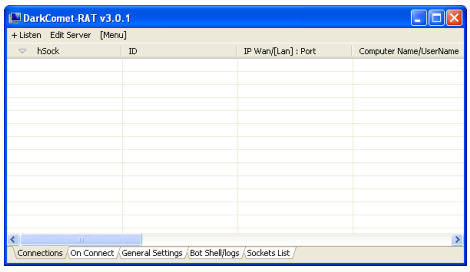
# Pharming (I)

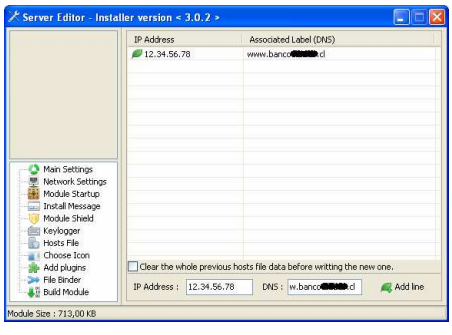



# Pharming
# Alternativa (II)

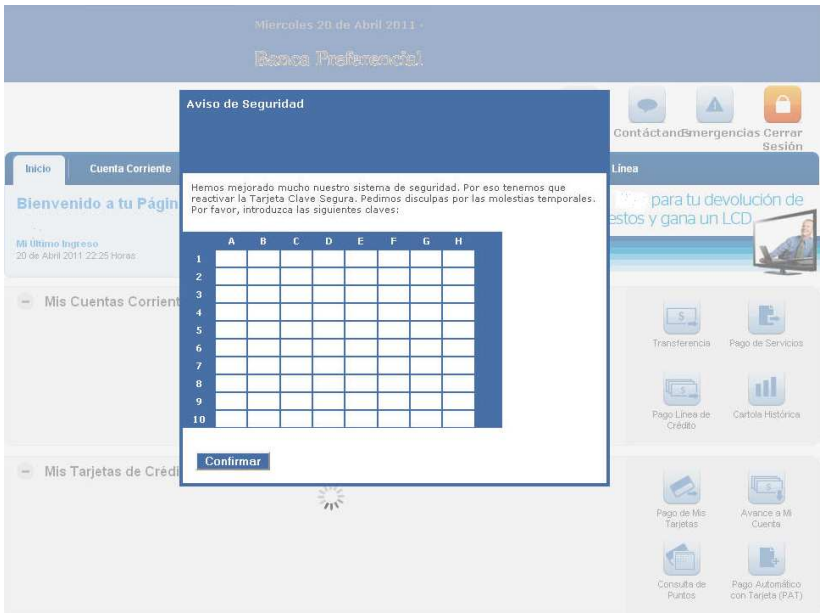
- C:\WINDOWS\system32\drivers\etc\hosts

Ejemplo en creación de Malware



# Nueva Modalidad de Fraude




## INFORMATICA FORENSE

Área de la informática que es auxiliar de la justicia en los ámbitos legales correspondientes a la informática.

Según FBI, es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y almacenados en un medio computacional.

(http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm)

## Importancia de la prueba en el proceso penal (CPP).

Artículo 340.- Convicción del tribunal. Nadie podrá ser condenado por delito sino cuando el tribunal que lo juzgare adquiriere, más allá de toda duda razonable, la convicción de que realmente se hubiere cometido el hecho punible objeto de la acusación y que en él hubiere correspondido al acusado una participación culpable y penada por la ley.

**El tribunal formará su convicción sobre la base de la prueba producida durante el juicio oral.**

No se podrá condenar a una persona con el solo mérito de su propia declaración.

## Prueba

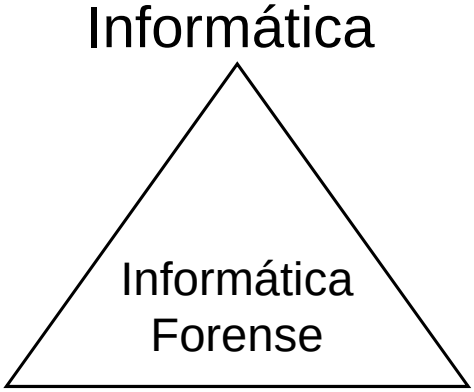
Justificación de la verdad de los hechos controvertidos en un juicio, hecha por los medios que autoriza y reconoce por eficaces la ley.

DICCIONARIO DE LA LENGUA ESPAÑOLA - Vigésima segunda edición

# Ciclo de la Prueba


| Señales, Rastros o Indicios | Evidencia | Prueba |
|---|---|---|
| Elementos, objetos o registros que se encuentran en el Sitio del Suceso y podrían ser de interés para el hecho investigado. | Elementos, objetos o registros levantados, embalados y rotulados desde el Sitio del Suceso. | Elementos, objetos o registros que son presentados en un juicio para crear convicción de un hecho. |

# Aspectos involucrados en la Informática Forense



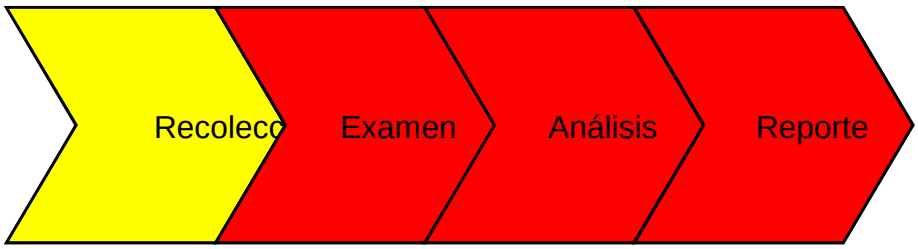

**Criminalística**

Metodología de trabajo en Sitio del Suceso.
Principios de la Criminalística.
Tratamiento de la Evidencia.

**Legislación**

Define marco legal de acción.
Derechos constitucionales.

## Etapas de la Informática Forense




| | | | |
|---|---|---|---|
| La evidencia es identificada, etiquetada, registrada y recolectada. | Se extrae la información de los dispositivos. | Se verifica la información y se selecciona aquella que es relevante para la investigación. | Se informa sobre lo efectuado. |

**Importante**: Durante todas las etapas la evidencia se debe mantener sin ningún tipo de modificación o alteración

## SITIO DEL SUCESO COMPUTACIONAL

Ante un delito podrían encontrarse diferentes ubicaciones geográficas pertenecientes al sitio del suceso computacional.

1. En primera instancia, están los lugares en que el delincuente utilizó un computador con el cual da inicio al delito.
2. Otro lugar que puede formar parte del sitio del suceso computacional es aquel en el cual se encuentra el objeto del delito.

# SITIO DEL SUCESO COMPUTACIONAL

3. En varios de los delitos vistos, se puede apreciar que para llevar a cabo un delito se necesita de un tercero donde se puedan alojar páginas web, se pueda dar el servicio de foros, se tenga un servicio de correo electrónico y en general, donde puedan alojarse y compartirse archivos.
4. Para los delitos en los que el medio utilizado es Internet, se tiene otro lugar perteneciente al sitio del suceso computacional no comentado antes, correspondiente a los proveedores de conexión a Internet.

# SITIO DEL SUCESO COMPUTACIONAL

# Principio de Intercambio de Locard

## y su aplicación en la Informática

El atacante utiliza herramientas “creadas” por si mismo al realizar un ataque