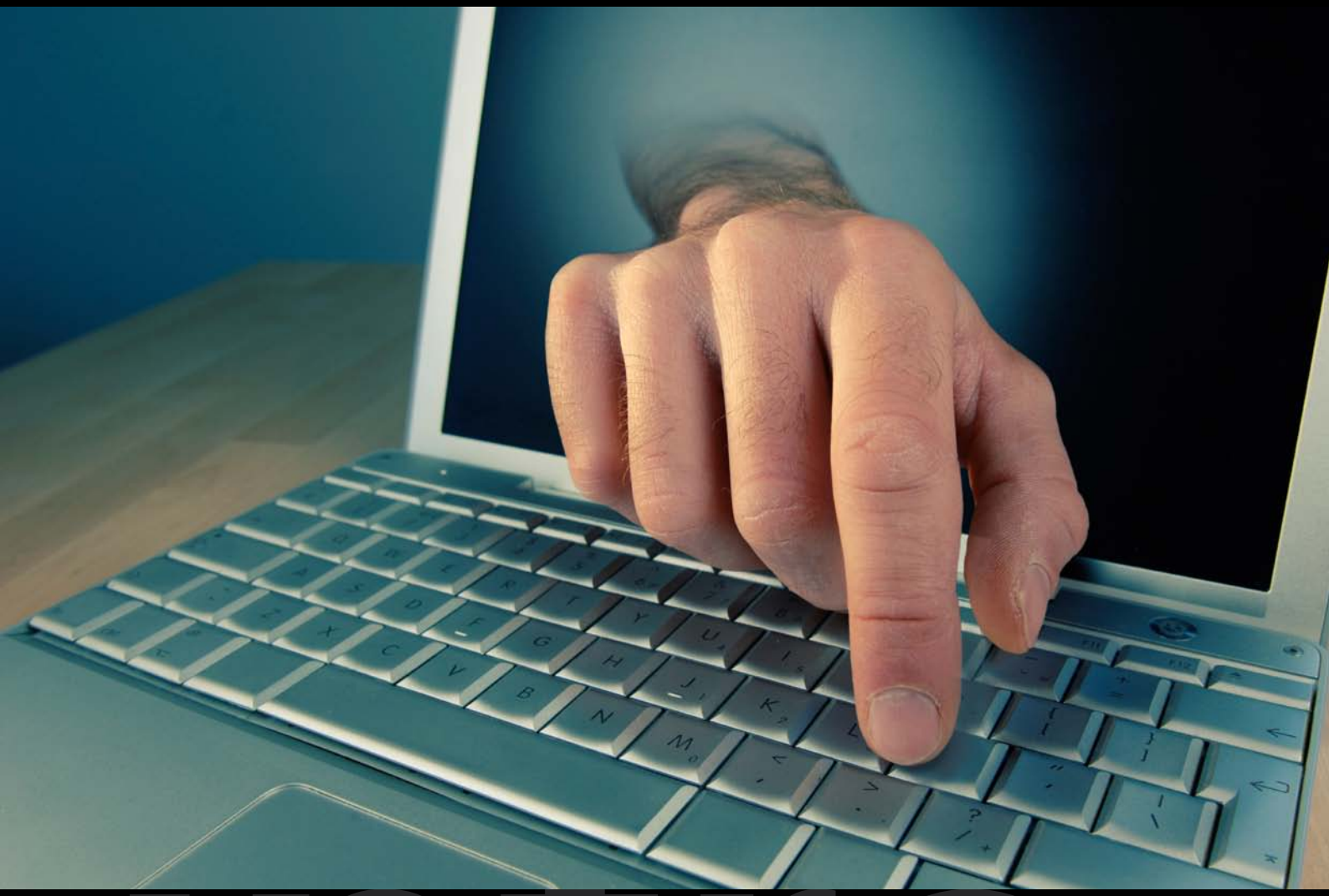
EL MERCADO NEGRO DEL CIBERCRIMEN AL DESCUBIERTO

PANDA SECURITY | *The Cloud Security Company*

ÍNDICE



intro

1. Introducción

Todo un negocio redondo, anónimo y sin duda muy rentable que seguramente estará dando de comer a muchas familias, eso sí, de forma fraudulenta y robando a los demás. desde la comodidad de un despacho o una habitación en casa, con sólo un ordenador como herramienta y amparados por la falta de regulación legislativa internacional y la ausencia de cooperación entre muchos países que facilite la investigación y la detención, estos cibercriminales llevan mucho tiempo viviendo de un negocio que, sin duda, promete ser muy lucrativo.

Muchas personas del equipo de Panda Security nos dedicamos a viajar y a asistir a eventos de todo tipo: tanto de la industria en sí como de otro tipo enfocados a empresarios, a usuarios finales, etc. Y aún a pesar de que afortunadamente cada vez se da más a conocer detenciones de hackers que se dedican a robar datos y a "hacer su agosto" con ellos de diferentes maneras, todavía hay público, no necesariamente dedicado al ámbito de la seguridad, que atónitos nos preguntan: "¿y a mí para qué quieren robarme información? No tengo nada de interés…"

Otro factor a tener muy en cuenta es que el malware actual destinado al robo de datos está especialmente diseñado para no hacerse notar, de forma que muchos nos daríamos cuenta de que hemos sido víctimas de este tipo de ataques cuando nos llegara el extracto del banco o de nuestra cuenta de Paypal.

Además, la percepción que se tiene es que éste es un problema que sólo afecta a usuarios domésticos, como si las empresas fueran inmunes. Pero el resultado de nuestras investigaciones, como podrás leer más adelante, demuestran que no es así: **hoy en día nadie –ni usuario doméstico ni empresa- es inmune ante el robo de información confidencial y su posterior venta**.

Y todo ello contando con que la concienciación y la educación en seguridad del público en general, indudablemente, ha aumentado en los últimos años, gracias a la labor de las autoridades gubernamentales de diferentes países, por supuesto, gracias a la industria de la seguridad y a otro tipo de entidades, instituciones, organizaciones, asociaciones, medios de comunicación, blogs, etc., que llevan ayudándonos a realizar esta labor desde hace bastante tiempo.

Además, aunque no hay datos exactos, creemos que este tipo de negocio ha proliferado con la crisis económica. Así como antes era realmente complicado llegar a localizar sitios o personas que se dedicaran a este tipo de negocio, ahora no es tan difícil encontrar ofertas en diferentes foros underground.

Y donde sin duda se nota la necesidad de dinero de estas mafias es en la proliferación de ofertas de venta, en la guerra de precios y en la diversificación de negocio. Hace unos años, sólo vendían unos pocos datos de tarjetas de crédito. Ahora, además de que ofrecen hasta la fecha de nacimiento de la mascota familiar de la víctima robada, se ofrecen a realizar otro tipo de servicios en nombre del comprador, como duplicar físicamente las propias tarjetas o realizar compras anónimas y enviarlas al domicilio del ordenante.

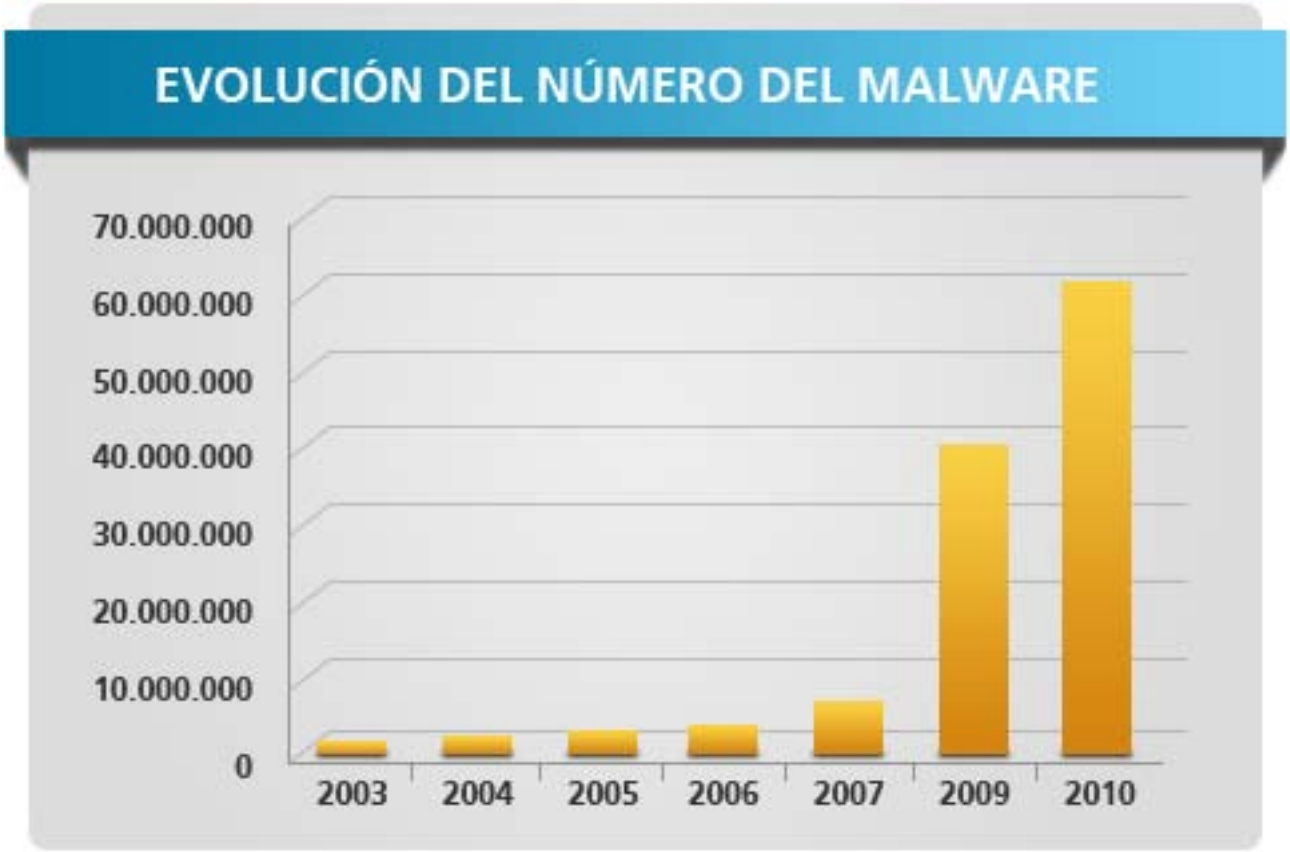
2. La evolución del malware enfocado al robo de datos bancarios

El auge del mercado negro dedicado a la venta de datos personales tiene su sentido si echamos un vistazo a los datos de evolución del malware de forma global o al crecimiento de las amenazas informáticas específicamente diseñadas para conseguir datos bancarios, en particular.

Que el malware está aumentando de forma exponencial en los últimos años es un hecho innegable acerca del cual las compañías de seguridad llevamos informando desde hace ya un tiempo. Si hace unos años hablábamos de 500 nuevas amenazas informáticas que se creaban al mes, actualmente, **PandaLabs, nuestro laboratorio anti-malware, recibe una media de 63.000 nuevas amenazas diariamente**. Y este número no es el total de todo lo que se crea, sólo lo que nos llega a nosotros.

Esto da como resultado no sólo un crecimiento exponencial, sino una tendencia que sigue al alza: si en 2009 cerrábamos el ejercicio con casi 40.000.000 de amenazas clasificadas en nuestra base de Inteligencia Colectiva, en 2010 hemos sido capaces de almacenar conocimiento de más de 20.000.000 más. Es decir, ya contamos **con más de 60.000.000…**

Hace cinco años, sólo había 92.000 ejemplares de malware clasificados tras 15 años de historia de la compañía. Esta cifra pasó a 14 millones en 2008 y a 60 en 2010, lo que, sin duda, supone un gran ratio de crecimiento.



El motivo de este espectacular aumento está claro: el dinero. El año 2003 supuso el nacimiento de los troyanos bancarios y el polimorfismo. Es decir, el crear tantas variantes de las amenazas como pueden para evitar ser detectados por el antivirus… ya que si éste es detectado, evidentemente, se quedan sin opción a infectar y a robar. Desde entonces, estos códigos maliciosos se han convertido en una de las formas más habituales de malware.

Cada día salen a la luz nuevas variantes que han evolucionado tecnológicamente para esquivar las medidas de seguridad de los bancos, tiendas online, pasarelas de pago, etc. Varias organizaciones han intentado unir a los diversos miembros de la industria de seguridad informática para contrarrestar los esfuerzos de los cibercriminales. Sin embargo, se trata de una batalla larga y dura, y ni siquiera está claro si podremos ganarla alguna vez.

En general, el motivo de que se creen más troyanos, keyloggers y bots que ningún otro tipo de malware es porque resultan los más útiles para el robo de identidad. En el año 2005, casi la mitad de los nuevos códigos maliciosos eran troyanos:

Al cierre de 2010, la situación es mucho peor, ya que los troyanos suponen más del 71 por ciento del nuevo malware.

Al igual que en cualquier otro negocio, los delincuentes informáticos buscan operar de la forma más eficaz posible. A la hora de desarrollar un troyano, deben decidir qué plataformas soportará y el número de víctimas potenciales. Windows es la plataforma atacada en más del 99 por ciento de los casos, siendo también la que más usuarios tiene hasta la fecha.

El objetivo final de los delincuentes es obtener beneficio económico del malware. Los troyanos son la herramienta perfecta para robar información. Sin embargo, dicha información debe convertirse en dinero contante y sonante, y los criminales continuamente investigan y buscan métodos innovadores para conseguirlo.

3. Cómo funciona el mercado negro

Según el FBI, las organizaciones cibercriminales funcionan como empresas, contando con expertos especializados para cada tipo de trabajo y ocupación. A diferencia de una organización empresarial, estos cibercriminales trabajan sin horarios, sin vacaciones y sin fines de semana.

Cuando hablamos de Mercado Negro, más parece un título de una novela negra de espionaje o gangsters que de una situación real que, aunque no a la vista de todo el mundo, está sin duda marcando el rumbo de toda la industria de la seguridad.

Pero… ¿qué es realmente el llamado "Mercado Negro" y cómo opera? ¿Cuáles son sus responsables? ¿Cuál es el proceso a partir de la creación de un troyano por el cual éste se distribuye, se consigue dinero, se blanquea y pasa a manos de indeseables?

Veamos, primero, qué tipo de figuras encontramos en lo que llamamos cibermafias criminales.

Las profesiones cibercriminales

En numerosas ocasiones hemos hecho referencia a que las mafias de ciberdelincuentes que operan en Internet están muy organizadas, tanto desde el punto de vista de visión estratégica como desde la operativa, logística y despliegue de sus operaciones. Y, además, no sólo pueden parecer verdaderas compañías, sino que son organizaciones multinacionales, ya que operan a lo largo y ancho del planeta.

Recientemente, el FBI ha hecho pública la "clasificación" de las diferentes "profesiones" que están encontrando en el mundo de los cibercriminales, en un intento de tipificar las figuras más comunes que podemos encontrar en el proceso mafioso de generar dinero mediante el robo, la extorsión y el fraude a través de Internet.

Así, las "profesiones" o especializaciones más comunes que tipifica el FBI son las siguientes:

1. Programadores. Desarrollan los exploits y el malware que se utiliza para cometer los cibercrímenes.

2. Distribuidores. Recopilan y venden los datos robados, actuando como intermediarios.

3. Técnicos expertos. Mantienen la infraestructura de la "compañía" criminal, incluyendo servidores, tecnologías de cifrado, bases de datos, etc.

4. Hackers. Buscan aplicaciones exploits y vulnerabilidades en sistemas y redes

5. Defraudadores. Crean técnicas de ingeniería social y despliegan diferentes ataques de phishing o spam, entre otros.

6. Proveedores de hosting. Ofrecen un entorno seguro para alojar contenido ilícito en servidores y páginas.

7. Vendedores. Controlan las cuentas y los nombres de las víctimas y las proveen a otros criminales mediante un pago.

8. Muleros. Realizan las transferencias bancarias entre cuentas de banco.

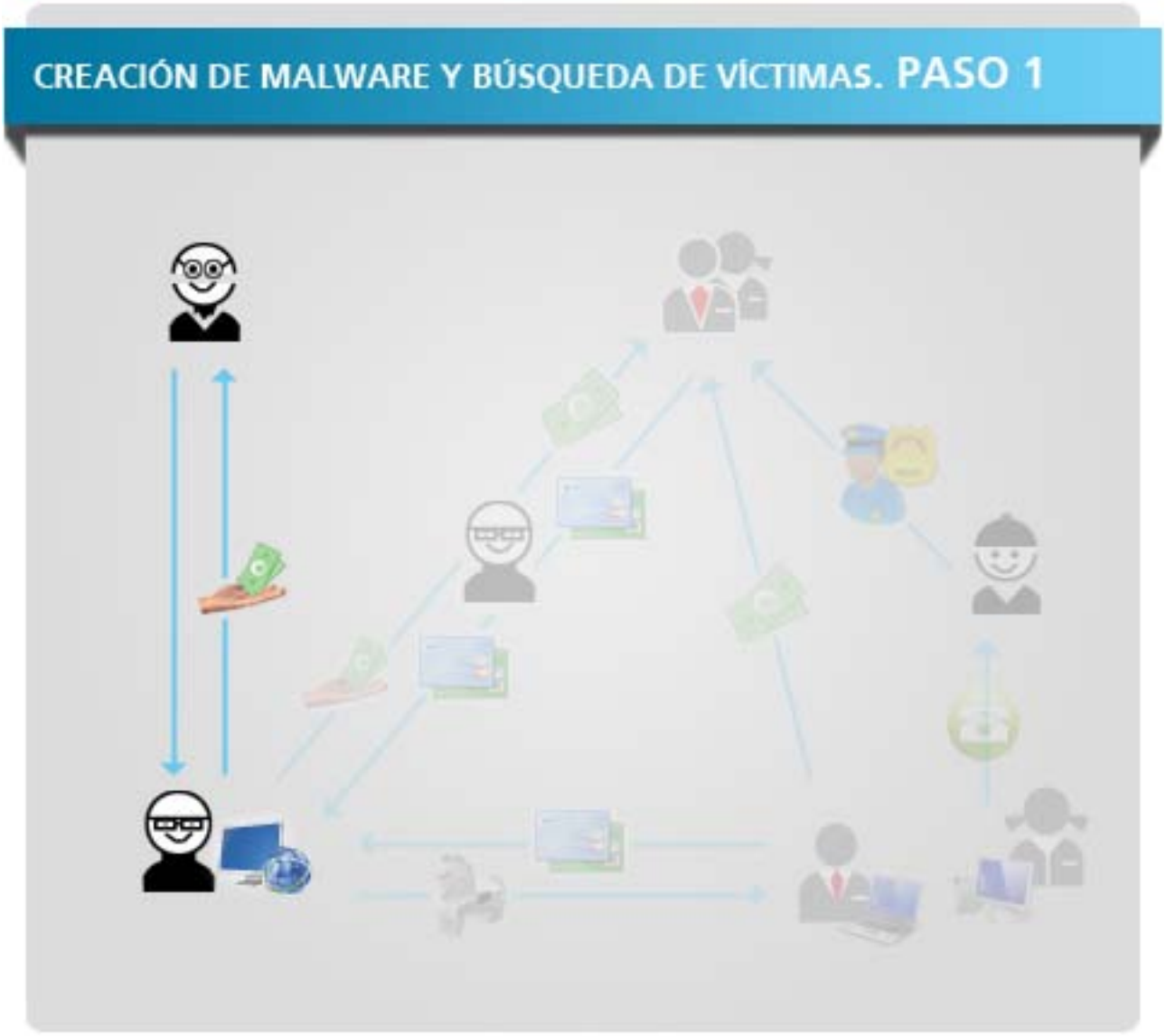
9. Blanqueadores. Se ocupan de blanquear los beneficios.

10. Líderes de la organización. Frecuentemente, personas normales sin conocimientos técnicos que crean el equipo y definen los objetivos.

Las organizaciones cibercriminales se organizan, además, de forma jerárquica, y cada paso diferente de la cadena cuenta no con uno, sino con varios especialistas. Si pensamos que la operativa de producción se despliega en numerosos países, podemos tener una idea bastante cercana de cuántas personas, beneficiándose del anonimato de Internet, pueden llegar a estar implicadas en estas redes mafiosas…

El proceso…

Paso 1. Creación de malware y búsqueda de víctimas



Todo comienza en las cabezas de los líderes de la organización, que encargan a programadores y a hackers, junto a técnicos expertos, el llevar a cabo ataques indiscriminados. Estas figuras pueden actuar de forma independiente o coordinados entre sí, y también una serie de personas pueden asumir diferentes roles a la vez.

De este proceso hemos hablado en numerosas ocasiones, y realmente ofrece pocas novedades desde el punto de vista de metodología. **En general, los hackers de la organización encargan a otros hackers (o en ocasiones lo hacen ellos mismos) la creación de troyanos, phishing, bots, spam, falsas webs para indexarlas en motores de búsqueda, etc.**

Una vez realizadas, las distribuyen utilizando métodos de ingeniería social para engañar a sus víctimas utilizando los vectores de distribución más populares: el correo electrónico sigue siendo uno de ellos, pero ahora está muy de moda usar las redes sociales (como Facebook, YouTube, MySpace, Twitter, etc.) e indexar falsas páginas web posicionadas con términos de búsqueda populares (los conocidos como ataques de BlackHat SEO).

El carácter libre e internacional de la red favorece varios factores:

- El nuevo malware puede ser creado y distribuido en cuestión de minutos, gracias al uso que hacen de kits ya preparados, a la compra online de dichas amenazas informáticas y a la sencillez con la que un mensaje con un poco de gancho puede llegar a distribuirse utilizando vectores de propagación populares.

- Se pueden crear muchas amenazas en diferentes idiomas o utilizar el inglés como idioma común, pero las víctimas que alcancen sus creadores pueden ser de muchos países diferentes.

Ya hemos comentado anteriormente que la plataforma más ampliamente atacada es Windows, ya que es la que ofrece la mayor masa de usuarios utilizando todo tipo de servicios online: banca, compras, pasarelas de pago, etc., aunque el mercado Apple comienza a ser atractivo debido a la cuota de mercado que está consiguiendo en los últimos dos años, gracias a los lanzamientos de sus periféricos (iPad, iPhone, etc.).

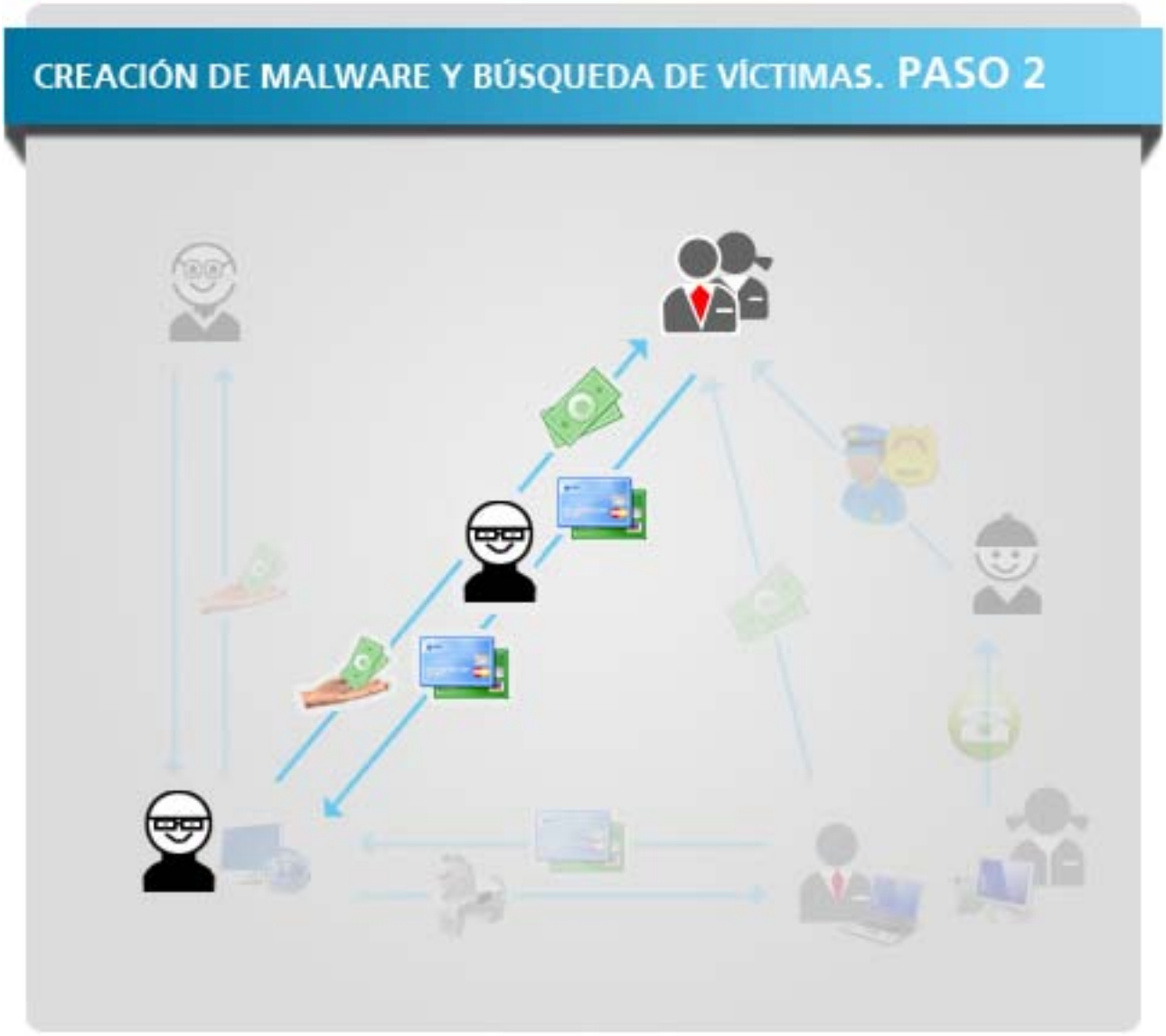
Una vez han conseguido engañar a la víctima y conseguir sus datos bancarios, de tarjetas, etc., éstos se suelen almacenar en un servidor al que los hackers tienen acceso, disponiendo desde ese momento de total acceso a las cuentas de víctimas que, de momento, ignoran que su intimidad ha sido vulnerada.

Paso 2: venta de datos y blanqueo de dinero

La pregunta más habitual que nos podemos hacer es: si estos cibercriminales ya tienen los datos bancarios, ¿no sería más sencillo que ellos mismos robaran de las cuentas y se quedaran con el dinero? Pues en muchas ocasiones, así sucede, pero no es lo habitual.

Muchos de estos datos acaban en el mercado negro, o bien se distribuyen a comerciantes minoristas que se encargan de su venta. La lectura es bien sencilla:

- Es menos arriesgado traficar con los datos que realizar el robo de forma directa.
- Habitualmente, el delito se comete en un país diferente a donde se consiguen los beneficios: cuantos más intermediarios haya en la cadena, más se diluyen las pistas para perseguir el delito.
- Además, a estas organizaciones se les da pie para la venta de otro tipo de servicios que no son necesariamente la venta en sí de los datos, como veremos más adelante.



Una vez los datos están en el mercado, los minoristas son los que se encargan de su venta. Lo curioso es que este mercado es exactamente el mismo a través del cual contrataron a los hackers originalmente o compraron los troyanos, o bots, o los kits…

Este tipo de mercado tiene todos los ingredientes necesarios para satisfacer la ley de la oferta y la demanda: compiten en precios, ofrecen servicios añadidos, dan pruebas sin compromiso, garantizan la devolución si los datos no son operativos (o si la cuenta no tiene un capital mínimo garantizado)… incluso hacen compras anónimas para los vendedores.

A través de post publicados en sitios a los que no es fácil llegar se lanzan las ofertas, y los potenciales criminales que quieren hacer uso de dicha información (tanto de numeraciones como de bandas magnéticas copiadas) para duplicar tarjetas físicas con las que operar en cajeros, robar el dinero directamente mediante transferencias o realizar compras, acuden contactando con métodos indetectables hasta conseguir la mercancía.

Aquéllos que optan por la opción de robar dinero directamente de las cuentas, mediante transferencias bancarias en la mayoría de las ocasiones y por cantidades notables, se ven muchas veces obligados a añadir un eslabón más en la cadena: buscar muleros que tengan a bien prestarse para su blanqueo.

Así, lanzan falsas ofertas de trabajo donde ofrecen sueldos o comisiones altos (entre un 3 o un 5% del total de dinero a blanquear) por el mero hecho de recibir dinero en una cuenta bancaria y hacer un envío a través de servicios como Western Union. Estas víctimas, en muchas ocasiones, no saben que lo son, ya que sólo ven beneficios en un trabajo tremendamente sencillo.

EJEMPLO: FALSA OFERTA DE EMPLEO

We are happy to inform you that at the moment we have one vacancy available:

Financial Reporting Manager.

The global network of our Financial Reporting Managers ensures that the highest level of our services and operations is guaranteed to our customers in every region of the world. Our highly trained brokers and accountants work 24/7 to monitor the Commodity markets.

Financial Reporting Manager responsibilities include:
- Holding accounts with certain banks or payment systems;
- Reception and processing of payments;
- Creating reports;
- Providing support to our customers;
- Following the instructions of the Company.

Working process:
You process the transfers from our customers with wire transfers, checks, money orders or any other express payment system like Money Gram, Travelex and etc. All transfers to your bank account are made by USA/North American and sometimes European investors (our business associates). Initially the transfer method is always chosen by our customer.

Payment:
Your basic salary equals the amount of 3,000 EUR (payment method: wire transfer, direct deposit or paypal transfer in the end of every working month) + commission. Financial Reporting Manager?s commission depends on the total amount of the payment orders processed.
In the beginning your commission equals 3 % from the total payment order amount. It is possible to raise your commission percentage up to 5% if you prove to perform the job promptly, with no delays and, what matters the most, with outstanding efforts.

If you are interested in this vacancy, please respond as soon as possible. As soon as we hear back from you, we will send you all further details regarding the vacancy available at the moment.

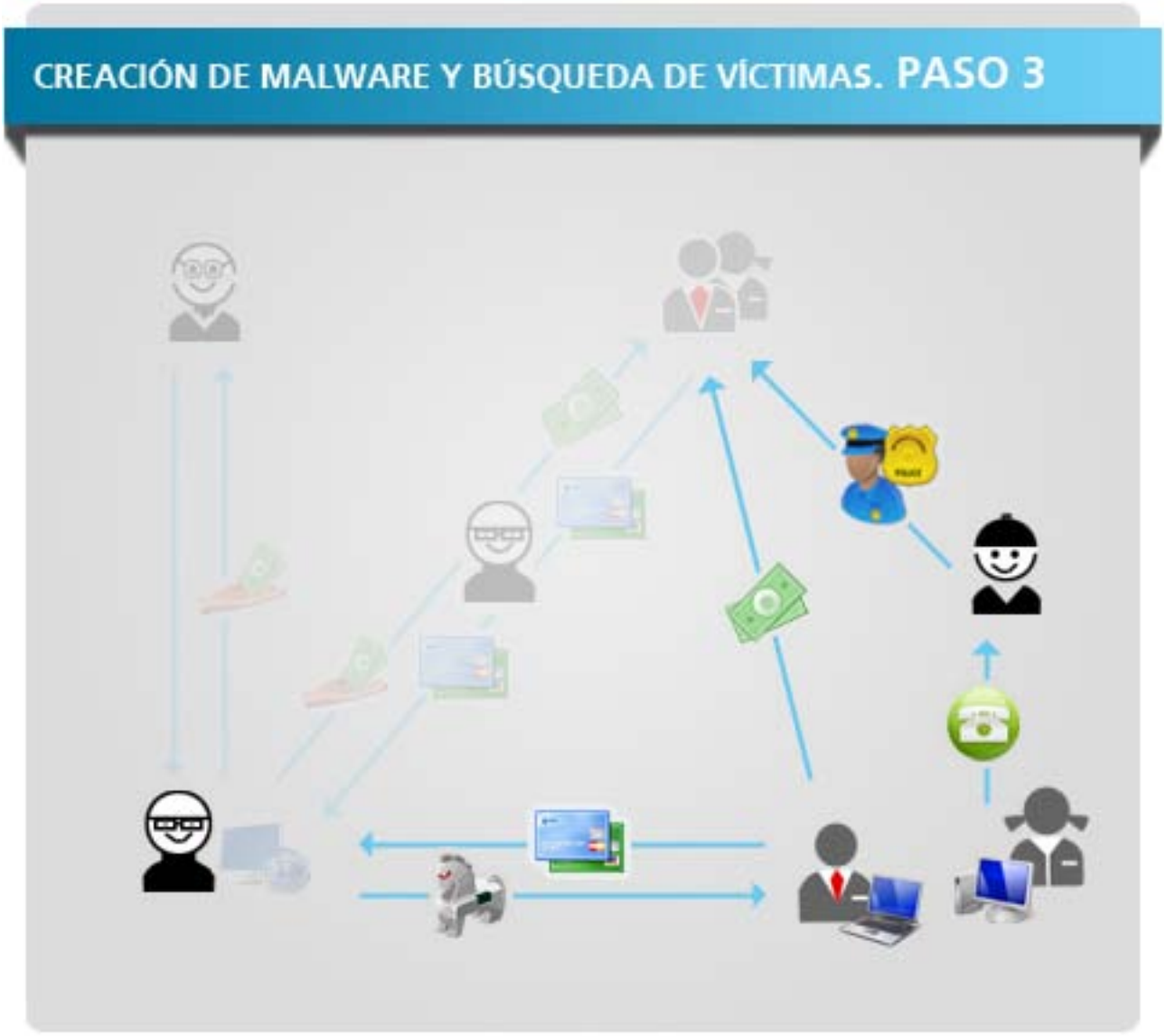
Please reply ONLY to our e-mail: chris.departmentama@gmail.com

We look forward to hearing from you soon

Thank You for Your time and for your attention

Yours faithfully,
Joseph Smith
Hiring Department of Advanced Management Associates

Para los criminales, el añadir otro eslabón en la cadena (y habitualmente en otro país diferente) hace que las pistas se diluyan todavía más, y además ponen cabezas de turco en medio que pueden servir de objeto de detención en el caso de investigaciones forenses.



Estos muleros no suelen estar mucho tiempo en activo, ya que cuando las víctimas denuncian el robo de dinero de sus cuentas y se investiga, la única cuenta que figura como receptora de la transacción es la del mulero, y a partir de ahí, se pierde totalmente el rastro…

4. El mercado negro de un vistazo

A modo de ficha, a continuación ofrecemos de un vistazo las principales características del funcionamiento del mercado negro:

Tarjetas de crédito	Precio
Tarjetas de crédito	Desde 2$ hasta 90$
Tarjetas de crédito físicas	Desde 180$ + coste de los datos
Máquinas duplicadoras de tarjetas	Desde 200 hasta 1.000 $
Cajeros automáticos falsos	Hasta 3.500$
Credenciales bancarias	Desde 80 y hasta 700$ (con garantía de saldo)
Transferencias bancarias y cobro de cheques	Entre el 10 y el 40% del total a transferir o cobrar 10$ para cuenta simple sin saldo verificado
Cuentas de tiendas online y pasarelas de pago	Entre 80 y 1.500$ con saldo verificado
Diseño e implementación de falsas tiendas online	Según proyecto (sin especificar)
Compra y envío de productos	Entre 30 y 300$ (dependiendo producto)
Alquiler envío de spam	A partir de 15$
Alquiler SMTP	A partir de 20$. 40$ para uso durante 3 meses
Alquiler VPN	20$ para utilización para 3 meses

- **Contacto:** Mediante ICQ, Messenger o similar o por email (dirección genérica).
- **Try & Buy:** La mayoría ofrecen tests o demos gratuitos para probar en el sitio. También utilizan sitios online de chequeos de algoritmos, para garantizar autenticidad de los datos de las tarjetas.
- **Pedidos mínimos y escalado por volumen:** Solicitan pedidos mínimos (5 ó 10 unidades para el caso de tarjetas o cuentas bancarias). Ofrecen descuentos por volumen de compra.
- **Tiendas online especializadas:** Una vez establecido el contacto, muchos utilizan sitios online a modo de tiendas para la distribución de sus soluciones (imposibles de acceder si no se tiene el login y el password).
- **Métodos de pago:** Western Union, Lyberty Reserve, WebMoney o similares.
- **Reclamaciones y Soporte:** ofrecen servicio de garantía. Si el producto distribuido no funciona (no es válida la numeración, los logins, etc.), los cambian por otros operativos.
- **Promoción:** principalmente, a través de foros underground, aunque algunos más atrevidos utilizan las redes sociales y tienen cuentas en Facebook y Twitter, entre otros.

proceso

5. El proceso de compra-venta

Los hackers buscan el beneficio económico, y la venta de los datos que consiguen mediante las infecciones, redes de bots, phishing, etc., prueba que no se trata de un argumento del último éxito de hollywood, sino de una realidad.

Lógicamente, el mercado negro tiene sus propias peculiaridades: operar en la clandestinidad obliga a tomar serias precauciones, y parece que en este sentido, los cibercriminales que se dedican a "colocar" el producto en la cadena de valor, lo tienen bien aprendido.

A continuación, vamos a dar un repaso tanto a la oferta que se encuentra disponible en la actualidad en Internet, así como cada paso del proceso en sí mismo de compra-venta. Es importante reseñar que toda la información contenida en este informe es de 2010. Los hallazgos más antiguos datan del pasado mes de junio.

El producto

Del Mercado Negro se ha escrito bastante en los últimos años, sobre todo, porque era la realidad tangible de la historia que la industria de seguridad llevábamos ya contando hace algún tiempo: detrás de cada amenaza, de cada troyano, de cada bot… hay un negocio.

Sin embargo, históricamente nos hemos centrado mucho en la venta de tarjetas de crédito, y ésta es sólo una parte de lo que actualmente se vende en el mercado negro. Este es un listado de los diferentes productos que se ofrecen.

Tarjetas de crédito

Por supuesto, las tarjetas de crédito siguen ocupando buena parte de los anuncios. Pero ahora esta venta se ha vuelto, sin embargo, mucho más profesional:

- **Diferentes emisores.** Y no sólo ofrecen tarjetas AMEX, VISA o Maestro, sino de más entidades emisoras internacionales y además las dividen por país, con un coste diferente. Por regla general, las tarjetas de países europeos y asiáticos suelen ser más caras que las americanas o canadienses.

  - Las tarjetas a la venta más populares son Visa Classic, Visa Gold, Visa Platinum, Visa Business, Mastercard Standard y Gold / Platinum, y American Express.

  - Este tipo de numeraciones para Estados Unidos cuestan 2$ que sólo incluye los datos básicos, y 25$ para las standard (40$ para las Gold, Platinum y Business) con toda la información completa. Los precios para Europa suben hasta 5$ para las primeras, y 50$ para las segundas (90$ en el caso de las más exclusivas). Estos precios varían, por supuesto, entre diferentes vendors, pero suponen una media de la diferente información capturada de este tipo de sitios. Además, como veremos posteriormente, ofrecen descuentos por volumen.

EJEMPLO: FALSOS DESCUENTOS POR COMPRAR CON TARJETA

* Credit Card
US : Visa/Master : 2$, Amex/Discover : 5$,FUllz Info : 20$
UK : Visa/master: 5$, Amex/DOB : 15$, FUllz Info : 30$
EU : Germany/France/Italia/Brazil/Ireland ..: 15$

* DUMPs EURO:
AUSTRALIA,SPAIN,SWITZERLAND,TURKEY,ARABIAN (101) clas - 120 USD , OTHER - 170 USD
GERMANY(101) - clas - 120 USD , OTHER - 150 USD
ITALY (101)(201) - CLASSIC - 120 USD , OTHER - 150 USD
INFINITI - 500 USD
ASIA (101),(201) - classic - 80 USD , OTHER - 100 USD
Amex - 80 USD

• **Datos de entrega.** Tradicionalmente se entregaba el número de la tarjeta y el PIN. Sin embargo, ahora el número de datos ha crecido considerablemente entregándonos prácticamente todos los datos que pudiéramos necesitar para cualquier tipo de operación online u offline. Estos datos se ofrecen también para la venta de cuentas de redes sociales, de correos, de validación en redes privadas, etc.

¿Cuáles son los datos que recibimos junto a la compra de las tarjetas? Los siguientes:

EJEMPLO: DATOS DE ENTREGA

Fulls come with this info:

Firstname:*********
Lastname:*********
Address:*********
City:*********
State:*********
Zipcode:*********
Phone:*********
SSN:*********
Mother'sMaidenName:*
DOB:*******
CardBank:*********
CardType:*********
Cardname:*********
Cardnumber:********
Expiry Date:**-****
CVV2:***
Employment:********
Position Held:*****

Fullz info:

Address 1:
Address 2:
City:
State:
Zip:
Country:
Home Phone:
Date Of Birth:
Social Security Number:
Mothers Maiden Name:
Drivers License Number:
Drivers License State:
Secret Question 1:
Secret Question Answer 1:
Secret Question 2:
Secret Question Answer2:
Name On Card:
Credit Card Number:
Credit Card Brand:
Credit Card Type:
Start Date:
EXP Date:
issue Number:
Credit Card PIN Number:
Card ID Number:
Card Bank Name:
Card 1800 Number:
Verified By Visa Pass:
email:
email pass:
ip:

Tarjetas de crédito físicas

Esta es una novedad respecto a la oferta de productos: en la actualidad, los hackers ofrecen el servicio no sólo de vender la numeración y las claves de identificación (información con la que posteriormente se podía operar en internet de forma directa o bien en cajeros automáticos mediante la creación de duplicados), sino que ahora también ofrecen directamente el envío de las tarjetas ya fabricadas en físico, por supuesto, con un suplemento.

Los precios varían por "vendedor", siendo la media de **150$** por una tarjeta terminada, para un **pedido mínimo de 5 unidades**. El coste del "plástico" va aparte: **30$** para plástico en blanco, y **80$** para impresión en color. A este precio hay que sumar el coste de la información (el número de la tarjeta, PIN y otros datos) que, como hemos visto anteriormente, hay varias ofertas.

Eso sí: garantizan que la tarjeta es de alta calidad (en la imagen adjunta hablan de 2.800 dpi) y que es idéntica que la original del banco, tanto en diseño como en holograma.

EJEMPLO: DESCRIPCIÓN DE TARJETAS DE CRÉDITO

1) Manufacturing plastic cards ready for shopping
2) Record on white and color plastic.
1) Manufacturing plastic of bank quality is made on the newest
equipment with use of own technologies.
I make following kinds of cards:
MasterCard
Visa
AMEX
I guarantee a correct bank microfont, with an excellent sig strip. Quality card 2800 dpi.
The design of a card is identical to the bank original. Holograms on cards are IDENTICAL to the present designs.
The price 150 USD for 1 ready card. Cost is not included in cost of plastic dumps. Minimum order of FIVE cards.
2) Record on white and color plastic Record on white plastic - 30 USD.
Record on color plastic - 80 USD. Cost of record does not include cost

Duplicadoras de tarjetas y falsos cajeros

Y ya metidos en el negocio, ¿por qué no distribuir las máquinas para que los usuarios puedan realizar la duplicación ellos mismos? Este servicio también lo ofrecen como valor añadido. Existen diferentes modelos, y los precios varían desde 200$ hasta los 1.000$.

También venden y distribuyen falsos cajeros automáticos. de esta forma, colocando sobre los cajeros lícitos estas imitaciones, y cuando el usuario hace sus operaciones ordinarias, el falso cajero registrará todo, inclusive números y pins. en algunos casos, también se ha quedado con las tarjetas físicas, quedando disponibles para su utilización posterior por parte de los ciberdelincuentes. el coste de uno de estos cajeros falsos puede llegar incluso a 3.500$. eso sí, el envío es gratuito.

EJEMPLO: DUPLICADORAS y FALSOS CAJEROS

ATM Skimmer NCR: $3000
ATM Skimmer Diebold Opteva: $2500
ATM Skimmer Diebold:$2500
ATM Skimmer Universal:$3500
ATM Skimmer Small:$2000

MSR MACHINE
MSR505 = MSR2000 :$600
MSR505 = MSR300:$450
MSR505 = TA-48:$400
MSR206 = MSR3000:$300
MSR206 = MSR300:$250

Dump Writer and Reader Machine :
MSR206 Reader/Writer USB

Introduction
Magnetic Swipe Card Reader/Writer MSR206 is designed to offer a card reading/writing solution
for ISO 7811/1~6 formats. It reads and writes up to 3 tracks of data, e.g. decoding/encoding and verifying up
to 3 tracks of data simultaneously. Also, MSR206 Reader/Writer provides a standard RS-232 interface to
communicate with host system or other terminal computers.
That will attractively complement an existing system.

Features
* Reading/Writing magnetic stripe card complied with ISO 7811/1~6 formats
* Read/Write High & Low Coercive force of magnetic stripe (300~4000Oe)
* High/Low Coercivity encoding circuitry selectable on screen
* Program software for Windows 98/Me/XP
* Programming software for various read/write performance
* Programmable leading bit, raw data, DMV/AAMVA, and user defined forma
* Manual Swipe to read and/or write card with RS-232 output
* Writing and verifying data on single, dual, or triple track in one swipe
* 5~35ips operational swipe speed of writing data
* 5~55ips operational swipe speed of reading data
* +24VDC+/-10%, 2.0A Max., external power adapter attached
* Good size with dimensions of 210(L) x 60(W) x 65(H) mm
* CE, FCC, UL, cUL certified
Price : 200$
With Free Shipping.

Cuentas bancarias

Ya no se ciñen sólo a la venta de información relativa a tarjetas de crédito, sino a credenciales para el acceso a cuentas de bancos online. La lista de bancos de los cuales ofrecen información de acceso es muy larga:

EJEMPLO: CUENTAS BANCARIAS

Avaliable bank logins
Alliance & Leicester
Abbey bank
Barclays
Bremer Online Banking
Banque Nationale
Banque Nationale
citibank
Chase Bank
Credit Union
First Trust Bank
Flagstar Bank
HDFC Bank
hsbc
halifax
Jodrell Bank
Lloyds TSB Bank
Northern Bank
natwest
RBC
royal bank of scotland
Postbank
Pen Air Federal
welsfargo
Wamu
wachovia & bank of america. And more

De nuevo, los precios varían dependiendo de qué banco estemos hablando. E igualmente hay diferente precio dependiendo de si se adquiere información de una cuenta bancaria con un saldo garantizado o sin garantía.

Las garantías de saldos disponibles en cuenta pueden llegar hasta el medio millón de dólares, y comienzan en unos 20.000. Dependiendo del tipo de banco (y sus medidas de seguridad) así como el saldo disponible, los datos de acceso varían entre 80$ llegando a contar hasta incluso 700$.

Un dato importante a tener en cuenta es que muchos de estos vendedores distinguen entre cuentas personales y datos de acceso a cuentas empresariales (de ahí las altas cantidades de dinero disponibles).

EJEMPLO: CUENTAS BANCARIAS

BankLogin | Shoppin site logins, dell, amazon, apple MAC | Monstergulf Arab KSA Dubai Oman Egypt
make Booking or pay for site | DHL FEDEX ACP POSTAL APO
#
BALANCE IN CHASE .....70K TO 155K ========170$
#
BALANCE IN WASHOVIA.....24K TO 80K==========80$
#
BALANCE IN BOA.....75K TO 450K==========300$
#
BALANCE IN CREDIT UNION.....ANY AMOUNT=========300$
#
BALANCE IN HALIFAX.....ANY AMOUNT=========300$
#
BALANCE IN COMPASS.....ANY AMOUNT=========300$
#
BALANCE IN WELSFARGO.....ANY AMOUNT=========300$
#
BALANCE IN BARCLAYS.....80K TO 100K=========400$
#
BALANCE IN ABBEY.....82K ==========700$
#
BALANCE IN HSBC.....50K========350$

Transferencias bancarias y cobro de cheques

Estos mismos vendedores se ofrecen para hacer transferencias de dinero. Lo más lógico es pensar que está enfocado al blanqueo de capital. Es decir, hacen el trabajo que pudiera hacer cualquier mulero captado mediante una oferta falsa de trabajo.

Las comisiones también varían: desde el 10 hasta el 40% de la cantidad transferida. La competencia, en este caso, parece estar más en la rapidez en realizar la transacción (y la seguridad de la misma) que en la propia comisión de la transferencia.

EJEMPLO: TRANSFERENCIAS BANCARIAS Y COBRO DE CHEQUES

My service is nothing especial compared to my fellow service providers. The only difference is speed.
I offer a much faster transaction simply because I have funds ready to go in my different accounts.
No need to wait for conversions. Once Im informed of successful pick, I can make the transfer right
away if the send back option is LR (already available) or WMZ (soon). My team can pick transfers
between 15-30 minutes from receipt of transfer details. I can do any names so need providing any Drop names.

My Rates:
Amount Received - My Cut
$200 - $399 - 40%
$400 - $599 - 30%
$600 - $999 - 20%
$1,000 Over -15%

Sendbacks (senders share) will be sent out in the following time-frame:

LR and WMZ 15 Minutes from transfer pick.

We make Wire transfer and cheque transfer to
UK and US banks .. HSBC // Nationwide //Halifax //Abbey // Capital // BOA // watchovia //
Barclays // FCU / Regions / Wells // etc.. contact us if u dont have acct with the following banks.
we can trf to our acct and send to u by wu but we charge extra on this cost is 10% upfront
of whatever amount you want us to transfer for you (will accept an order depending on the reciever country
and amount to be transfered)

Venta de cuentas de sitios online

Igualmente, a un precio muy asequible, podemos conseguir cuentas de Paypal, de eBay, Click and Buy, AlertPay, MoneyBookers, de correos privados (Hotmail, GMail, etc.) o de perfiles de redes sociales (Facebook, Twitter, etc.).

Los precios en este caso no sólo varían por países, sino por antigüedad de la cuenta. es decir, si el registro se ha producido hace tres meses o menos, el precio es un 80% más caro que si no se garantiza cuándo se ha dado de alta. Lógicamente, a menor antigüedad, se supone una mayor actividad. En el caso de Paypal, la venta comienza en los 10$ (sin garantía de tiempo, pero sí con acceso verificado). Y de nuevo, el precio sube si queremos adquirir cuentas con un balance monetario garantizado: 80$ por cuentas garantizadas de 1.500$.

EJEMPLO: VENTA DE CUENTAS DE SITIOS ONLINE

Paypal Login :
We Have Verified And Unlimited Paypal Account With Balance And Add Cc And BAnk Acc***.
All Our PayPa Acc Have Full Info And With Email Access and With All Security Answer .
And With Orginal Ip And A Program For Fake Your System Ip To Orgina Ip For Full Access To PayPal Acc.

Ebay Login :
Fresh And Verified And Unlimited Ebay Account.
With Ful Info And Full Access.

MoneyBookers Account :
Verified And Full Access MoneyBookers Account.
Verified With Good Balance.
From All Country.

ClickAndBuy And Alertpay Account Is Available ....

Diseño e implementación de tiendas online falsas

Uno de los servicios, también novedad, que ofertan es la creación, desarrollo, implementación e indexación de falsas tiendas online. El objetivo está claro: engañar al público comprando algo que nunca recibirán y que proporciona, además del dinero de la transacción, los datos de las tarjetas de crédito utilizadas.

EJEMPLO: VENTA DE CUENTAS DE SITIOS ONLINE

Merchand Account :

WE can make fake ecommerce sites that can help you get approved for MERCHANT ACCOUNTS.

Compra y envío de productos

Muchos de los compradores que buscan información de tarjetas de crédito lo utilizan para comprar bienes. De esta forma, "limpian" ese dinero de forma inmediata. Pero tiene un pequeño inconveniente: a la tienda hay que darle datos para la identificación y el envío de la mercancía.

Pues bien, estos vendedores también ofertan el servicio de realizar las compras y enviarlo posteriormente a cualquier dirección suministrada, evitando de esta manera al comprador el ser localizado en caso de reclamación.

Por supuesto, este servicio tiene un coste adicional:

EJEMPLO: COMPRA Y ENVÍO DE PRODUCTOS

PAYING FOR SHIPPING TO YOUR ADDRESSS

LAPTOP	300$
IPHONES	60$
DIGITAL CAMERA	30$
PLASMA TV	100$
PORTABLE DVD	30$
CAMCORDER	30$
HOME THEATER	50$
PROJECTOR	150$

Shipping Service : I Have Good and Safe Service For Ship Product To Your Address.
My Service Is Very Fast and Without Delay.
You Can Select Your Item In Shopping and Give link .
I buy your Product For You and send To Your Address.
I Can Ship All Item TO WorldWide Ship Address.
My Service Is Very Cheap.

I Can Ship Laptop and Iphone And All Electronic Item To Your SHipping Address.

Alquiler de redes para el envío de spam

Este servicio no es nuevo. De hecho, muchas de las redes de bots que se crean diariamente tienen como fin su uso para enviar spam, servicio por el que los hackers cobran. Y dentro de este tipo de servicio se oferta prácticamente de todo para que los usuarios puedan enviar spam de una forma segura: bases de datos con direcciones a las que enviar el spam; alquiler de uso de las máquinas desde las que enviar el spam (redes de bots); conexiones vpn para facilitar la conexión a los paneles de control de forma anónima, etc.

EJEMPLO: ALQUILER DE REDES PARA EL ENVÍO DE SPAM

Spamming Service : I Have Good stuff For Spamming.
If You are Spammer. I Have Good And Work Stuff for You.

Inbox Mailer : Web Mailer and Good Mailer Software Is Available for You.
I Have Good Php and Ajax Web Mailer For You.
And I Have Good Software For Spamming For All Spammer.

Mail List And Lead : I Have Fresh And Active And New Mail List And Lead For You.
All Mail List And Lead Is From Bank Member or Shopping User.
and My Price for Spamming Stuff Is cheap.
and mail list from all country is available.

Cpanel and Hosting and Shell:
Cpanel with dedicated Ip And big space And High Speed For Spamming is Available For You.
and good hosting panel is Available for you. this is very good offer for spamming.

Shell: yes i have good shell for you.
i have php and asp shell for sale.
this is special offer for spamming.

Remote Desktop (RDP) : I Have High Speed And Bandwith For Spamming.
with windows server 2003 and with windows server 2008.
and all server have big hard space.
very good offer for big download and big upload from this.

SMTP: I Have Good SMTP For All Big Spammer.
With Good Ip . and high speed.

Mail Sender And Mail Spider : Email Spider Gold . to Auto Haverst emails from the internet "Websites
Advanced Mass Sender (This Best Program To spam email useing SMTP where , and forums"
u will get them using Smtp scanner "Hscan")

El contacto

Cuando hablamos de un entorno de cibercriminales, es lógico pensar que utilizarán todo tipo de maniobras para pasar lo más desapercibidos posible. De esta manera, se anuncian en hilos de foros públicos, pero a los que llegar es difícil. Este tipo de comunidades suelen tener una característica en común: suelen ser bastante underground, de forma que se aseguran que se dirigen a un perfil de público específico.

Una vez localizamos los post con las ofertas de los servicios, prácticamente la única forma que existe de contactar con estos minoristas es a través de aplicaciones de mensajería instantánea: icq, yahoo messenger y similares. Otros ofrecen alguna forma de contacto a través de e-mail (por supuesto, un e-mail gratuito y genérico).

Los que ofrecen el contacto por ICQ o similar, suelen indicar incluso a qué horas están disponibles: o 24 horas conectados u otro tipo de horario más laboral (horario de oficina). Incluso avisan cuándo se van a ir de vacaciones.

EJEMPLO: CONTACTOS

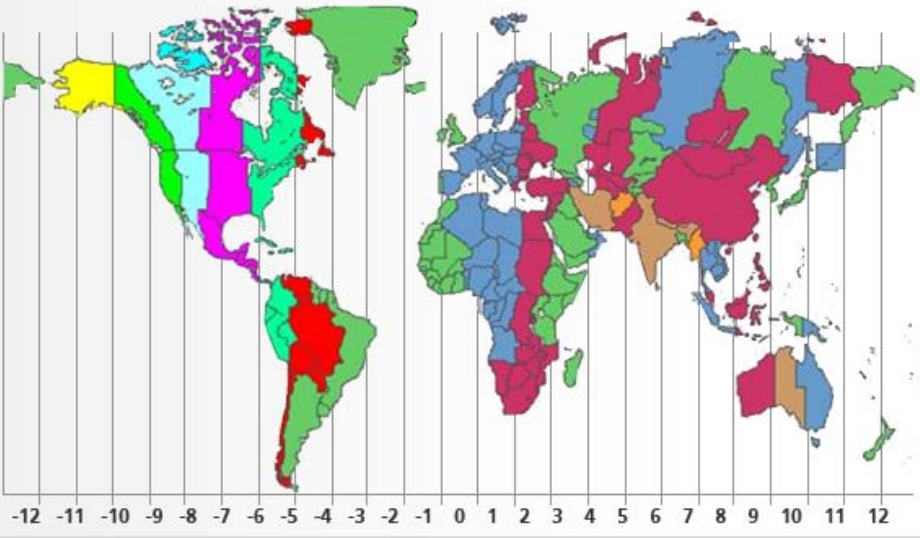
Online Rules
||AM online 24hours and i service all in best way i can.
Before any holiday will let every1 know before taking holiday

Los que ofrecen el contacto por ICQ o similar, suelen indicar incluso a qué horas están disponibles: o 24 horas conectados u otro tipo de horario más laboral (horario de oficina). Incluso avisan cuándo se van a ir de vacaciones.

EJEMPLO: CONTACTOS

Conditions - In order for me to meet the above time frames, the following conditions must exist:
1. Transfers details must be received by me through ICQ within 6:00 a.m. and 5:00 p.m. my countrys time.
   I belong to GMT+8 time zone.

EJEMPLO: CONTACTOS



Try & Buy

"Busque, compare, y si encuentra algo mejor, le devolvemos el dinero…". El que pudiera ser un eslogan de cualquier campaña publicitaria, se convierte en una realidad. Especialmente con la crisis –y con más personas en el paro o malviviendo con sueldos ajustados-, están proliferando este tipo de servicios. Su principal preocupación es cómo generar confianza en el cliente. No debemos olvidar que, al final, estamos tratando con delincuentes.

EJEMPLO: PRUEBA Y COMPRA

!!!!!! DO NOT email asking for tests, demos, freebies, telling me how you
got scammed and crying and telling me I need to prove myself because your *** got ripped.
I do NOT have time

Hay dos extremos en este sentido: los que ofrecen (y publican en estos foros) **pruebas gratuitas de numeración de tarjetas de crédito, acceso a cuentas bancarias, etc., para probar que su "género" es de buena calidad**, y los que claramente indican que no ofrecen pruebas gratuitas, **pero que garantizan su producto** (si no funciona, proceden a la sustitución de los datos por otros).

EJEMPLO: PRUEBA Y COMPRA

DEMO:

Austria

France

Germany

Spain

Turkey

Poland

Switzerland

Czech Republic

Mexico

EJEMPLO: PRUEBA Y COMPRA

PERSONAL DETAILS::::
[redacted]

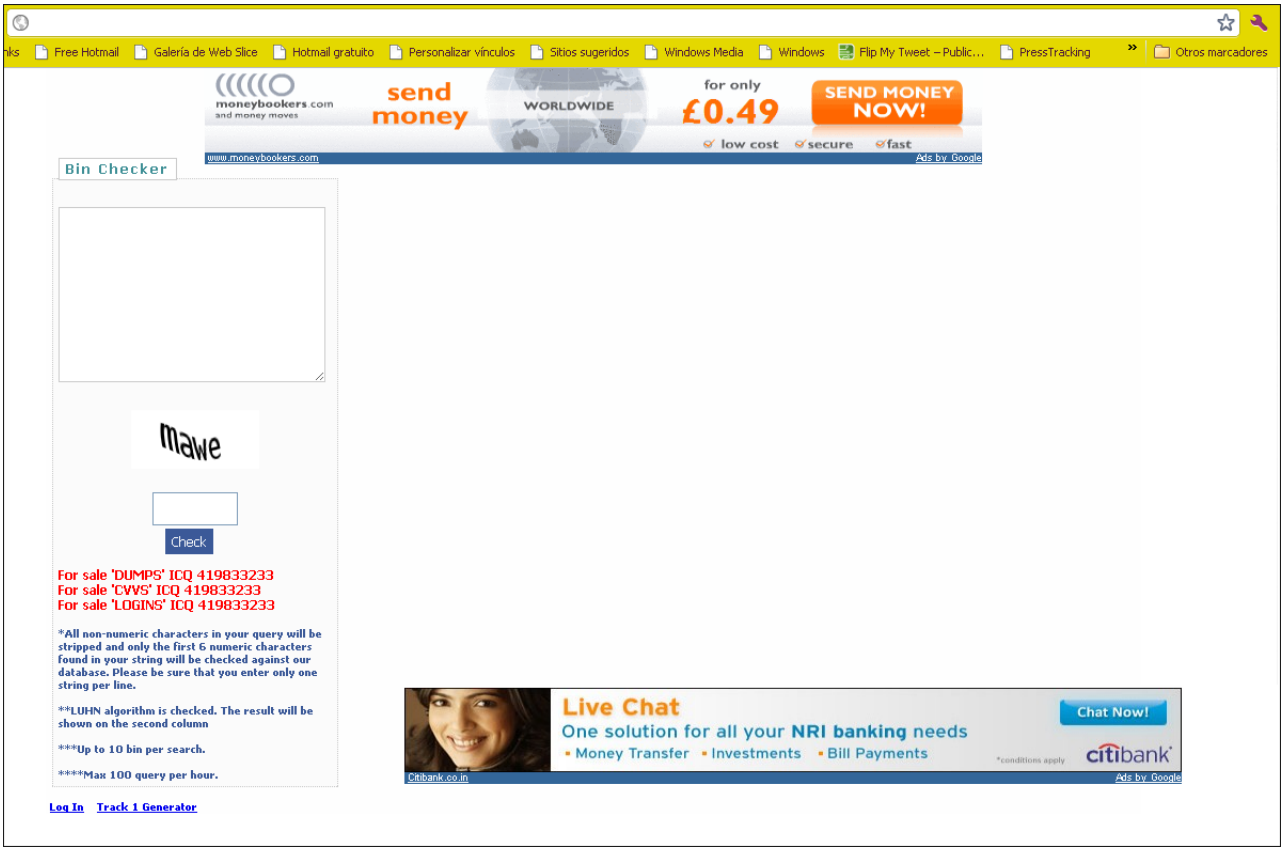
SMTP Domain Sample:
[redacted]

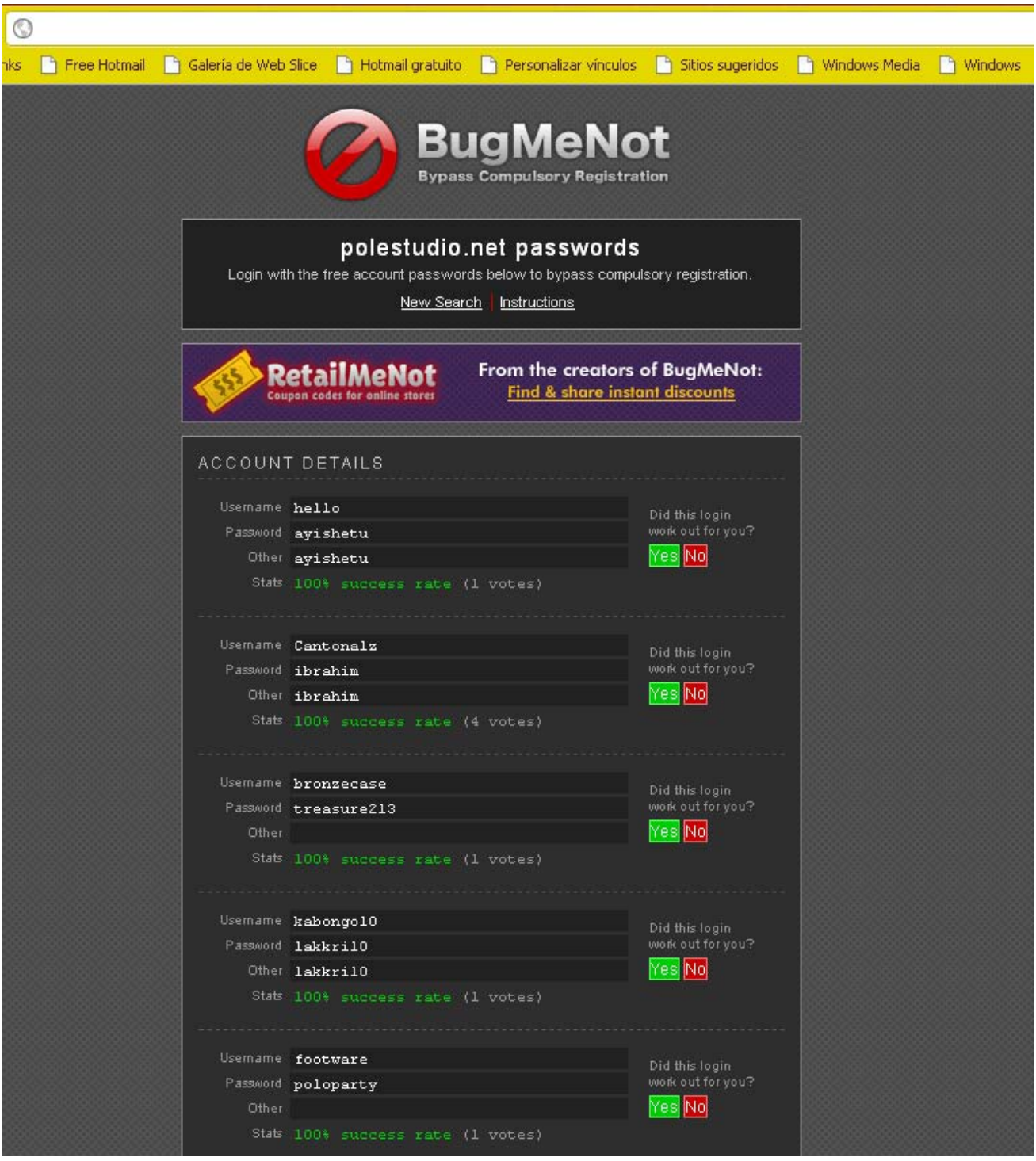
SMTP Ip Sample:
195.227.118.252 - test/test
smtp 88.2.161.78-eva-eva 80.148.7.11-mail-mail123 64.173.103.196-david-1234 212.122.224.24-test-123456 217.37.5.93-sonia-password
203.191.151.66-test-123456

N: B
I DONT GIVE FREE TEST,IF YOU WANNA BUY?,YOU BUY AND TEST .... NO S**T TALK
PAYMENT METHOD:LIBERTY RESERVE*LR* ,WMZ,....
[redacted]

Sistemas de prueba online

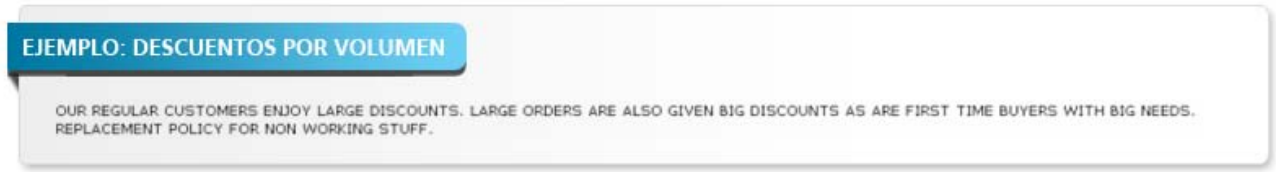
Algunos ofrecen el chequeo gratuito de la validez de los datos proporcionados a través de un sistema online que tienen supuestamente conectado con aplicaciones como iTunes, que chequean que la numeración es correcta basándose en los diferentes algoritmos utilizados por entidades bancarias y de pago para generar dicha identificación.




Free Hotmail
Galería de Web Slice
Hotmail gratuito
Personalizar vínculos
Sitios sugeridos
Windows Media
Windows
BugMeNot
Bypass Compulsory Registration
polestudio.net passwords
Login with the free account passwords below to bypass compulsory registration.
New Search | Instructions
RetailMeNot
Coupon codes for online stores
From the creators of BugMeNot:
Find & share instant discounts
ACCOUNT DETAILS
Username hello
Password ayishetu
Other ayishetu
Stats 100% success rate (1 votes)
Did this login work out for you?
Yes No
Username Cantonalz
Password ibrahim
Other ibrahim
Stats 100% success rate (4 votes)
Did this login work out for you?
Yes No
Username bronzecase
Password treasure213
Other
Stats 100% success rate (1 votes)
Did this login work out for you?
Yes No
Username kabongo10
Password lakkri10
Other lakkri10
Stats 100% success rate (1 votes)
Did this login work out for you?
Yes No
Username footware
Password poloparty
Other
Stats 100% success rate (1 votes)
Did this login work out for you?
Yes No

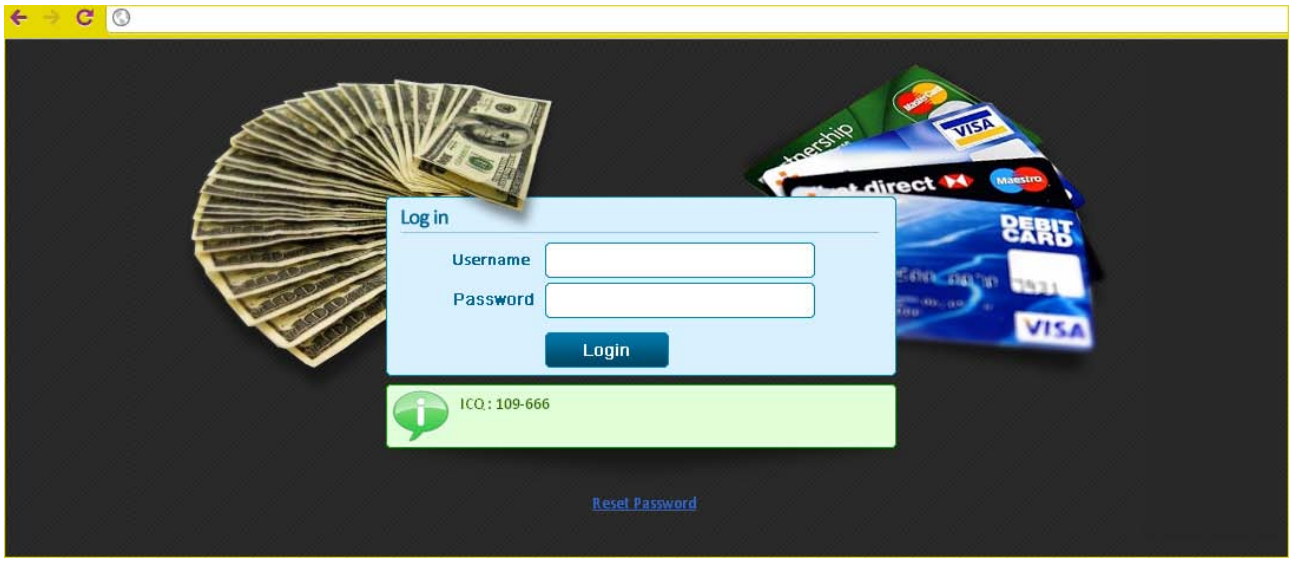
Pedido mínimo y escalado por volumen

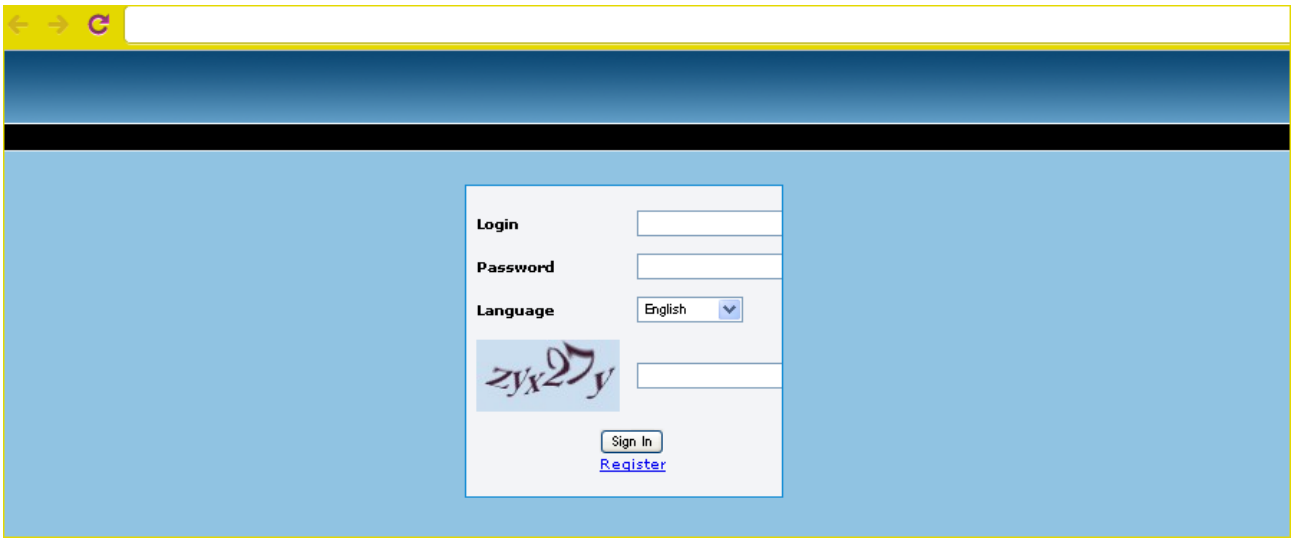
Por supuesto, prácticamente todos exigen un pedido mínimo de cualquiera de los productos ofertados (los que tienen un coste bajo, como las tarjetas de crédito o los accesos bancarios) y también ofrece descuentos por volumen.

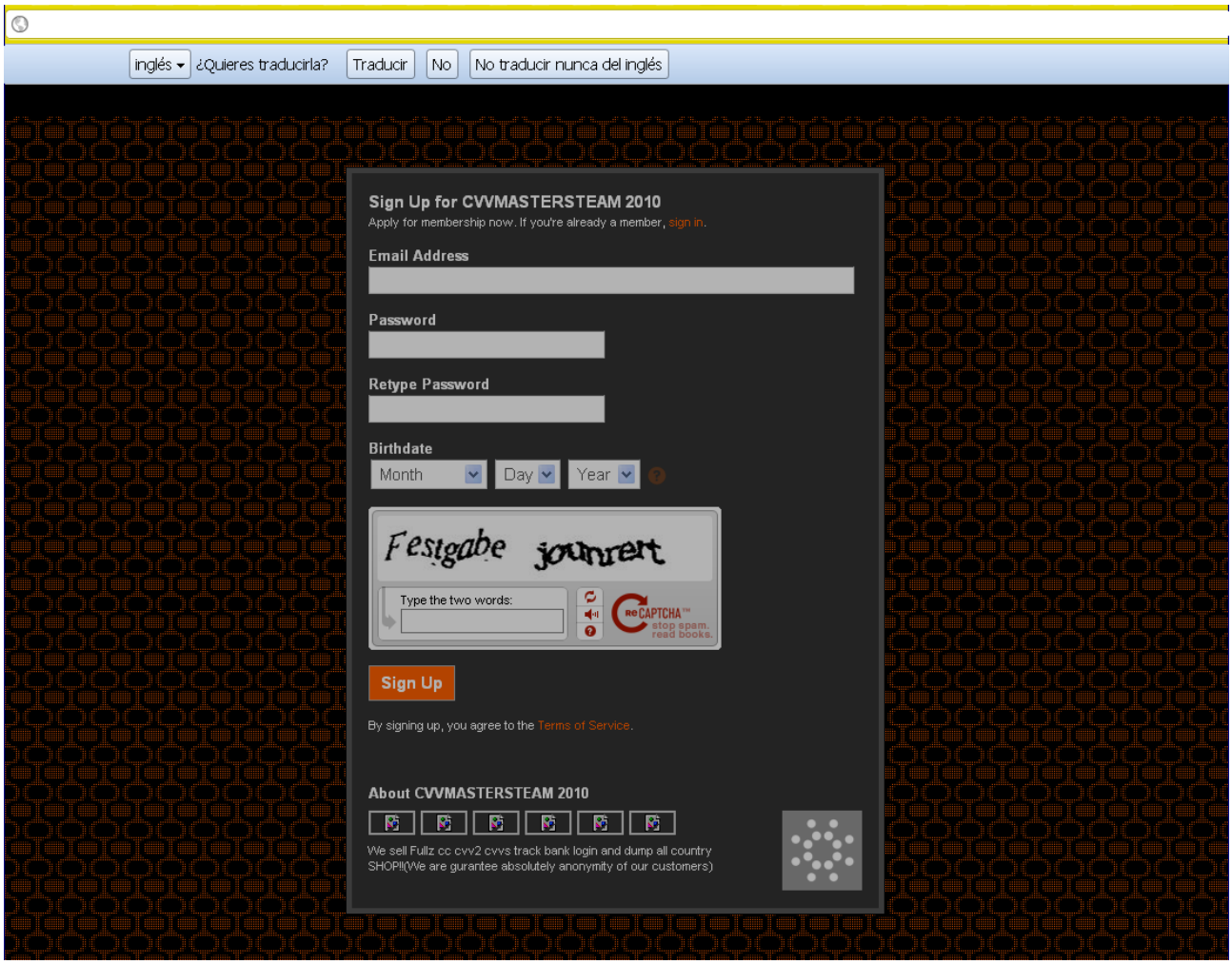


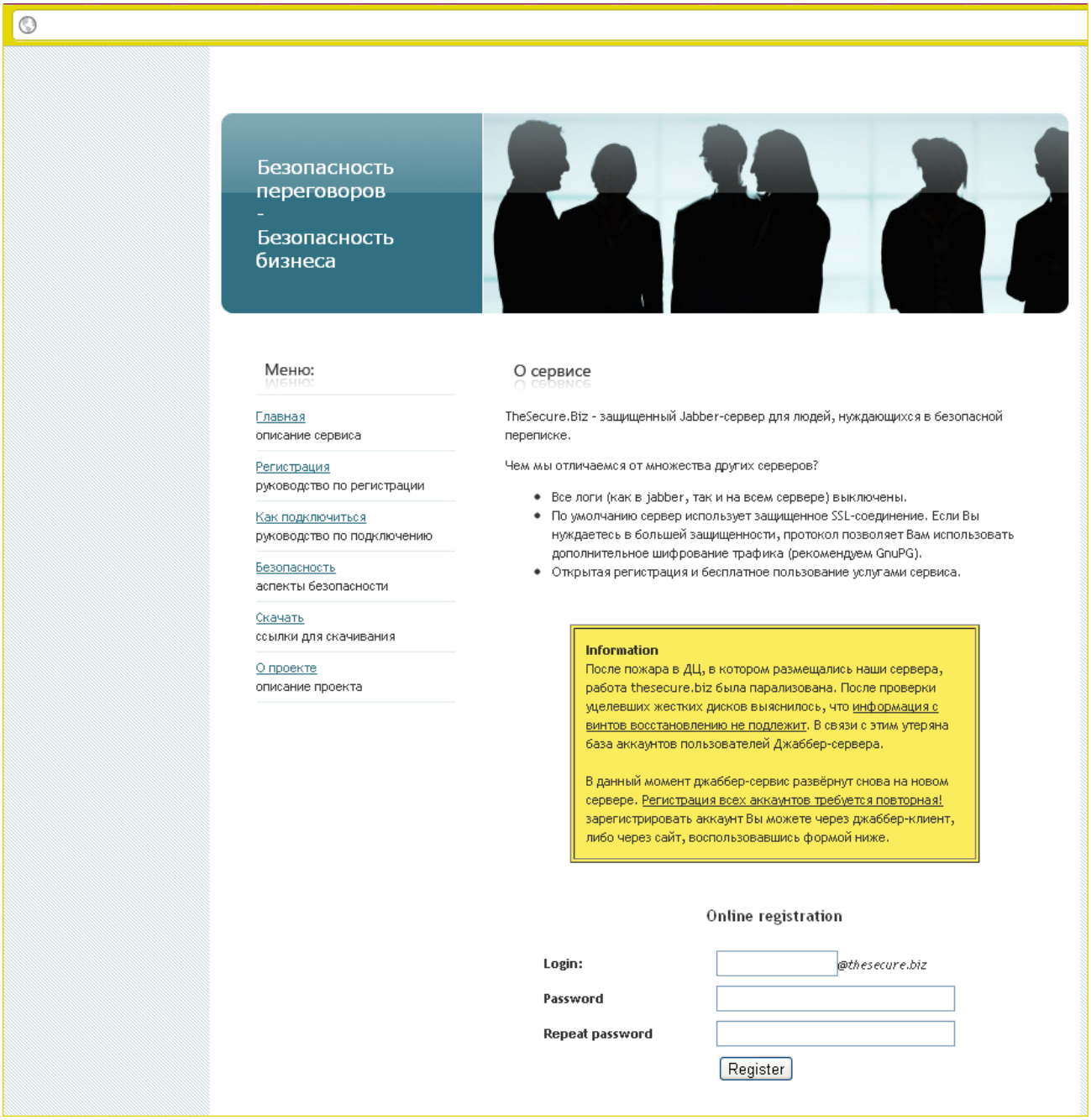
Tiendas online especializadas

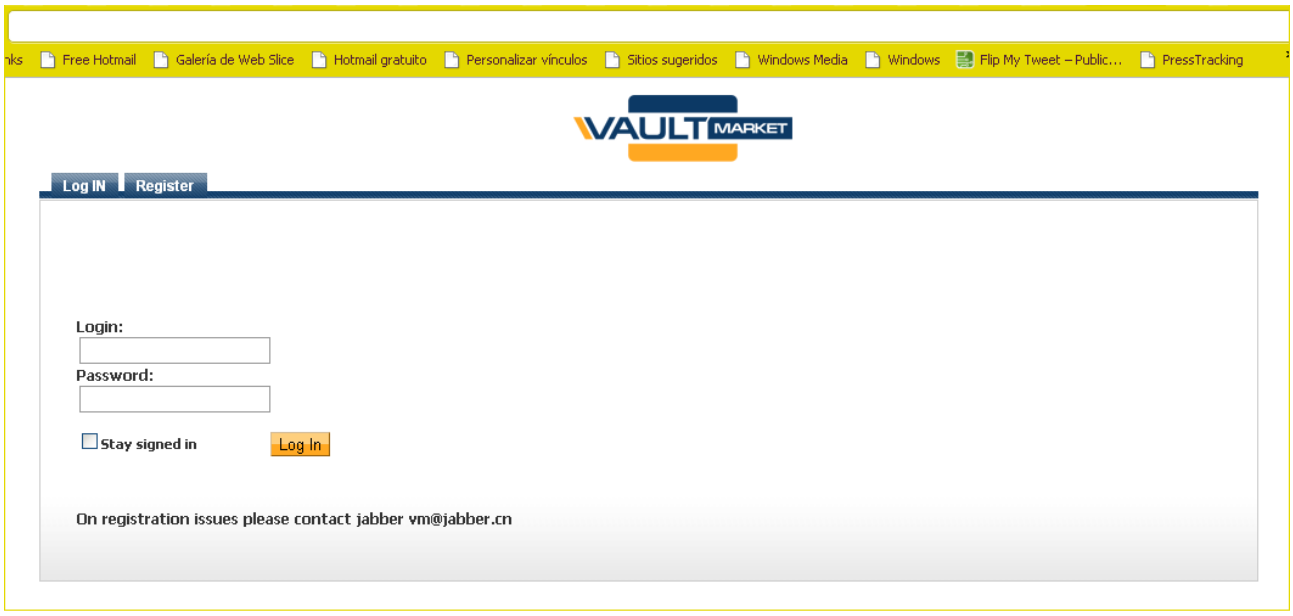
Tras el contacto mediante las vías "autorizadas", algunos de ellos suministrarán y venderán directamente el producto elegido y otros proporcionarán claves que nos den acceso a las numerosas tiendas on-line desde las cuales se puede acceder a un catálogo de e-commerce exactamente igual que si se tratara de una tienda normal. Eso sí: llegar a ellas es realmente complicado, y el acceso, sin login ni password, imposible.

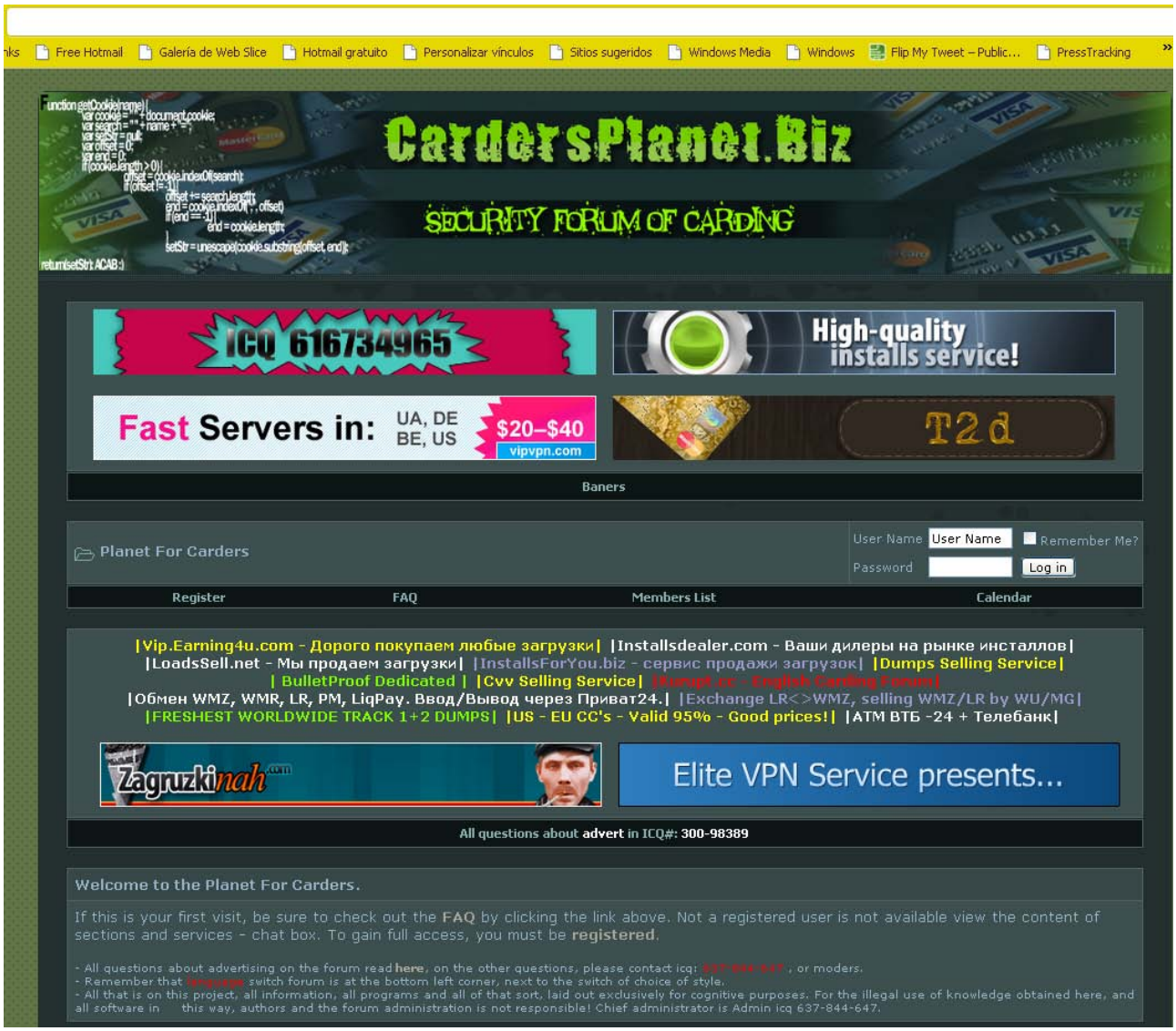


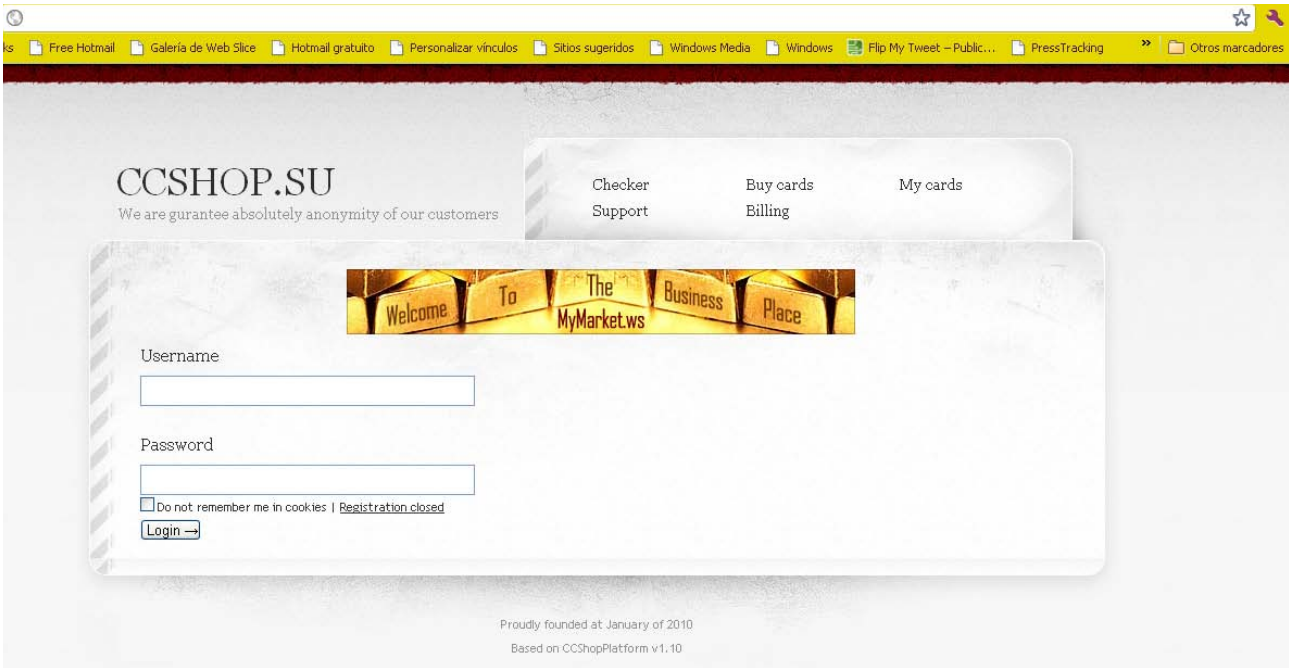


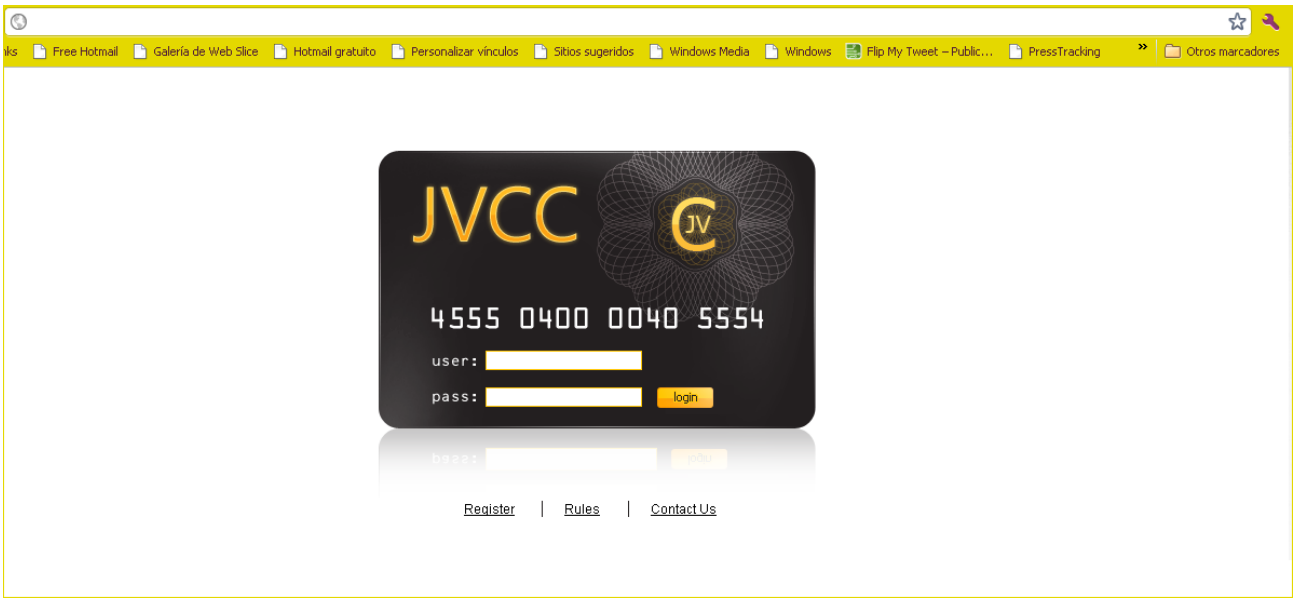

inglés
¿Quieres traducirla?
Traducir
No
No traducir nunca del inglés
Sign Up for CVVMASTERSTEAM 2010
Apply for membership now. If you're already a member, sign in.
Email Address
Password
Retype Password
Birthdate
Month
Day
Year
Festgabe
Type the two words:
Sign Up
By signing up, you agree to the Terms of Service.
About CVVMASTERSTEAM 2010
We sell Fullz cc cvv2 cvvs track bank login and dump all country
SHOP!!(We are gurantee absolutely anonymity of our customers)


Безопасность
переговоров
-
Безопасность
бизнеса
Меню:
Главная
описание сервиса
Регистрация
руководство по регистрации
Как подключиться
руководство по подключению
Безопасность
аспекты безопасности
Скачать
ссылки для скачивания
О проекте
описание проекта
О сервисе
TheSecure.Biz - защищенный Jabber-сервер для людей, нуждающихся в безопасной переписке.
Чем мы отличаемся от множества других серверов?
Все логи (как в jabber, так и на всем сервере) выключены.
По умолчанию сервер использует защищенное SSL-соединение. Если Вы нуждаетесь в большей защищенности, протокол позволяет Вам использовать дополнительное шифрование трафика (рекомендуем GnuPG).
Открытая регистрация и бесплатное пользование услугами сервиса.
Information
После пожара в ДЦ, в котором размещались наши сервера, работа thesecure.biz была парализована. После проверки уцелевших жестких дисков выяснилось, что информация с винтов восстановлению не подлежит. В связи с этим утеряна база аккаунтов пользователей Джаббер-сервера.
В данный момент джаббер-сервис развёрнут снова на новом сервере. Регистрация всех аккаунтов требуется повторная! зарегистрировать аккаунт Вы можете через джаббер-клиент, либо через сайт, воспользовавшись формой ниже.
Online registration
Login:
@thesecure.biz
Password
Repeat password
Register


Free Hotmail
Galería de Web Slice
Hotmail gratuito
Personalizar vínculos
Sitios sugeridos
Windows Media
Windows
Flip My Tweet – Public...
PressTracking
VAULT MARKET
Log IN
Register
Login:
Password:
Stay signed in
Log In
On registration issues please contact jabber vm@jabber.cn

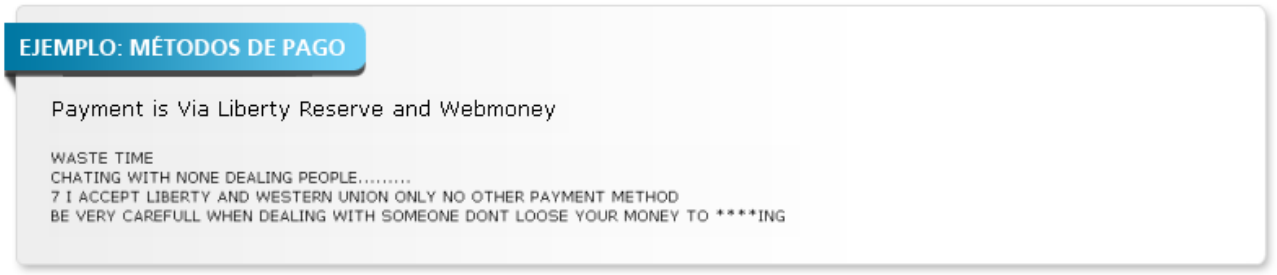

CardersPlanet.Biz
SECURITY FORUM OF CARDING
ICQ 616734965
High-quality installs service!
Fast Servers in: UA, DE BE, US $20–$40 vipvpn.com
T2d
Baners
Planet For Carders
User Name
Remember Me?
Password
Log in
Register
FAQ
Members List
Calendar
|Vip.Earning4u.com - Дорого покупаем любые загрузки| |Installsdealer.com - Ваши дилеры на рынке инсталлов|
|LoadsSell.net - Мы продаем загрузки| |InstallsForYou.biz - сервис продажи загрузок| |Dumps Selling Service|
| BulletProof Dedicated | |Cvv Selling Service| |Exchange LR<>WMZ, selling WMZ/LR by WU/MG|
|Обмен WMZ, WMR, LR, PM, LiqPay. Ввод/Вывод через Приват24.| |FRESHEST WORLDWIDE TRACK 1+2 DUMPS| |US - EU CC's - Valid 95% - Good prices!| |АТМ ВТБ -24 + Телебанк|
Zagruzkinah
Elite VPN Service presents...
All questions about advert in ICQ#: 300-98389
Welcome to the Planet For Carders.
If this is your first visit, be sure to check out the FAQ by clicking the link above. Not a registered user is not available view the content of sections and services - chat box. To gain full access, you must be registered.
- All questions about advertising on the forum read here, on the other questions, please contact icq: 637-844-647 , or moders.
- Remember that forum.ua switch forum is at the bottom left corner, next to the switch of choice of style.
- All that is on this project, all information, all programs and all of that sort, laid out exclusively for cognitive purposes. For the illegal use of knowledge obtained here, and all software in this way, authors and the forum administration is not responsible! Chief administrator is Admin icq 637-844-647.


CCSHOP.SU
We are gurantee absolutely anonymity of our customers
Checker
Buy cards
My cards
Support
Billing
Welcome To The MyMarket.ws Business Place
Username
Password
Do not remember me in cookies | Registration closed
Login →
Proudly founded at January of 2010
Based on CCShopPlatform v1.10



Métodos de pago

Prácticamente sin excepción, el método de pago más demandado por los hackers es a través de servicios de envío de dinero. Los más comunes son liberty reserve y western union, pero también mencionan otros como webmoney, por ejemplo. También resulta lógico, dado que dichos servicios garantizan un anonimato que se pierde en el caso de pago por tarjeta, transferencia, etc… Y ya puestos, ¿quién estaría dispuesto a pagarles mediante estos métodos cuando es precisamente lo que venden? El usuario estaría exponiéndose.



Reclamaciones y soporte

Si hay algo en común entre este tipo de venta es el ofrecimiento del cambio del producto adquirido si éste no cumple las expectativas: básicamente, si no funciona. Eso sí, algunos de ellos establecen un período de devolución (igual que los comercios normales) que, en determinadas ofertas, se restringe a las primeras 24 horas desde la recepción de la mercancía.

EJEMPLO: RECLAMACIONES Y SOPORTE

||Hello My Dear Customers.||

{Here are all my rules . All who follow that will enjoy my service.}

{New customers are always welcome to try my service!}
(WMZ|LR)- NO MINIMUM!!! DONT LOOSE YOUR CHANCE
(WU)MINIMUM-550$

||High valid rate 95% valid.
||Daily update.
||Lowest price.
||I'm not resellers like somebody else.
||Am not checking dumps before u ask, Am very very sure in quality of my dumps and youll become my regular customer i will add some bonus in any purchase.

Replacement
||Dumps checking by ask customer.
||I dont replace checked dumps, unchecked dumps i can replace but only in 24 hours.
||replayce always will be checked!!!
||If u cheat me for replacements.I will put you ignore list!!!

Order Rules
||Give me bin u need in all same 1 line message and i'll ansswer u to pay total.

Online Rules
||AM online 24hours and i service all in best way i can.
Before any holiday will let every1 know before taking holiday

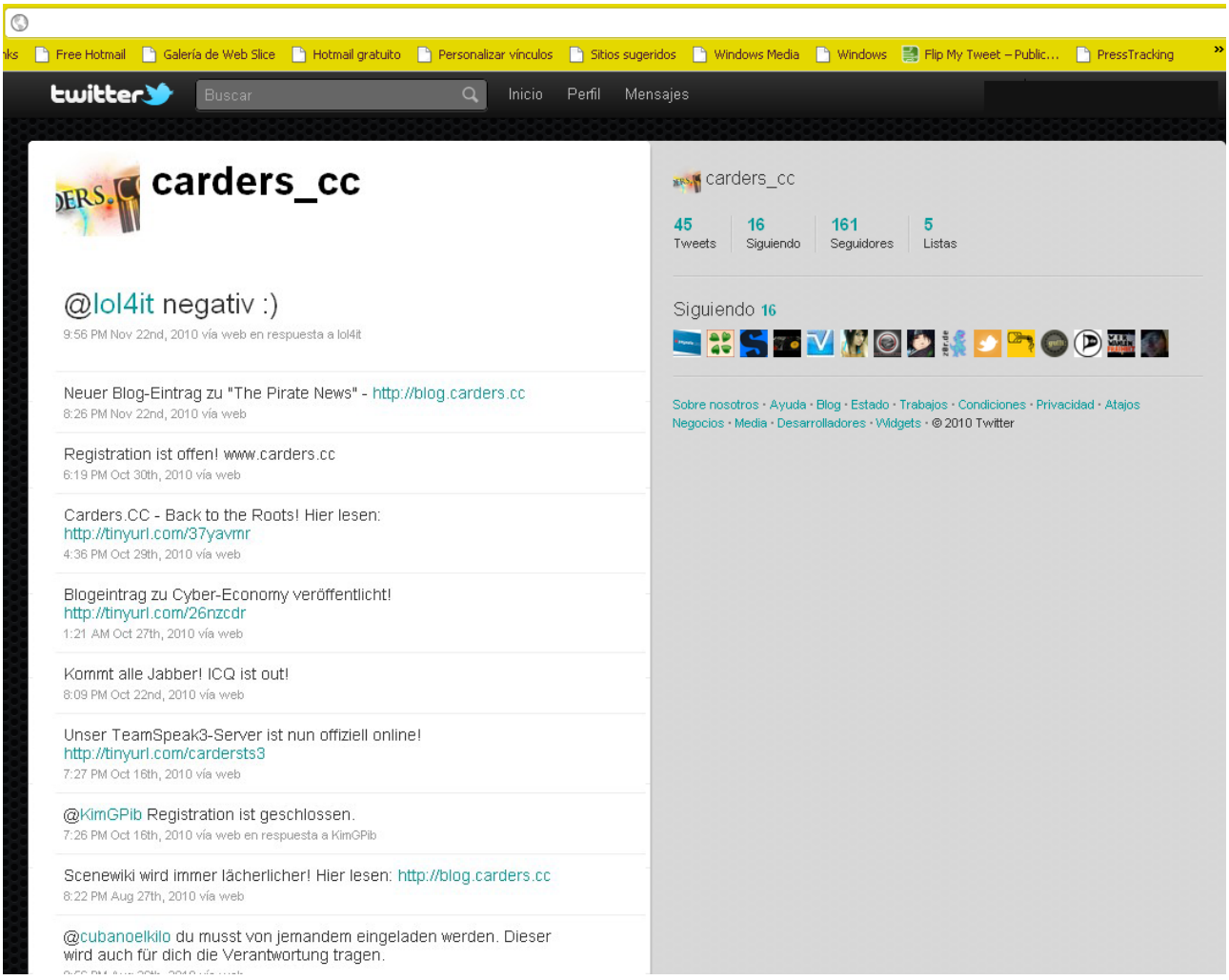
Delivery Rules
||Instantly delivery.

All prices and countries contact on ICQ

||Contact me||

Promoción

Y finalmente, como cualquier negocio que se precie, estos hackers se intentan dar a conocer, eso sí, con sumo cuidado… **Además de publicar sus ofertas en foros underground, algunos de ellos son más atrevidos y van más allá: utilizan las redes sociales para promocionarse.**



Y también tienen críticas, como cualquier producto o servicio que se ofrezca online:

EJEMPLO: PROMOCIÓN

beware of this fake hackers..they are here to steal people money..they will attract you with good cvv..
and push you to buy dumps..after all the money you sent to them..they will run away with it...they are thieves..
they robbed me about 900usd..that is not good..there add
are....freeman_hacker10@yahoo.com
and the other is moon_sad_123@yahoo.com...pls becareful with them....

6. ¿Cómo minimizar el riesgo?

Como siempre decimos, lo mejor para mantenerse protegido es utilizar el sentido común, que muchas veces es el menos común de los sentidos. Y, por supuesto, contar con una buena protección en el ordenador (si es personal) y en todos los posibles vectores de infección de la red (en el caso de una empresa).

Pero, hay una serie de buenas prácticas que también nos pueden ayudar, particularmente en caso de utilización de la banca online, de realizar compras o transacciones bien on u offline, etc. Son las siguientes:

Qué hacer para prevenir

- Mantener la información personal siempre guardada en un sitio seguro.
- Firmar las tarjetas de crédito tan pronto se reciba.
- Mantenerse alerta a la hora de pagar en cualquier establecimiento (cuidar que las transacciones con tarjetas se hagan siempre delante del cliente).
- Guardar los recibos y compararlos con los informes del banco, para detectar cualquier irregularidad.
- En el caso de detectar cualquier movimiento sospechoso en la cuenta bancaria, informar rápidamente al banco o a la entidad emisora de la tarjeta de crédito o débito.
- Cuidar la correspondencia física: es recomendable siempre destruir todas las facturas y cartas en la que aparezca nombre, dirección, datos de la seguridad social, número de cuenta, etc.
- Revisar las facturas para buscar actividades no autorizadas.
- Revisar los informes de las tarjetas de crédito con asiduidad.
- Ante dudas sobre la legitimidad de un mensaje recibido de cualquier tipo de entidad bancaria, financiera, tienda online, pasarela de pago, etc., contactar con el departamento de atención al cliente de la compañía de la que parece llegar el mensaje.
- Si estás de viaje, pide a alguien de confianza que recoja el correo y lo guarde durante tu ausencia.
- La mayoría de los bancos y compañías de tarjetas de crédito tienen alertas de notificación de los últimos movimientos.
- Nunca des tu información personal por teléfono o en Internet si no conoces la compañía o el sitio web. Y aun así, actúa con precaución.
- Guarda los recibos de los cajeros automáticos o rómpelos en pequeños pedazos. Pueden contener información confidencial.
- Memoriza todas tus contraseñas, no las guardes en tu ordenador o las tengas en la cartera o en tu agenda de teléfono.
- Instala un buen antivirus y un buen firewall en tu ordenador personal para prevenir el robo de identidad y datos confidenciales. Intenta contar siempre con las últimas tecnologías de protección, capaces de detectar nuevo malware incluso sin conocerlo con anterioridad.
- Mantén tu antivirus siempre actualizado.
- Cierra todas las sesiones web, de navegador, y no guardes las contraseñas en tu ordenador.
- Elimina los datos de tu ordenador cuando hayas terminado de hacer una transferencia online. Presta especial atención a archivos temporales, cookies, etc.

Qué no hacer

- No dejes tu tarjeta a nadie, y siempre mantenlas contigo en todo momento.
- No firmes nunca un recibo en blanco.
- No des tu número de cuenta o contraseñas por teléfono, a menos que estés en una conversación con una empresa fiable o hayas llamado tú para solicitar un servicio.
- Nunca imprimas tu número de seguridad social o número de teléfono en tus cheques de banco.
- No respondas a correos no solicitados, mensajería instantánea, mensajes de texto, pop ups que parecen llegar de tu banco, compañía de tarjeta de crédito, proveedor de telefonía, tienda online, pasarela de pago, etc.
- No uses tarjetas de débito online para hacer compras online. Son menos seguras que una tarjeta de crédito en caso de fraude.

Qué hacer si has sido víctima

Actualmente, la mayoría de entidades financieras, bancos, compañías emisoras de tarjetas, etc., suelen hacerse cargo en caso de haber sido víctima de un fraude. Por eso, es muy importante detectarlo cuanto antes y ponerlo en conocimiento de los terminales adecuados:

- Contacta con la institución financiera en la que tengas tus cuentas y en la que hayas sido víctima de fraude. Debes cancelar las tarjetas y parar las órdenes de pago, cambia tus claves de la tarjeta.
- Informa a las autoridades del hecho para ponerlo en su conocimiento. Los bancos, compañías de tarjetas de crédito y otras instituciones pueden solicitar la denuncia

PandaLabs es el laboratorio antimalware de Panda Security, y representa el centro neurálgico de la compañía en cuanto a tratamiento del malware se refiere:

- Desde **PandaLabs** se elaboran en tiempo real y de forma ininterrumpida las contramedidas necesarias para proteger a los clientes de Panda Security de todo tipo de códigos maliciosos a escala mundial.

- **PandaLabs** se encarga asimismo de llevar a cabo el análisis detallado de todos los tipos de malware, con la finalidad de mejorar la protección ofrecida a los clientes de Panda Security, así como para informar al público en general.

- Del mismo modo, **PandaLabs** mantiene un continuo estado de vigilancia, siguiendo muy de cerca las diferentes tendencias y evoluciones acontecidas en el campo del malware y la seguridad. Su objetivo es avisar y alertar sobre inminentes peligros y amenazas, así como formular previsiones de cara al futuro.

- Se puede obtener información sobre las últimas amenazas descubiertas en el blog de **PandaLabs** en: **http://pandalabs.pandasecurity.com/**.

www.pandasecurity.com