THE CYBER-CRIME BLACK MARKET: UNCOVERED
INDEX

1. Introduction

2. The evolution of malware aimed at stealing bank details

3. How the black market works

4. The black market at-a-glance

5. The sales process
   5.1. The product
   5.2. The contact
   5.3. Try & Buy
   5.4. Online testing
   5.5. Minimum orders and bulk discounts
   5.6. Specialized online stores
   5.7. Methods of payment
   5.8. Customer services and support
   5.9. Promotion

6. How to minimize the risk?
1. Introduction
Many of us in the team at Panda Security spend a lot of time traveling and attending all types of events: from specialized IT industry fairs and congresses, to those aimed at businesses, end-users, etc. Yet even though it is becoming more common to hear about the arrest of hackers that steal information and profit from it in many different ways, there are still many members of the public, not necessarily dedicated to IT security, who ask us: “Why would anyone want to steal information from me? I don’t have anything of interest…”

Another factor to bear in mind is that today's profit-oriented malware is designed to steal data surreptitiously, so the first indication that you have been a victim is when you get your bank or Paypal account statement.

Moreover, there is a general perception that this problem only affects home users, and that businesses are immune. The result of our research, as you will read below, shows that this is not the case: Today nobody –neither home users nor businesses- is safe from confidential data theft (and the consequent fraud).

This is despite the increased effort in recent years to improve awareness and education in IT security, initiated by governmental agencies in many countries, and of course, thanks to the security industry as a whole, along with other institutions, organizations, media, blogs, etc., who have been assisting with the task for some time now.

Although we don’t have precise data, we believe that this nefarious business has expanded with the economic crisis. Previously it was no way easy to locate sites or individuals dedicated to this type of business, yet now it’s relatively simple to come across these types of offers on underground forums.

Price wars, numerous ‘special offers’ and the diversification of the business are all indications of how these mafias are desperately trying to drive up revenue. A few years ago, it was just a question of the sale of a few credit card details. Now, in addition to offering all types of information about victims -even the name of the family pet-, other services are available, including physical cloning of cards or making anonymous purchases and forwarding the goods to the buyer.
2. The evolution of malware aimed at stealing bank details
The global evolution of malware, and specifically the growth of IT threats designed to steal bank details, explain why the black market for selling confidential personal details has expanded.

The exponential growth in malware in recent years is an undeniable fact, as security companies have been affirming for some time now. A few years back we were reporting that some 500 new threats were being created every month whereas now, PandaLabs, our anti-malware laboratory, receives on average 63,000 new threats every day. And this doesn’t account for everything that is created, just what reaches us.

It is not just a question of exponential growth, but an increasing trend. By 2009, our Collective Intelligence database contained almost 40,000,000 classified threats, and in 2010 we added some 20,000,000 more. That means we now have more than 60,000,000…

Five years ago, there were only 92,000 strains of malware cataloged throughout the company’s 15-year history. This figure rose to 14 million by 2008 and 60 million by 2010, which gives a good indication of the rate of growth.

The reason for this spectacular increase is clear: profit. The year 2003 saw the creation of the first banker Trojans and polymorphism. i.e., creating numerous variants of a threat to avoid detection by antivirus products, as when a threat is detected, it will no longer be able to effectively infect computers and steal data. Since then these malicious codes have become one of the most common types of malware.
Every day, increasingly sophisticated variants emerge, designed to evade the security measures put in place by banks, online stores, pay platforms, etc. Several organizations have tried to bring together members of the IT security industry to counter the efforts of cyber-criminals. It is a long, hard struggle however, and it is not yet clear that it is one we can win.

In general, the reason that more Trojans, keyloggers and bots are created than other types of malware is that they are more useful for identity theft. In 2005, almost half of new malicious codes were Trojans.

Now, at the end of 2010, the situation is worse still, with Trojans accounting for 71 percent of new malware.

As with any other business, cyber-crooks seek to maximize the effectiveness of their operations. When developing Trojans, they have to decide which platforms to attack and the number of potential victims. Unsurprisingly, Windows is the target in 99 percent of cases, as it is the most widely-used operating system.

The ultimate objective of these cyber-criminals is to profit financially from malware. Trojans are the perfect tool for stealing information. However, this information still has to be converted into hard cash, and criminals are always on the lookout for innovative ways of achieving this.
3. How the black market works
When we talk about the black market, it often invokes an image of spy rings and gangsters rather than the quite real situation which is dictating the way that the security industry must act.

But what is the black market, and how does it work? Who are the chief operators? What happens after a Trojan is created? How is money obtained and laundered?

Let’s first take a look at the various cyber-criminal profiles.

The cyber-criminal professions

We have often described how online mafias are highly organized regarding strategic and operational vision, logistics and deployment. Not only do they seem like real companies, they are also international organizations operating across the globe.

The FBI has recently classified the different ‘professional positions’ they have encountered in the cyber-crime business, in an attempt to describe the most common figures that profit through online theft, extortion and fraud.

According to the FBI, cyber-crime organizations operate like companies, with experts specialized in each area and position. Yet unlike most companies, they don’t have timetables, holidays or weekends.

The most common ‘positions’ or specializations according to the FBI are:

1. Programmers. Who develop the exploits and malware used to commit cyber-crimes.
2. Distributors. Who trade and sell stolen data and act as vouchers for the goods provided by other specialists.
3. Tech experts. Who maintain the criminal enterprise’s IT infrastructure, including servers, encryption technologies, databases, and the like.
5. Fraudsters. Who create and deploy various social engineering schemes, such as phishing and spam.
6. Hosted systems providers. Who offer safe hosting of illicit content servers and sites.
7. Cashiers. Who control drop accounts and provide names and accounts to other criminals for a fee.
8. Money mules. Who complete wire transfers between bank accounts. The money mules may use student and work visas to travel to the U.S. to open bank accounts.
9. Tellers. Who are charged with transferring and laundering illicitly gained proceeds through digital currency services and different world currencies.
10. Organization Leaders. Often “people persons” without technical skills. The leaders assemble the team and choose the targets.
Cyber-crime organizations have a hierarchical structure whereby every action is performed by specialists. If you think about the different countries they are present in, you will get a clear idea of the number of people involved in these criminal activities, and who benefit from the anonymity provided by the Internet.

The process…

**Step 1. Creating malware and finding victims**

The heads of the criminal organizations start the ball rolling; they contract programmers and hackers, along with other technical experts, to launch indiscriminate attacks. Sometimes they will operate on their own and other times in coordination, often certain individuals will have several roles.

We have described this process on several occasions, and there is nothing much new in terms of the methodology. In general, hackers belonging to the criminal organization assign other hackers (or they take on the task themselves) the task of creating, phishing, bots, spam, fake Web pages to be indexed on search engines, etc.
Social engineering is then used to trick victims through the most popular distribution vectors: email continues to be one of the most frequently used, although now social media (such as Facebook, YouTube, MySpace, Twitter, etc.) and fake Web pages positioned on well-known search engines (so called BlackHat SEO) are becoming increasingly popular.

The freedom and international nature of the Internet contributes to the task in several ways:

- New malware can be created and distributed in just a few minutes, thanks to pre-prepared kits, the online purchase of computer threats and the simplicity with which the message -with a little bit of social engineering- can be distributed across popular channels.

- Threats can be created in many different languages, or simply in English as a common language, reaching victims across many countries.

We have previously mentioned how the most common target is Windows, as it offers the greatest mass of users who access all types of online services: banks, shops, payment platforms, etc. Nevertheless, Apple platforms are becoming more attractive as the market share has grown over the last two years, particularly due to the launch of devices such as the iPad, iPhone, etc.

Once victims have been caught in the trap and their bank or credit card details, etc. stolen, this information is stored on a server to which hackers can access, and from then on, they can enter users’ accounts or use cards without their knowledge.
Step 2: Sale of data and money laundering

One of the most frequent questions we hear is: If these cyber criminals have the bank details, why don’t they just steal the money and keep it themselves? The truth is sometimes that is what happens, but it is not the norm.

Much of the data ends up on the black market, or is distributed to others that sell it to the ‘end-user’. The reasons are simple:

- It is less risky to traffic in data than it is to steal directly.
- Very often the crime is committed in a different country to the one where the profit ends up: the more intermediaries in the chain, the more difficult it is to track down criminals.
- Moreover, these organizations can then offer other services, not just the sale of the data itself, as we will see later.

Once the information is on the market, it is the ‘resellers’ that take care of selling it. Interestingly, this market is the same one through which the hackers were originally contracted or the Trojans, bots, or kits were bought.
These types of markets operate in line with the normal laws of supply and demand: there are competing prices, additional services are offered, free trials, money-back guarantees if the data doesn’t work (or if the account doesn’t have a guaranteed minimum balance)... even anonymous shopping by third-parties.

Offers are posted on underground sites, and potential criminals who want to use this information (both the numbers and the copied magnetic strips) to clone cards which they can then use in ATMs, to steal money directly through transfers or simply to shop, use a series of discreet methods to contact the seller and purchase the goods.

Those that opt to steal money directly from accounts, through bank transfers and often for considerable sums, have to add another link to the chain: they need ‘mules’ in order to launder the money.

To recruit them, they post false job offers, promising high commission (between 3% and 5% of the total money laundered) just for receiving the money in a bank account and then forwarding it via services such as Western Union. These mules, who are also victims, frequently don’t know what they are doing and just see an easy way to make money.

**Example: False Job Offer**

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:
- Managing accounts with certain banks or payment systems;
- Receiving 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, Traveler’s Checks.

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 1,000 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.departmentana@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
For the criminals, adding another link in the chain (often in a different country) covers their tracks even more, and leaves the mules as scapegoats who will be arrested in the event of a forensic investigation into the crime.

These mules are rarely active for very long, as whenever victims report the theft from their accounts and there is an investigation, it is easy to track down the account to which money has been forwarded, but from there on the trail is lost…
4. The black market at-a-glance
Below we offer a brief overview of some of the typical offers available on the black market:

<table>
<thead>
<tr>
<th>Products</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit card details</td>
<td>From $2-$90</td>
</tr>
<tr>
<td>Physical credit cards</td>
<td>From $190 + cost of details</td>
</tr>
<tr>
<td>Card cloners</td>
<td>From $200-$1000</td>
</tr>
<tr>
<td>Fake ATMs</td>
<td>Up to $35,000</td>
</tr>
<tr>
<td>Bank credentials</td>
<td>From $80 to 700$ (with guaranteed balance)</td>
</tr>
<tr>
<td>Bank transfers and cashing checks</td>
<td>From 10 to 40% of the total</td>
</tr>
<tr>
<td>Online stores and pay platforms</td>
<td>From $80-$1500 with guaranteed balance</td>
</tr>
<tr>
<td>Design and publishing of fake online stores</td>
<td>According to the project (not specified)</td>
</tr>
<tr>
<td>Purchase and forwarding of products</td>
<td>From $30-$300 (depending on the project)</td>
</tr>
<tr>
<td>Spam rental</td>
<td>From $15</td>
</tr>
<tr>
<td>SMTP rental</td>
<td>From $20 to $40 for three months</td>
</tr>
<tr>
<td>VPN rental</td>
<td>$20 for three months</td>
</tr>
</tbody>
</table>

• **Contact:** Via ICQ, Messenger or similar or via email (generic addresses).

• **Try & Buy:** Most offer tests or free demos. They also use online sites for checking algorithms to guarantee the authenticity of the card details.

• **Minimum orders and bulk discounts:** Minimum orders are established (5 or 10 units in the case of credit card or bank details). There are discounts for bulk buying.

• **Specialized online stores:** Once contact has been made, many use online sites set up as stores for distributing their products (which can’t be accessed without a username and password).

• **Methods of payment:** Western Union, Liberty Reserve, WebMoney or similar.

• **Customer services and support:** They offer service guarantees. If the product does not work (if the numbers, login credentials are not valid, etc.), they will be changed for others that are operative.

• **Promotion:** These services are mainly advertised through underground forums, although some of the boldest use social media and have accounts on Facebook and Twitter, etc.
5. The sales process
Obviously, the black market has its own peculiarities: Clandestine activities require a series of precautions, and to this end the cyber-criminals who put the products in the marketplace are no fools.

We will now take a look at the products that are available on the Internet, as well as each phase of the sales process. We must remind you that the information contained in this report is from 2010. In fact, the oldest references just date back to last June.

The product

There has been much written about the black market in recent years, above all because it was a tangible reality behind much of the information that the security industry has been publishing for some time now: behind every threat, every Trojan, every bot... there is business.

However, we have focused considerably in the past on the sale of credit cards, but this is just a small part of what is sold on the black market. Here is a list of the different products on offer.

Credit cards.

Of course, credit cards still figure largely. Yet the illicit sale of these has become much more professional:

- **Different issuers.** It’s not just AMEX, VISA or Maestro cards that are offered, but also those of many different international institutions, and they are organized by country, each with a different price. As a general rule, cards from European and Asian countries are more expensive than those issued from the US or Canada.

  - The most popular cards are Visa Classic, Visa Gold, Visa Platinum, Visa Business, Mastercard Standard and Gold / Platinum, and American Express.

  - Details from these cards issued in the US can cost as little as $2 for basic information, and $25 for standard cards ($40 for Gold, Platinum and Business) with complete information. Prices for European cards rise to $5 in the first instance, and $50 for full information ($90 for most exclusive cards). The prices vary of course among different vendors, but these are average prices calculated from the information we have obtained across these sites. As we will see later, there are also discounts for bulk buying.

  - DUMP$ EURO:
    - AUSTRALIA, SPAIN, SWITZERLAND, TURKEY, ARABIAN (101) class - 120 USD, OTHER - 170 USD
    - GERMANY (101) - class - 120 USD, OTHER - 150 USD
    - ITALY (101)(201) - CLASSIC - 120 USD, OTHER - 150 USD
    - INFINITI - 500 USD
    - ASIA (101)(201) - class - 80 USD, OTHER - 100 USD
    - Amex - 80 USD
Delivery details. In the past, the credit card number was delivered with the PIN. Now however, the amount of data needed has increased considerably, and the information delivered covers all the needs for any online or offline operation.

The following data is supplied when buying credit card details:

**Physical credit cards**

This is a relatively new feature in the offer of products. Now hackers have gone from offering credit card numbers and the corresponding verification details (which can be used directly for operations on the Internet or in ATMs with cloned cards), to directly supplying the physical cards, for a greater fee obviously.
Prices vary according to the vendor, although the average is $150 for a complete card and a minimum order of five units. There is an additional cost for the plastic: $30 white plastic, and $80 for color printing. You also have to add to the cost of the information (the card number, PIN and other details) for which, as we’ve seen before, there are various offers.

The sellers guarantee the quality of the card (the image below talks about 2,800 dpi) and that it will be identical to the bank original, even including the hologram.

**Example: Credit Cards Description**

1) Manufacturing plastic cards ready for shopping
2) Record on white and color plastic.
   1) Manufacturing quality is made on the newest equipment with use of own technologies.
   1) Make following kinds of cards:
      MasterCard
      Visa
      AMEX
   I guarantee a correct bank microfont, with an excellent sig stmp. 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.
Card cloners and fake ATMs
And why stop there? Why not offer the cloning machines so that users can create their own cards? This ‘added-value’ service is also on offer. There are several different models, and prices run from $200 up to $1,000.

They also distribute fake ATMs. These can be installed over legitimate machines, so when someone goes to use them, the fake machine registers all information including card numbers and PINs. In some cases, they can also be set to steal the physical card, which can then be used by the criminals. The cost of one of these fake cards can reach $3,500. Delivery is free.

EXAMPLE: CARD CLONERS AND FAKE ATMS

**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:** $500
**MSR505 = MSR3000:** $450
**MSR206 = TA-49:** $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/Write magnetic stripe card complied with ISO 7811/1~6 formats
- Read/Write High & Low Coercive force of magnetic stripe (300~40000G)
- High/Low Coercivity encoding circuitry selectable on screen
- Program software for Windows 98/Me/XP
- Programming software for various read/write performance
- Programmable, led by, raw data, EMV, and user defined format
- 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=35ps operational swipe speed of writing data
- 5=55ps operational swipe speed of reading data
- +24VDC+-10%, 2.0A Max., external power adapter attached
- Good size with dimensions of 210(L) x 50(W) x 65(H) mm
- CE, FCC, UL, cUL certified

**Price:** $200
With Free Shipping.
Bank accounts
Criminals do not restrict themselves just to the sale of credit card information, they also directly offer the details needed to access online bank accounts. The list of banks for which information is available is very long:

**EXAMPLE: BANK ACCOUNTS**

<table>
<thead>
<tr>
<th>Available bank logins</th>
<th>hsbc</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alliance &amp; Leicester</td>
<td>halifax</td>
</tr>
<tr>
<td>Abbey bank</td>
<td>Jodrell Bank</td>
</tr>
<tr>
<td>Barclays</td>
<td>Lloyds TSB Bank</td>
</tr>
<tr>
<td>Bremer Online Banking</td>
<td>Northern Bank</td>
</tr>
<tr>
<td>Banque Nationale</td>
<td>Natwest</td>
</tr>
<tr>
<td>Banque Nationale</td>
<td>RBC</td>
</tr>
<tr>
<td>Oldbank</td>
<td>Royal Bank of Scotland</td>
</tr>
<tr>
<td>Chase Bank</td>
<td>Postbank</td>
</tr>
<tr>
<td>Credit Union</td>
<td>Pen Air Federal</td>
</tr>
<tr>
<td>First Trust Bank</td>
<td>Wells Fargo</td>
</tr>
<tr>
<td>Flagstar Bank</td>
<td>Wamu</td>
</tr>
<tr>
<td>HDFC Bank</td>
<td>Wachovia &amp; Bank of America. And more</td>
</tr>
</tbody>
</table>

Once again, the prices vary depending on the bank in question. And similarly, there are different prices depending on whether the information corresponds to an account with a guaranteed balance or not.

The guaranteed bank balance can be as much as $0.5 million and start at $20,000. Depending on the type of bank (and its security measures) as well as the available balance, prices for information range from $80 to $700.

It is important to bear in mind that many of these vendors distinguish between personal accounts and business accounts (which have higher available balances).
Bank transfers and cashing checks
These same vendors also offer bank transfers. The most obvious reason is for the laundering of money. This is effectively the same work that is done by ‘mules’ enticed by fake job offers.

The commission charged also varies: anything from 10% to 40% of the amount transferred. Competition among vendors appears to center around the speed of the transaction (and the security) rather than the commission itself.

**EXAMPLE: BANK TRANSFERS AND CASHING CHECKS**

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 I’m informed of successful pick, I can make the transfer right away if the send back option is LR (already available) or WM2 (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:**

<table>
<thead>
<tr>
<th>Amount Received</th>
<th>My Cut</th>
</tr>
</thead>
<tbody>
<tr>
<td>$200 – $999</td>
<td>40%</td>
</tr>
<tr>
<td>$400 – $999</td>
<td>30%</td>
</tr>
<tr>
<td>$600 – $999</td>
<td>20%</td>
</tr>
<tr>
<td>$1,000+</td>
<td>15%</td>
</tr>
</tbody>
</table>

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

LR and WM2: 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 // TELL / Regions / Wells / etc. contact us if you don’t have acct with the following banks.

if we try 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 receiver country and amount to be transferred.)

Sale of online service accounts
For a modest amount, you can also buy accounts for Paypal, eBay, Click and Buy, AlertPay, MoneyBookers, webmail (Hotmail, Gmail, etc.) or social networks (Facebook, Twitter, etc.).

Prices in these cases tend to vary not by country, but by the age of the account. For example, if the account was set up less than three months ago, the price is 80% higher than if there is no guarantee to the age of the account. Evidently, more recent accounts tend to have more activity. In the case of Paypal, prices start at $10 (with no guarantee on the age of the account, but with verified access). Again, accounts with guaranteed balances fetch higher prices: $80 for an account with a guarantee of $1,500.

**EXAMPLE: SALE OF ONLINE SERVICE ACCOUNTS**

Paypal Login:
We Have Verified And Unlimited Paypal Account With Balance And Add Co And Bank Acc +++. All Our Paypal Acc Have Full Info And With Email Access and With All Security Answer. And With Origin Ip And A Program For Fake Your System Ip To Origina Ip For Full Access To PayPal Acc.

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

MoneyBookers Account:

ClickAndBuy And Alertpay Account Is Available ....
Design and publishing of fake online stores
Another new service on offer is the creation, development, implementation and indexing of fake online stores. The objective here is clear: to trick the public into buying goods which they will never receive, and in addition, to obtain credit card details.

Purchase and forwarding of products
Many of the buyers who are looking for credit card details use them to buy goods. This is a way of immediately laundering the money. But there is a small problem: they have to give details for identifying the buyer and sending the merchandise.

With this in mind, vendors also offer a service for purchasing goods and forwarding them to any address, thereby preventing the buyer from being located.

Obviously this service also comes at an additional cost:
Rental of botnets for sending spam
This service is not new. In fact, many of the botnets created every day are designed specifically to send spam, and hackers charge for these services. It is particularly aimed at users that want to send spam safely: databases with spammable addresses; rental of systems from which spam can be sent (botnets); VPNs to connect anonymously to control panels, etc.

EXAMPLE: RENTAL OF BOTNETS FOR SENDING 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 using SMTP where ,and forums"

u will get them using thirst scanner "Itscan"
The contact

The criminals involved in these activities obviously use all types of strategies to avoid detection. Although they advertise on threads in public forums, it is not easy to find them. These types of communities often have a common feature: they are essentially underground, aimed at a very specific target market.

Once you come across a post offering these services, practically the only way of contacting with the vendor is through instant messaging: ICQ, Yahoo Messenger or similar. Others offer the possibility to contact via email (using of course, free webmail addresses).

Those who can be contacted through ICQ or similar channels, will normally specify a timetable of availability: maybe 24 hours, or maybe office hours. They even advise when they will be on holiday.

Some even reveal their geographic location to aid the logistics of connection (in the image below, GMT + 8). There is no surprise here, as many of these cyber-mafias operate from Russia or neighboring countries, such as China or other Asian states.
Try & Buy

“Search, compare, and if you find a better offer we will return your money...”. This could be the slogan of any advertising campaign, but it is also the case on the black market. Especially with the economic crisis—and with people struggling to make a living—these types of services are on the increase. The main concern is to generate trust among clients. After all, we’re dealing with criminals here.

Here there are two extremes: those who offer (and advertise on these forums) free trials for credit card numbers and bank details, etc., to test the quality of the goods, and those who clearly specify that there are no free trials, but who guarantee their product (if it doesn’t work, the data will be substituted for others).
EXAMPLE: TRY AND BUY

PERSONAL DETAILS:

SMTP Domain Sample:
http://cybermail.com
user:john.doe@cybermail.com
password:secret123
SMTP IP Sample:
195.227.139.252 - test/test
smtp 88.2.161.78-eua-eua 80.140.7.11-mail-mail123 64.173.103.196-david-1234 212.122.224.24-
test-123456 217.37.5.03-sonia-password
203.191.153.66-test-123456

N: B
I DON'T GIVE FREE TEST, IF YOU WANNA BUY, YOU BUY AND TEST .... NO S**T TALK
PAYMENT METHOD: LIBERTY RESERVE* LR*, WMZ, ....
Online testing

Some allow the validity of the data to be verified through an online system supposedly connected with applications such as iTunes or similar checks on the credentials based on the various algorithms used by banks to generate the numbers.
### Account Details

<table>
<thead>
<tr>
<th>Username</th>
<th>Password</th>
<th>Did this login work out for you?</th>
</tr>
</thead>
<tbody>
<tr>
<td>hello</td>
<td>ayishetu</td>
<td>Yes No</td>
</tr>
<tr>
<td>cantonais</td>
<td>sbrahma</td>
<td>Yes No</td>
</tr>
<tr>
<td>treasure210</td>
<td></td>
<td></td>
</tr>
<tr>
<td>habongol0</td>
<td>lambr10</td>
<td>Yes No</td>
</tr>
<tr>
<td>lootware</td>
<td>potoparty</td>
<td></td>
</tr>
</tbody>
</table>

Each account has a note indicating whether the login worked or not, along with the password used. The website also has a feature to select and use passwords from the list, with a success rate indicated for each entry.
Minimum orders and bulk discounts

Of course practically all vendors demand a minimum purchase for many of the products of (particularly low cost products, such as credit cards or bank details) and also offer discounts for bulk buying.

Specialized online stores

After contact is made through the agreed channels, in some cases the products will be sold and delivered directly and in other cases the credentials will be provided for accessing online stores through which buyers can purchase any of the goods, just like a normal store. That said, actually reaching these stores is no easy task, and impossible without the password.
Sign Up for CVMASTERSTEAM 2010
Apply for membership now. If you're already a member, sign in.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Address</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
<tr>
<td>Retype Password</td>
<td></td>
</tr>
<tr>
<td>Birthday</td>
<td></td>
</tr>
<tr>
<td>Month</td>
<td></td>
</tr>
<tr>
<td>Day</td>
<td></td>
</tr>
<tr>
<td>Year</td>
<td></td>
</tr>
<tr>
<td>Two Words</td>
<td></td>
</tr>
</tbody>
</table>

By signing up, you agree to the Terms of Service.

About CVMASTERSTEAM 2010
We sell legitimate CODC, currency, drugs, and out-of-country SHOPS. We guarantee accessibility and anonymity of our customers.
Безопасность переговоров
- Безопасность бизнеса

Меню
Главное
описание сервиса

Регистрация
рекомендации по регистрации

Особенности
рекомендации по подключению

Безопасность
аспекты безопасности

Оценка
оценка для ознакомления

Оформление
описание продукта

О сервисе


Чем мы отличаемся от конкурентов других сервисов?
- Все почты (включая jabber, так и на всех серверах) закрыты.
- По умолчанию сервер использует защищенное SSL-соединение. Если Вам нужна большая защищенность, можно позвонить нам использовать дополнительное шифрование трафика (ключи шифрования OpenPG).
- Открытая регистрация и бесплатное пользование услугами сервиса.

Information
После входа в ДШ в которого размещены наши аккаунты, работа TheSecure.Biz была перенесена. После проверки удаления, было сделано заявление, что информация была восстановлена и на ДШ. В связи с этим удалялась база аккаунтов пользователей Jabber сервера.

В данный момент джаббер сервер разработчики своими силами, они же, как и ранее, совершенствовали процесс регистрации аккаунтов. Они помогут вам зарегистрироваться в сети вы можете через джаббер-сервер, новый железный, используя свой же.
Login:

Password:

Stay signed in

Log In

On registration issues please contact jabber.vmd@jabber.cn
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? No problem, you are not required to post. To gain full access, you must be registered.

- All questions about advertising on the forum must be directed to the moderators.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
- All attachments must be relevant to the topic, and must not contain malware. All attachments are reviewed and moderated.
Methods of payment

Almost without exception, the payment method used by these hackers is through money transfers services. The most commonly used are Liberty Reserve and Western Union, but there are others, such as Webmoney, which are also mentioned. Needless to say these services guarantee anonymity which wouldn’t be the case with payment by credit card or normal bank transfers, etc… And given the sort of merchandise on offer, who would want to pay these people by credit card?
Customer services and support

One common feature across these types of sales is the offer of exchanging products if they do not meet the buyer’s expectations; basically, if they don’t work. Some will establish a return period (as with normal shops) which in some cases is limited to the first 24 hours after the goods are received.

EXAMPLE: CUSTOMER SERVICES AND SUPPORT

- 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!]
- (MWZ[LR]) - NO MINIMUM!!! DON'T LOOSE YOUR CHANCE
- (WU)MINIMUM-550$]
- High valid rate 95% valid.
- Daily update.
- Lowest price.
- I'm not resellers like somebody else.
- I am not checking dumps before u ask. Am very very sure in quality of my dumps and you'll 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.
- replayed always will be checked!!!
- If u cheat me for replacements I will put you ignore list!!!

*Order Rules*
- Give me bin u need in same line message and i’ll answer u to pay total.

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

*Delivery Rules*
- Instantly delivery.

*All prices and countries contact on IQ*
- Contact me!!
Promotion

And finally, as with any business, these hackers need to advertise themselves, although with great care... In addition to posting offers on underground forums, some of the more daring go much further: using social media to advertise directly.

Carders.CC - Fangruppe

45 16 161 5

Siguendo 16

And there is also room for complaints, as with any online product or service:

EXAMPLE PROMOTION

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. How to minimize the risk?
As we always insist, the best way to protect yourself is to use common sense (sometimes the least common of the senses). And of course, to have good protection on your computer (if it is your own) and to cover all possible infection vectors on a network (in the case of companies).

Yet there are other good practices which can also help, particularly if you use online banking, or when you shop or make transactions, whether online or offline, etc. These are as follows:

What to do

- Keep all your personal information in a secure place.
- Sign credit cards as soon as you receive them.
- Be alert when paying in any establishment (when paying by card, make sure your card is always in view).
- Save receipts and compare them with your bank statement, to detect any irregularity.
- If you detect any suspicious transactions in your bank account, quickly inform your bank or the issuer of your credit or debit card.
- Be careful with physical correspondence: It is advisable to destroy any invoices or letters that include your name, address, Social Security details, account number, etc..
- Check invoices thoroughly for any unauthorized items or actions.
- Check your credit card statements carefully.
- If you have any doubts about the validity of messages received from any banks, online stores, payment platforms, etc, contact the customer services department of the company from which the message has supposedly been sent.
- If you are on holiday, ask someone you trust to collect your mail and save it while you are away.
- Most banks and credit card companies offer notification services for any transactions. Use this service.
- Never give any personal information by telephone or on the Internet if you do not know the company or the website. And even then, be careful.
- Save all ATM receipts or destroy them. They may contain confidential information.
- Memorize your passwords, do not save them on your computer or in your telephone book.
- Install a good antivirus and a good firewall on your personal computer to prevent theft of your identity or confidential data. Try to ensure that you have the latest protection technology, which can detect new malware without having previously identified it.
- Keep your antivirus up to date.
- Close all active Internet and browser sessions and never save passwords on your computer.
- Delete data from your computer when you have completed an online transaction. Pay special attention to temporary files, cookies, etc.
What not to do

• Never give your card to anyone, keep it with you at all times.
• Never sign a blank receipt.
• Never give your account number or passwords over the telephone, unless you are 100% sure about the reliability of the company or you have initiated the call to request a service.
• Never include your Social Security number or telephone number in checks.
• Do not respond to unsolicited emails, IM messages, SMS, or pop-ups that appear to come from a bank, credit card company, telephone company, online store, payment platform, etc.
• Never use your debit card for online purchases. These are far less success than credit cards.

What to do if you have fallen victim

At present, most banks, financial entities, credit card issuers, etc. will often bear the cost if you have been a victim of fraud. That’s why it is essential to detect it and report it as quickly as possible:

• Contact the bank or financial institution with which you have the account or card that has been the target of the fraud. Cancel all cards and stop all payments. Change your bank or card passwords.
• Report the crime to the police. Banks, credit card companies and other institutions may insist that you report the crime.
PandaLabs is Panda Security’s anti-malware laboratory, and represents the company’s nerve center for malware treatment:

- **PandaLabs** creates continually and in real-time the counter-measures necessary to protect Panda Security clients from all kind of malicious code on a global level.

- **PandaLabs** is in this way responsible for carrying out detailed scans of all kinds of malware, with the aim of improving the protection offered to Panda Security clients, as well as keeping the general public informed.

- Likewise, **PandaLabs** maintains a constant state of vigilance, closely observing the various trends and developments taking place in the field of malware and security. Its aim is to warn and provide alerts on imminent dangers and threats, as well as to forecast future events.

- For further information about the last threats discovered, consult the **PandaLabs** blog at: [http://pandalabs.pandasecurity.com/](http://pandalabs.pandasecurity.com/)