State and trends of the “Russian” computer crime market in 2010

Group-IB
107023, Moscow, Mazhorov pereulok, building 14, block 2
+7 495 661-55-38
www.group-ib.ru

Contents

Introduction

The report contains the survey results of the state of the "Russian" computer crime market in 2010. It focuses on the main threats related to different types of hacker activity, analyzes general services offered by computer mafia, estimates "Russian" segment share in the global cybercrime market and gives predictions on the market development tendencies for this year.

The report is prepared by analysts of Investigation Department and specialists of Cyber Forensic Laboratory of Group-IB in association with experts of ESET Viruses research and analysis center and analysts of LETA company.

About companies

Group-IB (www.group-ib.ru) is the first company in Russia and CIS which is professionally and fully engaged in investigation of computer crime cases, violations of information security and computer forensics. It is a part of LETA Group.

ESET (www.esetnod32.ru) is an international developer of antivirus software and computer security solutions for corporate and home users. ESS Distribution Company, possessing exclusive rights to all ESET products in CIS countries, is a part of LETA Group.

LETA (www.leta.ru) is one of leaders of information security market in Russia. It is the first Russian operator of typed IT-services which provides its customers with complex solutions on information security. It is a part of LETA Group.

General notes

1. "Russian" cybercrime market is a market of computer crimes committed by citizens of the Russian Federation, CIS and Baltic states as well as by immigrants from Former Soviet Union Republics who live in other countries. The cybercrime market of Russia is an integral part of "Russian" market and it represents a market of computer crimes committed exclusively by the Russian Federation citizens.

2. Market expansion and simultaneous reduction of the prices for services led to increase in number of worldwide hacker attacks and growth of financial performance in 2010.

3. Group-IB experts estimate the global computer crime market turnover at 7 billion dollars while Russian cybercrime market share is estimated at 1.3 billion dollars. Total income of the whole "Russian" computer crimes market equals to a sum which is twice as much as the first one. Being located in different regions and committing their attacks all over the world, "Russian" hackers earned about 2.5 billion dollars in 2010.

4. Under corresponding factors of information technologies and cybercrimes markets development, it is possible to predict that this year "Russian" hackers will earn around 3.7 billion dollars and in 2013 they will double this amount. Approximately a half of the "Russian" industry revenue will belong to Russian intruders.

5. In 2010 the main threats from hackers were:
    - rampant increase in number and complexity of DDoS-atacks;
    - pointed attacks at financial industry and increase of incidents in online banking systems;
    - rapid burst of sms-fraud cases on CIS territory;
    - use of social engineering methods for stealing of personal information and online-frauds;
    - pointed attacks at crucial infrastructure objects.

6. To reduce activity of the hackers operating within the territory of CIS and Baltic countries, it is required to improve legal framework regularly and increase competence level of law-enforcement authorities which effect crime control in sphere of computer technologies. Also an important factor of cybercrime prevention is the development and implementation of innovative technical means and solutions which will allow realizing proactive response to revealed incidents and practically instant reaction to information security threats.

Definitions

Using a general term of "hackers" experts in sphere of computer crime investigation prefer to classify computer intruders a type of their specific activity and by a national identity.

In relation to the last one, a special attention is paid to the fact of significant difference in how the experts treat the term “Russian Hackers”. Russian computer criminalists prefer to denote by this term the Russian Federation citizens-violators who perform their criminal activities on the territory of the Russian Federation. In the USA and Europe the word “Russian” traditionally means not only citizens of the Russian Federation but also all those citizens and immigrants from the Former Soviet Union countries who are united by the common history and language. This feature is reflected in interpretation of the term “Russian hackers” by western countries specialists when they use it to indicate computer criminals for example from Ukraine, Baltic or Central Asia countries.

That is why one of the survey tasks is not only estimation of the cybercrime market in the Russian Federation but also analysis of the state of the whole “Russian” industry of the global market.

Thus, hereafter in this report the term “Russian” cybercrime market will denote the market of computer crimes committed by the Russian Federation citizens as well as by the citizens of CIS and Baltic countries and immigrants from the Former Soviet Union countries that live abroad. The crimes committed by “Russian” hackers on territory of both their residential country and other countries all over the world will be taken into account when analyzing financial indicators of the industry.

The term Russian cybercrime market will denote the market of computer crimes committed by the Russian Federation citizens only. Only the crimes committed by the Russian hackers on the territory of the Russian Federation will be considered when analyzing financial indicators of this industry.

General trends of cybercrime market development

The following general trends in computer crime market development may be marked in 2010:

- increase of professionalism of its participants. Each year we have to admit professional growth of hackers who spend substantial resources to perfect criminal schemes, methods and tools. First of all it is due to the fact that more and more market participants see their criminal activity as the main income source.

- market expansion due to appearance of new participants. A chance to earn multimillion revenue and absence of hacker rigid prosecution in many countries causes annual increase in cybercrime market participants number. In Russia the situation is additionally worsen by a great amount of technical universities graduates and by unstable home economy situation as the result of which the mentioned specialists cannot find highly paid legal income.

- decrease of prices for in-demand services. Appearance of new participants leads to competition improvement in this industry, thus price decrease and even appearance of discounts for "wholesale" customers. Customers may be provided with a test period of service and even be given money back guarantee.

- growth of the internal cybercrime market. This market includes so called Cybercrime to Cybercrime services (C2C). It means cases when hackers render services to colleagues. For example, in a case of fraud from online banking systems, violators can order services from a "cash-outer" (violators who cash out the stolen money). The case when malicious software developer orders "loads" from another violator may also be seen as another example. The market embraces large volume cash flows in different payment systems and requires special research for understanding the overall cybercrime market picture.

- an orientation to a super-monetization. Period of 2003-2009 was admitted by the transition of cybercriminality to 100% monetization of its activity. The last year has shown that violators are aimed first of all at super-profit receipt. Thus, in 2010 Group-IB specialists recorded a one-time fraud in online banking system in 1 million dollars. At the same time the violators continued the development of further activity monetization scheme. For example, mobile phone accounts actually became a form of payment system in 2010 and thus caught attention of cyber criminals. As soon as a possibility to monetize a mobile account appeared (remittance to plastic cards, monetization through short numbers by means of sms-aggregators and other types of money withdrawal) – relevant attacks also appeared (Winlock viruses, Trojan programs for mobile phones etc.).

A consequence of the above mentioned tendencies is the following fact – services offered on the cybercrime market became more accessible that causes growth of hacker attacks' amount all over the world and increase in financial performance. Herewith the cybercrime market develops according to classical market laws: market pricing, monopolies, business competition, etc.

Major threads

The year of 2010 is characterized by activation of computer violators as well as continuing professionalization of the market all over the world. During the studied period the major hacker threats were:

- rampant increase in number and complexity of DDoS-atacks;
- pointed attacks at financial industry and increase of incidents in online banking systems;
- rapid burst of sms-fraud on CIS territory;
- use of social engineering methods for stilling personal information and online-frauds;
- pointed attacks at crucial infrastructure objects.

1. Rampant increase in DDoS-atacks

Besides improvement of malicious software development technologies, last year it was stated the increase in number and complexity of Distributed Denial of Service Attack (DDoS-attacks). In 2010 it was fixed a DDoS-attack with flow rate of 100 Gb/s which is the most powerful attack for the whole period of observation. It is twice as much as the most rigid attack in 2009. Another example reflecting the current power of such attacks is extremely powerful attack on a famous Wikileaks site.

Last year an absolute record by total volume of DDoS-traffic was set up which exceeded the traffic amount of all previous years of observation put together.

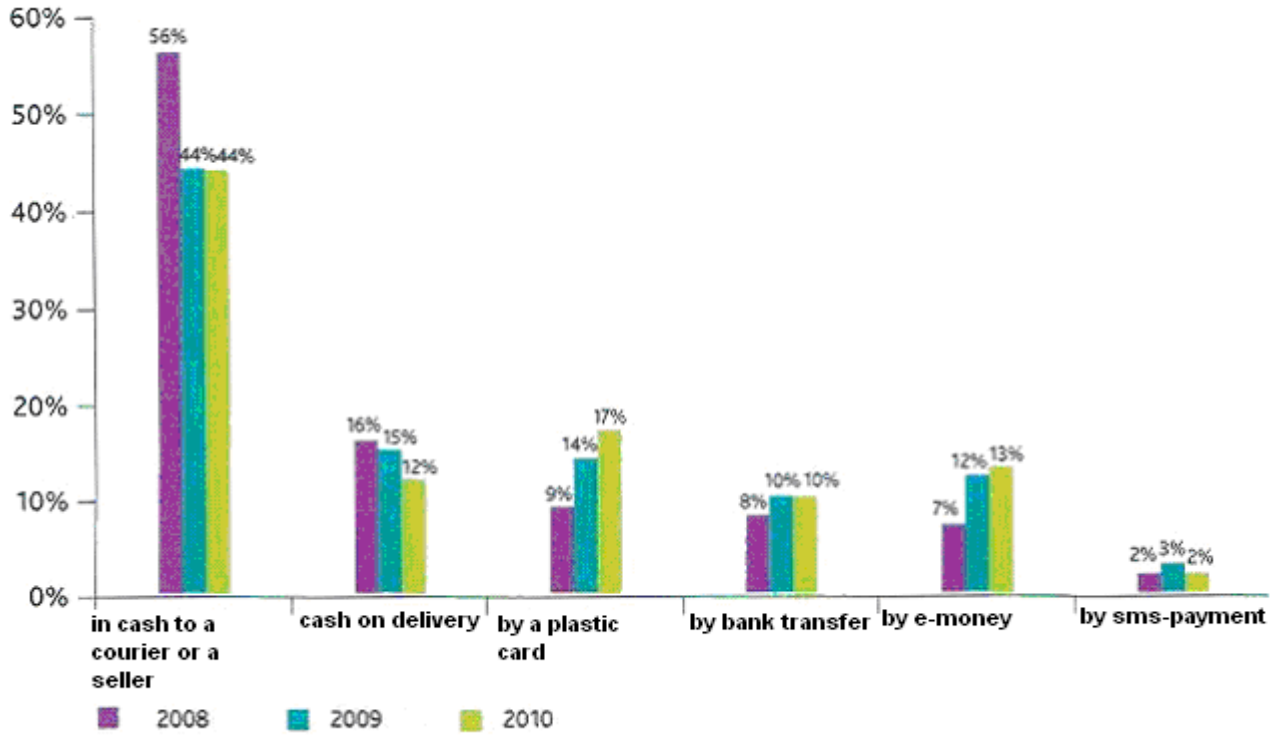
Decrease of such attacks cost is admitted alongside with growth of their complexity. That is why nowadays not only major customers but also those who are not so well-to-do address the cybercrime market for such services. Particularly that is the reason of rampant increase in DDoS-attacks on a global scale.

2. Pointed attacks at financial industry

FinCEN (U.S. Department of Treasury Financial Crimes Enforcement Network) has defined a cybercrime trend in financial sphere as the most fast-growing – quantity of such crimes has increased by 115 % during 2010. The most dangerous crime is fraud in online banking systems. In 2010 telebanking frauds in Russia became leading information security thread against the losses caused. In fact, it is a thread to the Russian Federation economy, bank industry, middle and small sized business. The spread of bank Trojan software and regular pointed hacker attacks at financial industry are caused by possibility to gain multimillion revenues. These threaten both legal and individual person monetary funds. It is related to an escalating use of internet-banking and internet-payments. In spite of payment in cash still being the leading payment method in RuNet, this category inevitably decreases last years that is accompanied by growth of payments by plastic cards and e-money. This indicates e-commerce increased popularity[1]. Payment by bank cards already shows a steady growth in comparison with other payment means. A bank card is akin to a mobile phone, it is convenient and above all this mass method of payment for services. Spreading of Internet payments by bank cards attracts fraudsters. Even now there is a great variety of money stealing from bank account schemes: skimming, shimming, phishing, viruses and multiple fraud techniques.

Figure 1. Online purchases payment methods in 2008-2010, RUmetrika pole

[1] Paying by bank cards is simple, quick and convenient // Internet in numbers. No. 4. 2010.



Source: Internet in numbers. No. 4. 2010

3. Rapid burst of sms-frauds

Total integration and spreading of a mobile communication has led to rapid growth of crimes in this direction. Development of new technologies such as mobile Internet, possibility to transfer money from one account to another, possibility to credit account in almost any part of the country and the use of mobile communication for various services payment has led to appearance of new methods of money stealing. Last year is characterized by growth of so called sms-fraud. As far as information security sphere is concerned, it is important to admit the burst of spread of malicious software intended for extortion money from a user. Such malware blocks the possibility to use a computer or makes its use inconvenient (for example, a half of a screen is covered by an image with a requirement to send sms on a short code). The computer may be unblocked only by receiving a code which is sent (but not always) in reply to a toll sms on a short code. It is necessary to note that this kind of fraud had strongly marked local nature and was widely spreading on the territory of CIS in 2010. It is related to the fact that in Western countries there are no content-providers which enable such scheme functioning and antivirus companies provide internet-services for free unblocking of infected computers.
Also some trends can be noted:

4. Use of social engineering methods: new wave

Another important trend in cybercrime world in 2010 is caused by growing popularity of social networks. More than a half of the world population under 30 is registered in social networks. Facebook exceeded Google in weekly traffic amount in the USA. This interest to such services from users led to appearance of a trend of malicious software distribution and managements of its installation through popular social services. Hackers were previously familiar to a mechanism of instruction transfer to a malware via instant text messaging systems but the massive use of such method hasn’t been registered yet. For example, forensic experts detected virus loaders that used Facebook messaging service as a tool of

commands sending and control of installation. Massive computer infecting leads to epidemics and enables hackers to create multimillion botnets.

5. Pointed attacks to crucial infrastructure objects

Last year experts in sphere of information security incident investigation registered unprecedented by complexity hacker attacks which enabled the violators to damage badly the IT-infrastructure of national economy large objects. Computer forensic specialists all over the world found the incident with Stuxnet warm to be the most expensive and technology intensive in viruses' creation history. It was the first case widely -publicized in Mass media that showed how to apply viruses for sabotage and terror attacks. Researches of degree of large industrial targets' security showed that currently the information security level of strategic industry companies doesn't correspond to new types of cyber threats. Moreover, the state of protection of Russian organizations is lower than world's average degree.

Overview of the "Russian" cybercrime market popular services

Basic components of the "Russian" cybercrime market

Within the report scope there were defined the following components of the computer crime market of Russia which are representing the greatest social danger:

- DDoS-attacks: network attacks intended to denial of service;
- Frauds in online banking systems: unauthorized sending of electronic payment order to steal money;
- spam: bulk e-mailing;
- traffic selling: services on installation of malware in a large number of computers and services on redirection of users to particular web-sites (related to C2Cmarket);
- partnership programs (illegal sales of medicines, sales of pirated software, downloads, etc.) (related to C2C market).

The following components of the "Russian" cybercrime market are interconnected:

- formation of botnets is directly connected with traffic sale;
- botnets are used to send spam, perform DDoS-attacks and fraud in online banking systems;
- spam mailing is used to promote services sold through partnership programs;
- DDoS-attacks are often performed when effecting unauthorized electronic payment orders etc.

Botnets as the main component of cybercrime market

The regarded components of the "Russian" computer crime market using botnets may be represented in the form of the following service schemes:

Table 1. Schemes of profit deriving from DDoS-attacks, fraud in online banking systems and spam mailing when using bot-nets

DDoS-attacks	Fraud in online banking	Spam mailing
Purchase of malicious software	Purchase of malicious software	Purchase of malicious software
Executable file encryption	Executable file encryption	Executable file encryption
Proxy server lease for botnet management	Proxy server lease for botnet management	Proxy server lease for botnet management
Traffic purchase ("installs")	Traffic purchase in particular regions of the RF	Traffic purchase ("installs")
Partnership programs	Sending payment orders	Partnership programs
Rendering DDoS-services	Cash withdrawal (cashout), its legalization	Purchase of data bases and accounts for mailing
Blackmail by DDoS-attack threat		Service rendering by message mailing

Source: Group-IB

DDoS-attacks, fraud in online banking systems and spam mailing as a component of computer crime

market should be considered from the point of development of botnet software component, final formation of botnets and deriving of profit from them.

Development of a software component of botnets may be represented in the form of the following services:

1. purchase of a malicious software used at botnet nodes (the price for such software is 3000 – 10000 USD);
2. encryption of the malicious software run files to complicate the detection of the program by antivirus software (the price of such service is 20 – 30 USD);
3. Proxy server lease for a managing botnet center. As a rule so called "bulletproof" hosting providers (which are loyal to existence of controlling botnet servers at their sites) are used (prices from 150 – 200 USD).

Final formation lies in botnet expansion by purchasing installs of malicious software on computers connected to the Internet in different regions and by participating in partnership programs (participation is free, traffic prices are stated below).

Botnets and major market services

Deriving of profit from formed botnets is carried out as follows:

- by performing DDoS-attacks: rendering of DDoS-services and blackmail by a DDoS-attack threat (according to open sources data the average price of a DDoS-attack is 70 – 90 dollars per attack day. According to advertisements on private resources the price is 300 – 500 dollars per attack day; the difference in prices appears due to difference in quality of the rendered DDoS-services and complexity of typical missions);
- by means of fraud in online banking systems: unauthorized mailing of electronic payment orders for large sums, their cash out ("upload") and legalization (average loss caused by incidents of such kind - from 70 to 100 thousand dollars);
- by means of spam mailing: rendering of services of spam mailing using e-mail address databases and instant messengers as well as services of spam mailing in social networks (a million e-mail address database costs 500 – 1000 dollars, 1000 social network accounts for spam mailing cost 30 – 50 dollars).

Download selling

Often botnets are used for sale of software loadings. In such case botnet nodes download programs provided by customers (Trojan software or Windows lockers as a rule). Herewith loadings in different parts of the world have different price categories. The cheapest regions are Asian countries and South America. The prices for downloads in European countries and the USA are higher. Download selling services are very popular among violators, earning their money on telebanking system frauds, in particular countries only because they allow building of botnet from computers used in accounting in the countries for which the intruders already have cash out and money legalization schemes.

Standard prices for 1000 downloads ("infected" computers) in different world regions are represented in Table 2.

Table 2. Prices for 1000 downloads

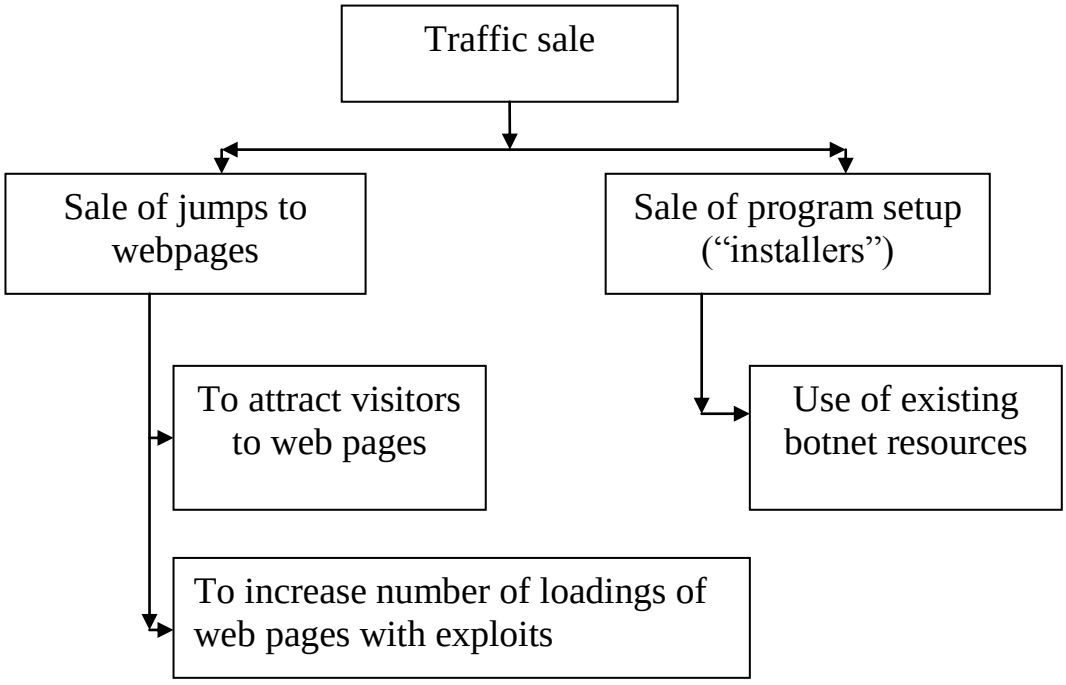
Region	**Price**
Asia	10 – 12 USD
South America	10 – 12 USD
USA	100 – 140 USD
Europe	70 – 130 USD
Russia	20 – 40 USD

Source: Group-IB

Traffic selling

Traffic selling may be performed in the form of selling of web-site visits in order to attract users to different web-sites (on-line shops selling medicine, porno sites, etc.) or to increase amount of users with fragile web-browser versions who visit exploit sites which leads to download and launch of malware on user computers (including those used for botnet creation). Selling of web-sites visits is often related to hacking of popular Internet portals inserting a code redirecting a web-browser to the page of a customer who purchased visiting service. The cracked portals are sold as resources with installed shells (scripts for system remote management). Average cost of 10 shells is from 900 to 3000 dollars.

Figure 2. Traffic selling scheme

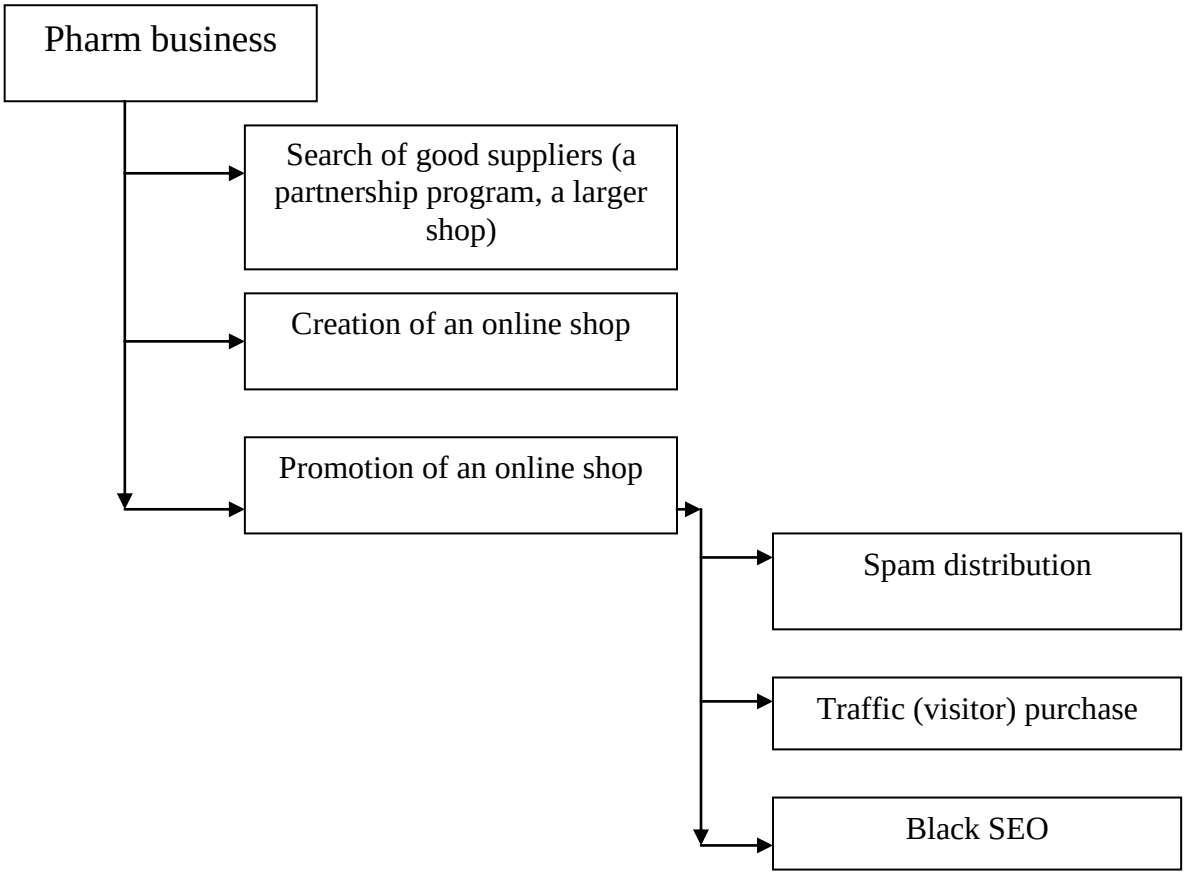


Source: Group-IB

Partnership programs and illicit pharm business

This type of cybercrime activity is marked as a separate direction of cybercrime sphere because it was one of the first direction and still keeps the leading position among partnership programs. Illicit pharm business is a reselling of counterfeit medicines and medicines which sales are subject to legal control (drugs are often received from lager online shops or sold immediately through partnership programs). Pharm business existence is based on advertisement of Viagra, steroids and other drugs by means of spam distribution, application of black promotion methods (black SEO) and attraction of online shop visitors by traffic purchase which is described above. Spam distribution throughout 10 million address database costs approximately 350-1500 dollars. Any other illegal business can be organized according to a similar scheme.

Figure 3. Online pharm business scheme



Source: Group-IB

Other spam related services

Spam mailing is extensively used by cybercriminals to increase sales of counterfeit software (operation systems, office applications, etc.) and to spread malicious software as scareware and pseudo firewalls.
Scareware and pseudo firewalls are used to extort money from users by asking payment for removal of computer viruses or for authorization of assertedly counterfeit software and different audio and video tracks found. Often the functioning of such programs is similar to Windows blockers, thus the program does not allow user working on the computer until the payment is performed.

Often promotion of serviced advertised via spam is performed through partnership programs: in terms of partnership programs the users having no direct relation to the advertised services independently from each other generate spam reference, containing links to goods and services, and receive revenue which depends on the number of clients attracted to the online shop.

Financial indicators of computer crimes market

Cybercrime market of any country is a part of its shady economy that can be approximately evaluated basing on implicit facts. Nevertheless, it must be admitted that due to the violators' activity stated above and to development of attack technologies and methods the global cybercrime market showed in 2010 an impressive growth rate of financial indicators.

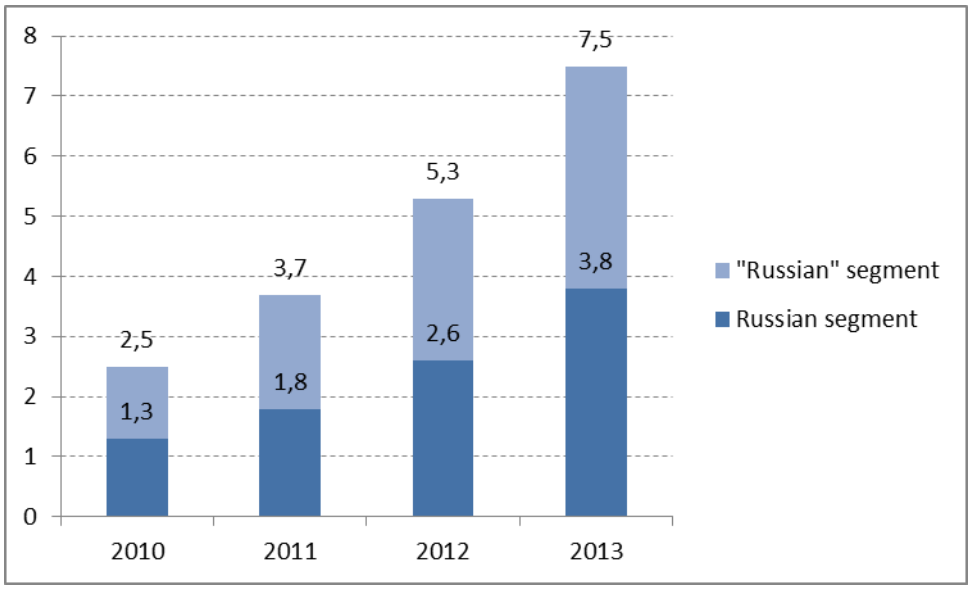
In October 2010 in terms of Securing Our eCity and Digital Crimes Consortium conferences representatives of the US competent organizations revealed for the first time preliminary evaluation of global cybercrime turnover for the year of 2010 which equaled to around 6 billion dollars. **The Group-IB experts estimate the total sum at 7 billion dollars.**

It should be admitted that computer crimes market, traditionally focused on sales of stolen bank and card details, has changed its basic business model in 2010. Now the market provides a wider selection of stolen confidential information, it is offered production of phishing sites, botnet lease and even services for its administration.

Group-IB specialists estimate the share **of Russian cybercrime market segment at 1.3 billion dollars.** Total revenue of the whole "Russian" computer crime market equals to the sum which is twice as much as the first one.

Being located in different regions and making worldwide attacks, **"Russian" hackers earned about 2.5 billion dollars**. This sum includes the income of the Russian segment. Thus Russian speaking violators earned up to 1/3 of total revenue from the computer crimes around the globe.

Figure 5. Predicted financial indicators of the Russian and "Russian" cybercrime market industries (in billion, US dollars)



Source: Group-IB

Under corresponding factors of information technologies and cybercrime market development it is possible to predict that "Russian" hackers will earn around 3.7 billion dollars as early as this year, and in

2013 they will double this value. Approximately a half of the “Russian” computer crime industry revenue will belong to Russian intruders.

Cyber threads of 2011: general trends

The analysis of the global cybercrime market and of its "Russian" segment enables to predict the following major cyber thread trends.

- In 2011 major hacker attacks will be targeted on internet-banking systems. Multimillion revenues, received by the criminals for such frauds, will make the intruders to develop new types of bank Trojans and advance mechanisms of traceless money stealing from bank clients.

- The further increase of DDoS-atack power is expected in this year. Computer crime market prices for this service are going down and this means the increase in demand on organizing such attacks. Besides, the criminals often use DDoS-attacks in fraud in online banking systems In connection with the general trend of cybercrime this fact also indicates a further increase in the number of such incidents.

- The growing popularity of social networks favors further use of social engineering methods for spreading malicious software and will enable hackers to perform avalanche-like infections of the trustful Internet users.

- The Stuxnet example allows supposing the appearance of such incidence targeted on damaging large industry objects this year. Cyber terror and industrial espionage with the help of information technologies are becoming real threats. The analysis of such threats requires serious efforts from the side of the whole expert community.

- Even though the experts had to deal with hacker attacks, caused by political motives, earlier, the hacktivism will become more popular event this year. If earlier hackers had mainly hunted for critical corporate data, but with the hacktivism growth, the number of cases of political information stealing and its use for discrediting political rivals is increasing. On the example of football fans' disorders in Moscow in the end of 2010 and revolution events in Arabian countries in the first quarter of 2011 can illustrate the power of hacktivists demonstrating the social-political position in the Internet and incite their supporters to start real protest acts.

Conclusion

Despite active counteraction to computer intruders from the side of the law-enforcement authorities and information security violations prevention and investigation specialists, the cybercrime market showed a rapid growth last year which influenced the number of violations and amount of revenue received by hackers. "Russian" intruders accounts for one third of total income from computer crimes all over the world. The global cybercrime market is characterized by increase of professional level, expansion of rendered services and promotion of their affordability which will lead to increase in damage from hacker activity in 2011.

Rapid growth of the "Russian" computer crime market industry must be especially admitted. This fact is related to weakness of legislation and law enforcement on the territory of the former Soviet Union states, high level of technical education, linguistic community and economic instability.

Basing on IDC data, information security market amounted to about 13 billion dollars in 2010. For comparison, world computer forensic market amounted to just 1.8 billion dollars. This number is many times lower than the international cybercrime financial indicators and is little more than Russian hackers' incomes.

The basis of the world market of computer crime counteraction lies in the fact that all public companies are obliged to declare committed crimes against them. This is made to protect shareholders and to correctly estimate the company investment risk. Thus, to decrease such risks the issuers have to invest money in both technical and organizational measures for crime investigations.

Russian authorities do not require such information disclosure. But, considering that particularly in Russia the cybercrime problem is of a special actuality, it is necessary to introduce the obligations to publicly inform on information security incidents. The introduction of such requirement by the government may significantly improve security systems of Russian corporations and make them implement investigation systems. Unfortunately, without pressure of state authorities domestic companies do not want to invest in protection which would correspond to up to date cyber threats. The example of Federal Law 152 and Bank of Russia Standard on Information Security Ensuring of Banking System Organizations of the Russian Federation show that exactly the direct State requirements can influence the increase of information security level.

To lower activity of hackers operating within territory of the CIS and Baltic countries it is necessary to carry out regular improvement of legal frame and increase of competence level of law enforcement bodies that effect crime control in sphere of computer technologies. Also an important factor of cybercrime counteraction is development and introduction of innovative technical means and solutions which enable to implement proactive feedback on information security threads. Penalty reinforcement, activation of interstate cooperation, engagement of industry associations and promotion of fundamental information security policy will favor the slowdown of contemporary pace of "Russian" cybercrime market growth.