State and Trends of Russian Cybercrime in 2011

Alex Kuzmin
Group-IB
CERT-GIB
Moscow, Russia

Abstract—This paper outlines the main risks associated with various types of hacker activities, analyzes the main trends in the development of the Russian cybercrime market, estimates the shares and the financial performance of the Russian segment of the global cybercrime market, and forecasts market trends for 2012.

Keywords—cybercrime; Russia; hackers; legal; finance; trends.

I. INTRODUCTION

Group-IB has published a report containing the results of the study of the state of the Russian cybercrime market in 2011. It examines the main risks associated with various types of hacker activities, analyzes the main trends in the development of the Russian cybercrime market, estimates the shares and the financial performance of the Russian segment of the global cybercrime market, and forecasts market trends for 2012.

This report was prepared by CERT-GIB analysts and the specialists from Group-IB’s computer forensics lab, and includes highlights of cases where hackers from Russia and countries of the former Soviet Union played a central role.

II. ABOUT GROUP-IB

Group-IB is the first company in Russia and the former Soviet Union working professionally and comprehensively in cybercrime investigation and computer forensics. Created on the basis of Group-IB, the CERT-GIB computer emergency response team operates around the clock. Group-IB is part of LETA Group.

III. ISSUES OF TERMINOLOGY

Cybercrime investigation experts, when using the generic term hacker, prefer to classify cybercriminals by the nature of their specific activities, as well as nationality.

The latter draws particular attention to the different ways experts interpret the term Russian hackers. Russian computer forensic specialists prefer to use this term for Russian citizens who carry out criminal activities inside Russian territory. In the United States and Europe, Russian traditionally refers to not only Russian citizens, but all citizens and immigrants from the countries of the former Soviet Union, sharing a common history and language. This distinctiveness is reflected in the way Western specialists interpret the term Russian hackers when referring to cybercriminals from the Baltics, Ukraine, or Central Asia.

Therefore, one of the goals of this study was the evaluation not only of the Russian cybercrime market, but also the analysis of the entire Russian segment of the global cybercrime market.

Thus, the term Russian-speaking cybercrime market shall apply to the market of cybercrimes committed by Russian citizens and citizens of the countries of the former Soviet Union, as well as citizens of other countries who have emigrated from the countries of the former Soviet Union. The analysis of the financial performance of this segment will not only consider the crimes committed by Russian-speaking hackers in their countries of residence, but also those committed by them in other parts of the world.

The term Russian cybercrime market shall mean the market of computer crimes committed solely by Russian citizens. In the analysis of this sector’s financial performance only those crimes committed by Russian hackers inside Russia will be considered.

IV. CYBERCRIME MARKET

The cybercrime market of any country is an integral part of its shadow economy. This market has four key aspects which can be highlighted:

- **Online fraud**, containing online banking fraud, phishing attacks, and theft of electronic funds. It should be noted that this aspect includes cashing services for stolen funds, taking up around 40% of this entire aspect.
- **Spam**, including not only services for sending unsolicited email, but also affiliate programs for unlawful sale of drugs and counterfeit products and software.
- **Internal market** (cybercrime to cybercrime, or C2C), including services for anonymization and sale of traffic, exploits, malware, and loaders.
- **DDoS attacks**, including services for organizing attacks aimed at denial of service.

Apart from the above aspects, there exists one more, including services which presently do not have a wide enough supply and demand, such as industrial espionage, brand attacks, attacks on mobile devices, and so on. This aspect combines such diverse threats, making it difficult to assign it a specific name, and is referred to as Other.
V. QUANTITATIVE ASSESSMENT

Below are quantitative assessments of the Russian cybercrime market in each key aspect:

<table>
<thead>
<tr>
<th>Trend</th>
<th>Total market share, %</th>
<th>Amount, million USD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online banking fraud</td>
<td>21.3</td>
<td>490</td>
</tr>
<tr>
<td>Cashing</td>
<td>16</td>
<td>367</td>
</tr>
<tr>
<td>Phishing</td>
<td>2.4</td>
<td>55</td>
</tr>
<tr>
<td>Theft of electronic funds</td>
<td>1.3</td>
<td>30</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>41</strong></td>
<td><strong>942</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trend</th>
<th>Total market share, %</th>
<th>Amount, million USD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam</td>
<td>24</td>
<td>553</td>
</tr>
<tr>
<td>Pharma and counterfeits</td>
<td>6.2</td>
<td>142</td>
</tr>
<tr>
<td>Fake software</td>
<td>5.9</td>
<td>135</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>36.1</strong></td>
<td><strong>830</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trend</th>
<th>Total market share, %</th>
<th>Amount, million USD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sale of traffic</td>
<td>6.6</td>
<td>153</td>
</tr>
<tr>
<td>Sale of exploits</td>
<td>1.8</td>
<td>41</td>
</tr>
<tr>
<td>Sale of loaders</td>
<td>1.2</td>
<td>27</td>
</tr>
<tr>
<td>Anonymization</td>
<td>0.4</td>
<td>9</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>10</strong></td>
<td><strong>230</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trend</th>
<th>Total market share, %</th>
<th>Amount, million USD</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDoS attacks</td>
<td>5.6</td>
<td>130</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>5.6</strong></td>
<td><strong>130</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trend</th>
<th>Total market share, %</th>
<th>Amount, million USD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other</td>
<td>7.3</td>
<td>168</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>7.3</strong></td>
<td><strong>168</strong></td>
</tr>
</tbody>
</table>

Thus, the analysis of cybercriminal activities in 2011 conducted by CERT-GIB analysts estimates the total share of the Russian cybercrime market at $2.3 billion, essentially doubling last year’s numbers.

The obtained data allowed us to determine the financial performance of the Russian-speaking cybercrime market, traditionally twice the amount of the Russian segment. While geographically located in different regions and carrying out their attacks around the world, Russian-speaking hackers have earned an estimated $4.5 billion. This amount includes the revenues of the Russian segment as well.

Studies in past years have shown that the Russian-speaking cybercrime market makes up about a third of the global market, which Group-IB’s experts estimate at $12.5 billion.

VI. QUALITATIVE ASSESSMENT

In 2011, the following general trends of cybercrime market development can be highlighted:

- Consolidation of the market participants, reflected in the formation of several major cybercrime groups on a consistent basis. As a result, there is a departure from the traditional model, based on the principle of disorganization, instead favoring the creation of organized groups with a centralized management system;

- Strengthening of the interlinking between the major groups, based on mutually beneficial sharing of compromised data, providing botnets, and cashing schemes. Thus, there have been incidents involving several cybercrime groups, creating complications in their investigation;

- Penetration of the cybercrime market by traditional organized crime groups, attempting to not only control the cashing of stolen funds, but the entire theft process. This trend leads to the merging of the two criminal worlds with the subsequent resource allocation from the mafia’s traditional areas of control (prostitution, drug and arms trafficking, and so on) in favor of cybercrime. With the imperfections in the existing laws, this has the threat of an explosive increase of attacks on the financial sector;

- Penetration of the cybercrime market by individuals with little technical education. Thus, cybercrime ceases to be the trade of “techies”, since it mainly requires capital investments, not specialized knowledge. The emergence of this trend has led to the expansion of the internal cybercrime market (C2C) and the appearance of outsourcing services (administration, training, consulting, etc.);

- Growth of the internal market. This market covers the C2C services, provided on a paid basis by specialized teams of hackers. In addition to the traditional market growth, this year is characterized by the emergence of the new trend of IT outsourcing.

As consequence of the above trends, the following fact is apparent: the Russian cybercrime market is experiencing a period of dynamic transition from a quantitative state to a qualitative one, moving away from the chaotic model of the development of the cybercrime world.

VII. SPECIFIC TRENDS: ONLINE BANKING

As predicted in our previous report, 2011 was a year of explosive growth of this area of the cybercrime market. Generally, this growth was caused by the improvements in banking malware and the formation of even more stable criminal groups whose professionalism and experience grew with each passing month and earned million. As a result, in December 2011 the largest banking botnet consisted of about 2 million computers. The largest banking botnets working successfully against Russian banks were those built on the following malware (listed in descending order by size): Carberp, Hodpro, Shiz, Lurk, Spy.Ranbyus, and Qhost.
Strengthening of protective measures by banks and the developers of online banking systems has led the criminals to actively experiment with employing remote access tools directly from the computers of their victims in order to successfully make fraudulent transactions. The most successful were the groups possessing the most stable and convenient remote access tools, such as TeamViewer, Hamachi, and Mipko. However, a Trojan using the Microsoft Remote Desktop protocol received the widest use.

Since 2009, Group-IB has been issuing warnings regarding automatic substitution of details in payment orders at the time of the document’s signing and sending, as well as regarding the possibilities of fully automated processes for creating and sending fraudulent payment orders via malware. This functionality, however, only came to be used in the fall of 2011. Its emergence has allowed the criminals to avoid the need for remote access or copying information from a user’s computer in order to bypass protective measures, such as virtual keyboards, PIN codes, VPN tunnels, and network filtering. At this time, among all malware targeting clients of Russian banks, only Carberp has such functionalities.

The emergence of such functionalities as automatic substitution and automatic loading required extensive testing, and the criminals discovered the perfect method, by which they would automatically transfer 1 ruble from the accounts of various charities and religious organizations for several months. Thus, with this “charity” work, the new functionalities were successfully tested.

Whereas in 2010 the victims of online banking fraud were mainly legal entities, in 2011 there was a dramatic surge in theft from individuals. For this type of theft the criminals actively used web inject technologies and Trojans to redirect users to phishing resources. As a result, just in the last quarter of 2011, tens of thousands of individuals were victimized by such Trojans for a total sum of $73.5 million in stolen funds.

Web injects is a well-known technology, widely implemented in all popular Trojans. However, its active use targeting clients of Russian banks started only in 2011. The reason for the use of web injects was the massive shift from using large banking software installed on the user’s computer to small clients with all operations performed via a browser. Additionally, another good incentive for the criminals was the fact that an increased number of individuals began using online banking.

However, banking phishing did not receive wide usage last year. After a group of phishers was eliminated in the first quarter of 2011 in Moscow, attacks of this type were practically non-existent. In late summer, nonetheless, another criminal group tested this method, gaining some success. As a result of their activities, one or two phishing resources a day are popping up, targeting clients of some of the largest banks.

In April 2011, the botnet built on the Hodprot Trojan (as classified by NOD32), in operation since 2009, ceased to exist. In its place, the criminals chose the new Carberp Trojan. Many information security experts have said that malware such as Zeus and SpyEye are involved in the theft of funds from clients of Russian banks. Before the end of 2011, however, there had been no registered theft using this malware. Still, in November and December 2011, the first working samples of Zeus and SpyEye were discovered, containing modules for working specifically with Russian online banking systems. The examination of these botnets showed that these modules were in the testing phases and did not yet receive active dissemination. We assume, however, that the emergence of these programs will certainly be palpable in 2012.

Beginning in late 2010, the number of DDoS attacks on banks after instances of theft of large amounts of funds sharply decreased. The same trend continued in 2011. This is because the fact of a DDoS attack has become a signal regarding theft of funds for the bank’s security personnel, resulting in these fraudulent transactions being promptly detected and prevented.

VIII. SPECIFIC TRENDS: SPAM

The general trends in this area stayed the same throughout 2011:

- The most common and simplest way to monetize spam is working with affiliate programs;
- The most common way to make a profit via affiliate programs is to sell counterfeit pharmaceutical products;
- This is followed by sale of counterfeit software under the guise of being licensed, sale of knockoffs of prestigious accessories, such as clothing or watches, advertising online dating sites, including fraudulent ones, and so on;
- Another, less popular spam monetization method is sale of services for sending messages to various categories of recipients and leasing software for spam mailing.

However, the total volume of spam sent does not change as a result of shutting down of some affiliate programs or their failure to pay out the spammers, since the major actors in this area are working with several affiliates at the same time, switching their resources to other programs whenever problems arise.

IX. SPECIFIC TRENDS: DDoS ATTACKS

The number of DDoS attacks in 2011 has grown as compared to previous periods. The main targets were usually online stores and other representatives of the online business sphere. It should be noted, however, that the average strength of attacks in 2011, as compared to 2010, has weakened, with botnets typically numbering no more than 10,000 nodes used for attacking.

There was a sharp increase in political DDoS attacks in 2011, carried out in order to block certain media sites, blogs, and forums. This was because of increased political activity in Russia due to the parliamentary and presidential elections.

In the summer of 2011, Igor Artimovich was apprehended in a high-profile arrest. He was executing DDoS attacks on Assist, one of the largest payment systems in Russia. This arrest was widely publicized in the media, and the public finally learned what a DDoS attack is and why it is dangerous, while the organizers and executors of DDoS attacks became con-
vinced that this crime can be successfully investigated. It should be noted that because of this case, law enforcement agencies gained valuable experience in counteracting such crimes.

Yet, in 2011, there was a significant reduction in the number of DDoS attacks against banking websites and online banking systems. First, this is due to their inefficiency from the viewpoint of the criminals, and second, banks have made substantial efforts to secure their network infrastructure, particularly pertaining to filtering malicious traffic.

A new trend in 2011 was attacks over HTTPS, which was a rare occurrence in prior years. To carry out such an attack and achieve the desired result (denial of service), minimal resources are required. Equipment for filtering and deflecting this type of attack is expensive and service providers rarely own them.

X. CERT-GIB PROFILES: VLADISLAV KHOROKHORIN


Vladislav Khorokhorin is the owner of online stores Dumps.name and BadB.biz specializing in sale of compromised data of bank card users. More than eight years of active participation on the carding scene.

BadB first caught the attention of the United States Secret Service in 2003 after the arrest of a Chinese-American carder, Jian Ping Wong, in Baltimore. Among Wong’s criminal ties, Secret Service agents specifically emphasized a certain BadB. Secret Service’s interest regarding BadB was rekindled after the arrest of Boa (also known as Roman Vega, spiritual leader of the Russian carder scene and one of the most active members of the CarderPlanet community). After data analysis performed by Secret Service agents, multiple mentions of professional criminal ties with BadB were discovered on Boa’s computer. When another carder, Redetti, based in Seattle, was arrested in 2009 with his computer having additional evidentiary data against BadB, it caused the United States intelligence to begin a concerted action of neutralizing BadB.

A special undercover Secret Service agent contacted BadB, bought from him several batches of compromised data of American and Israeli bank card users, and then conducted a number of additional investigative measures to strengthen the obtained evidentiary base. This information was forwarded to the Dutch authorities in order to gain access to the servers of Khorokhorin’s online resources Dumps.name and BadB.biz, hosted in Holland. When copies of the hard drives of the Dumps.name and BadB.biz servers were received from Holland, they were analyzed and attached to the indictment of a United States court.

In addition, the United States intelligence enlisted the assistance of their Israeli colleagues to conduct surveillance of Khorokhorin’s personal telephone and online communications. Previously, similar requests were addressed to the administrations of Yahoo and Google email services in order to gain access to Khorokhorin’s personal correspondence.

The charges made on the basis of the collected information were presented before a jury in a Washington, DC court on November 12, 2009. The verdict was only declassified in August 2010 to transfer the case to the French law enforcement agencies. On August 7, 2010, Khorokhorin was arrested by the French border agents at the airport in Nice prior to his departure for Moscow. Khorokhorin was charged with aggravated fraud and theft. If found guilty on both charges, he can face up to 12 years in prison. Additionally, each charge carries with it a fine of up to $250,000.

Presently, Khorokhorin is held in custody in France. American authorities are doing everything they can for his extradition to the United States. Khorokhorin is being represented by Bukh & Associates, an American legal firm, headed by Khorokhorin’s personal attorney Arkadiy Bukh, who represents Oleg Nikolayenko, another alleged cybercriminal. As with Nikolayenko, the defense insists on extradition of Khorokhorin to Russia.

XI. CERT-GIB PROFILES: OLEG NIKOLAYENKO

Also known as: Mega-D, Docent, King of Spam. Born July 13, 1987 (June 13, 1985 in some documents) in Rogan, Ukraine. Place of registered residence: Vidnoye, Moscow region, Russia. Citizenship: Ukrainian, Russian.

Oleg Nikolayenko is the presumed administrator and owner of the Mega-D botnet, which is also known as Ozdok, specializing in sending spam. During the period of activity, Mega-D had over 510,000 bots at its disposal. At the peak of its operational strength, it sent out approximately ten billion spam messages a day, accounting for nearly a third of the global spam traffic.

The FBI arrested Oleg Nikolayenko in Las Vegas in November 2010 on the charges of violating the CAN-SPAM Act, an anti-spam law in the United States. Nikolayenko’s arrest was preceded by the arrests of two American spammers, Jody Smith and Lance Atkinson, who provided the FBI agents with key information regarding Nikolayenko’s criminal activities.

The FBI charged Nikolayenko not only with violating the anti-spam law, but also with being complicit in various fraudulent schemes based on the massive use of spam, such as distributing a wide variety of counterfeit goods and illegal drugs and narcotics. Presently, Nikolayenko is awaiting sentencing in Milwaukee.

According to some sources, Oleg Nikolayenko is close to reaching a deal with the American judicial authorities after which he would be extradited to Russia to serve his sentence there, having paid a large fine. Nikolayenko is being represented by Bukh & Associates, an American legal firm, headed by Nikolayenko’s personal attorney Arkadiy Bukh.
Yevgeniy Anikin was given a suspended sentence of five years in a penal colony, while the prosecution demanded imprisonment of up to five years. However, the defendant pled guilty in settlement requiring him to compensate the damages sustained by the victim. Based on the facts of the case, Yevgeniy Anikin was given a suspended sentence of five years in prison.

A graduate of the Khakassia Business Institute and Novosibirsk State University, Anikin was arrested in Saint Petersburg along with Viktor Pleshchuk, his accomplice, and charged with misappropriation of funds (grand theft). After the indictment was confirmed by the city prosecutor, the case was transferred to Novosibirsk for a hearing. The case was considered under Article 158 of the Criminal Code of the Russian Federation on February 7-8 by the Zaeltsevskiy District Court of Novosibirsk.

The penalties stipulated by the Article include up to ten years in a penal colony, while the prosecution demanded imprisonment of up to five years. However, the defendant pled guilty in settlement requiring him to compensate the damages sustained by the victim. Based on the facts of the case, Yevgeniy Anikin was given a suspended sentence of five years in prison.

Maksim Glotov is presumed to be the author of the OSMP Grabber software. It is installed on computers of private entrepreneurs who own OSMP payment kiosks, sending the criminal the OSMP account details (terminal number, username, and password).

In recent years this software became well-known, and so-called trays with money were sold on forums at a discount of up to 80%. They were even emptied via spam ("recharge your mobile account for 50% off"), with the transfer of electronic funds via anonymous digital wallets.

Having regular unauthorized access to personal data, Glotov and his accomplices committed theft by modifying the information of the payment system agents. Glotov’s fraudulent actions resulted in unauthorized transactions totaling over ten million rubles.

OSMP Grabber made it possible to withdraw funds without the traditional drops or dummy individuals used for cashing, instead using legal entities. Therefore, OSMP kiosks acted as buffers in this scheme of cashing funds stolen from bank cards.

Glotov was initially arrested in Yekaterinburg at his rented apartment. The operation for his arrest took several months of fieldwork. It was decided not to hold Glotov in custody, instead letting him be released under travel restrictions. Glotov took advantage of this, appearing in court for the first hearing, and disappearing during the break. Glotov went to Kursk and then to Tyumen, underwent plastic surgery, and obtained a false driver’s license and passport under a new name. Later, Glotov was identified and arrested in November 2010.

At the present time, a criminal case has been initiated against Maksim Glotov and Adrian Stepanov on charges of fraud, unauthorized access to computer information, creation and dissemination of computer viruses, and forging a passport and driver’s license. The case is pending trial at the Zheleznodorozhniy District Court of Yekaterinburg with Glotov facing up to ten years of imprisonment and a heavy fine.

Andrey Sabelnikov


On January 23, 2012, Microsoft filed a lawsuit at a Virginia court against Andrey Sabelnikov, charging him with the creation of the Kelihos malware (the botnet is called Kelihos by Microsoft, while Kaspersky Lab calls it Hlux). The suit states that Sabelnikov used the virus to control, support, and develop the enormous botnet. Richard Boskovich, the senior attorney at Microsoft’s counter-cybercrime department, states that the charges are based on the data obtained as a result of analyzing the code of Kelihos.

Kelihos was used for unauthorized access to personal information located on over 41,000 computers worldwide. It was also used for massive spamming and DDoS attacks. Prior to September 2011, the botnet sent out approximately 3.8 billion spam messages a day.

Kelihos is a botnet operating on the peer-to-peer principle and composed of several levels, which include different types of nodes: routers (computers commanding the bots and controlling the dynamics of the peer network structure), controllers (infected computers, the public IP address of which is used by bots to send spam, steal email addresses, and detect private user information in the flow of network traffic), as well as working nodes.
An amateur photographer from Saint Petersburg, Andrey Sabelnikov came into view of IT security specialists after it was discovered that Kelihos was loading necessary data from sabelnikov.net, a website registered by Sabelnikov, and currently offline.

Sabelnikov is currently employed by a consulting company as a freelance programmer, but until recently he was employed as a software engineer and project manager at Agnitum, a Russian company specializing in the development of firewalls, antivirus and other security tools, the makers of the well-known Outpost Firewall Pro software.

Microsoft also stated they were able to locate Sabelnikov thanks to the testimony of Dominic Alexander Patty from the Czech Republic, owner of the dotFREE Group hosting company, which was involved in the registration of 3,723 .cz.cc domain names used to control the botnet. At the present time, the Kelihos botnet is active and continues its malicious activities, having undergone insignificant modifications.

Vrublevskiy was released from prison in December 2011 and is currently under travel restrictions.

According to the investigation, Vrublevskiy organized a DDoS attack on Assist’s servers in 2010, resulting in the payment processing company being blocked, leaving its clients unable to purchase airline tickets on Aeroflot’s website. According to Aeroflot, the attack began on July 16, 2010, and the company was able to restore sale of electronic tickets only seven days later. The FSB believes Vrublevskiy wanted to discredit Assist is this way. ChronoPay was bidding for a lucrative contract for electronic ticket sales as well, and tried getting rid of a competitor. ChronoPay was unsuccessful, as Aeroflot signed a contract with Alfa Bank.

At the present time, cybercrime is widespread throughout Russia, the countries of the former Soviet Union, and around the world. An important role in creating obstacles for preventing and investigating these crimes is played by several gaps in Russian laws. Unlike in other countries where laws provide a clear conceptual apparatus stipulating severe penalties, Russian laws require significant improvements. It should also be noted that other countries devote a lot of attention to training law enforcement officers and court officials regarding the main issues of IT security, allowing them to make independent judgments on various aspects of cybercrime. Thus, because of imperfections in Russian laws and the lack of severe penalties, stable law enforcement practice, and regular training regarding counter-cybercrime measures, cybercriminals are disproportionately liable for the crimes they commit.

For example, Evgeniy Anikin and Viktor Pleschuk, who hacked the WorldPay system of The Royal Bank of Scotland and stole $10 million from its accounts, were found guilty by a Russian court, yet only received suspended sentences, while those convicted of ordinary crimes, such as theft in the amount of up to $50,000, serve actual time in prison.

Currently, the trial is ongoing in the case of the DDoS attack on the Assist payment processing company, which sustained damages of over one million rubles. The investigation identified the presumed initiator of the attack who confessed to its organization. The court issued an arrest warrant. The amount of damages and loss of profits in this case are greater than the threshold for offences against property. Despite this fact, however, the measure of restraint was reduced to travel restrictions.

These examples illustrate the fact that Russian legislators and judicial authorities do not appreciate the full depth and danger of cybercrime.

Russian President Dmitriy Medvedev introduced a bill entitled “On Amendments to the Criminal Code of the Russian Federation and Certain Legislative Acts of the Russian Federation”, adopted by the State Duma on November 17, 2011, and enacted as Federal Law on December 7, 2011. Among other things, this law addresses Article 28 of the Criminal Code. The most significant changes to this portion of the Code which should be highlighted are the additional aggravating circumstances and increased severity of penalties, both of which will have a positive impact on the effectiveness of counter-cybercrime actions.

However, the amendments to Article 28 of the Criminal Code were made without taking into account the opinions of specialized law enforcement agencies with experience in investigating cybercrime and industry organizations, creating some controversial issues.

In order to enhance countermeasures against organized cybercrime by Russian law enforcement and judicial authorities, we propose to implement the following:

- Amend the law with an additional conceptual apparatus related to issues of information security and information technologies. For example, the term “botnet” needs to be introduced, perhaps under a different name,
which remains and will remain for the foreseeable future the main tool for committing the majority of cybercrimes.

- Amend the term “computer information” in the existing law, which does not fully reflect the nature of computer information, leading to possible incorrect interpretations of this term.
- Make the penalties for crimes committed using computer technologies more severe.
- Amend and augment the criminal procedure legislation as follows:
  - Introduce the term “digital evidence” and describe the procedures and actions related to its procuring, securing, and investigating;
  - Create a separate definition for the crime scene of a cybercrime and establish a specific place of investigation of such crimes.
- Organize federal and regional training programs for the judicial, prosecutorial, investigative, and law enforcement agencies, including seminars regarding the issues of cybercrime investigation.
- Develop a document for submission to the UN, establishing the principles of international interaction against cybercrime, while also respecting the sovereignty of the member states, as opposed to the Budapest Convention.

The implementation of these measures will significantly improve the number of solved computer crimes, change the existing law enforcement practices, and establish proper international cooperation in this field.

XVII. FORECASTS FOR 2012

The analysis of the Russian cybercrime market in 2011 allows us to make a prognosis regarding its main development trends.

We continue to anticipate growth in the number of attacks on online banking sites in 2012, as this field of activity still brings cybercriminals record profits. But unlike in 2011, this year the growth will be sporadic and largely dependent on theft from individuals. From the second quarter of 2012 and until the end of summer, we expect a gradual decline in the volume of theft due to the replacement of actors and the malware used in online banking fraud.

The automatic substitution and loading technology should dominate 2012 together with the use of web injects.

Given the current state and developmental level of criminal groups, the Carberp malware will lose its leader status, possibly giving way to its clones, as was the case with the Zeus malware. Additionally, the market will see new actors with new Trojans, which, given proper levels of development, will carve out a niche in the Russian segment of online banking fraud.

Experience shows that working with phishing resources is time-consuming, although people with little skill and small initial capital can develop this trend into a much larger phenomenon. In the end, this scheme may become very popular and the number of people involved in it will grow steadily.

The volume of unsolicited email messages will continue growing, while disabling botnet control servers used for sending spam will only result in temporary disruptions in the number of sent messages.

The largest underground affiliate programs will not cease their operations and will not be displaced by smaller actors.

In 2012, botnet operators will face some difficulties, as the majority of malicious traffic will be blocked without reaching its intended victim with the rise in the number of filtering and analyzing equipment installed at intermediate nodes.

There will continue to be growth in the number of attacks using HTTPS. The most frequent victims will continue to be resources associated with online sales. However, DDoS attacks on the banking sector will most likely finally die out due to their ineffectiveness.