

Russian financial cybercrime: how it works

By [Ruslan Stoyanov](#) on November 19, 2015. 10:57 am

PUBLICATIONS

CYBER ESPIONAGE

CYBERCRIME

CYBERCRIME LEGISLATION



[Download PDF version](#)

Introduction

The Russian-language cybercrime market is known all over the world. By ‘Russian-language market’ we mean cybercriminals who are citizens of the Russian Federation and some former USSR countries, predominantly Ukraine and the Baltic states. Why is this market known worldwide? There are two main factors: the first of these is frequent global media coverage of the activity of Russian-language cybercriminals. The second is the open accessibility of online platforms used by the cybercriminal community for communications, promoting a variety of “services” and “products” and discussing their quality and methods of application, if not for making actual deals.

Over time, the range of “products” and “services” available through this underground market has evolved, becoming more focused on financial attacks, and with an ever-increasing level of sophistication. One of the most common types of cybercrime was (and still is) the turnover of stolen payment card data. With the emergence of online stores and other services involving e-payment

transactions, DDoS-attacks and financial cybercrime have become especially popular with the fraudsters whose main targets are users' payment data or the theft of money directly from user accounts or companies.

Attacks on users' and companies' e-wallets were initiated by the Trojan ibank in 2006; then came ZeuS (2007) and SpyEye (2009) followed by the groups Carberp (2010) and Carbanak (2013). And this list is incomplete; there are more Trojans out there, used by criminals to steal users' money and data.

With online financial transactions becoming more common, the organizations supporting such operations are becoming more attractive to cybercriminals. Over the last few years, cybercriminals have been increasingly attacking not just the customers of banks and online stores, but the enabling banks and payments systems directly. The story of the [Carbanak cybergroup](#) which specializes in attacking banks and was exposed earlier this year by Kaspersky Lab is a clear confirmation of this trend.

Kaspersky Lab experts have been monitoring the Russian hacker underground since it first emerged. Kaspersky Lab regularly issues [reports on financial cyber-threats](#) which track changes in the number of financial malware attacks carried out over time. Information on the number of attacks may indicate the extent of the problem but does not reveal anything about who creates them and how. We hope that our review will help to shed light on this aspect of financial cybercrime.



Tweet

Between 2012-15, law enforcement agencies arrested over 160 Russian-speaking cybercriminals

The data presented in this article is compiled from dozens of investigations that Kaspersky Lab experts have participated in over the last few years, as well as their many years' experience observing the Russian cybercrime market.

Situation overview

According to Kaspersky Lab, between 2012 and 2015, law enforcement agencies from a number of different countries, including the United States, Russia, Belarus, Ukraine and the EU arrested over 160 Russian-speaking cybercriminals who were members of small, medium-sized and large criminal groups. They were all suspected of being engaged in stealing money using malware. The total damage resulting from their worldwide activity exceeded \$790 million dollars. (This estimate is based both on the analysis of public information about the arrests of people suspected of committing financial cybercrime in the period between 2012 and 2015 and on Kaspersky Lab's own data.) Of this sum, about \$509 million dollars was stolen outside the borders of the former USSR. Of course, this figure only includes confirmed losses, the details of which were obtained by law enforcement authorities during the investigation. In reality, cybercriminals could have stolen a much larger amount.



The number of arrests of Russian-speaking cybercriminals as officially announced during the period 2012 to 2015

Since 2013, Kaspersky Lab's Computer Incidents Investigation team has participated in the investigation of more than 330 cybersecurity incidents. More than 95% of these were connected with the theft of money or financial information.

Although the number of arrests of Russian-language criminals suspected of financial cybercrime increased significantly in 2015 compared with the previous year, the cybercriminal market is still "crowded." According to Kaspersky Lab experts, over the last three years Russian-language cybercrime has recruited up to a thousand people. These include people involved in the creation of infrastructure, and writing and distributing malware code to steal money, as well as those who either stole or cashed the stolen money. Most of those arrested are still not in prison.

We can calculate fairly precisely the number of people who make up the core structure of an active criminal group: the organizers, the money flow managers involved in withdrawing money from compromised accounts and the professional hackers. Across the cybercriminal underground, there are only around 20 of these core professionals. They are regular visitors of underground forums, and Kaspersky Lab experts have collected a considerable amount of information that suggests that these 20 people play leading roles in criminal activities that involve the online theft of money and information.

The exact number of groups operating across Russia and its neighboring countries is unknown: many of those involved in criminal activities participate in several thefts and then, for various reasons cease their activity. Some participants of known but apparently disbanded groups continue their criminal activities as part of new groups.

Kaspersky Lab's Computer Incidents Investigation Department can now confirm the activity of at least five major cybercriminal groups specializing in financial crimes. These are the groups whose activities have been monitored by the company's experts over the last few years.

All five groups came to the attention of the company's experts in 2012-2013, and are still active. They each number between ten and 40 people. At least two of them are actively attacking targets not only in Russia but also in the USA, the UK, Australia, France, Italy and Germany.



Tweet

There are ~20 of people, who make up the core structure of an active criminal group

Since the investigation into these groups has not been completed, it is not possible to publish more detailed information on the activities of these groups. Kaspersky Lab continues to investigate their activity and is cooperating with the law enforcement agencies of Russia and other countries in order to curb their cybercriminal business.

Investigation into the activities of these groups has allowed Kaspersky Lab experts to form an idea about their methods of operation and the structure of the cybercriminal market.

The structure of the Russian-language cybercriminal market

“A Range of products and services”

The cybercriminal market usually comprises a set of “services” and “products”, used for various illegal actions in cyberspace. These “products” and “services” are offered to users of dedicated online communities, most of which are closed to outsiders.

The “products” include:

- Software designed to gain unauthorized access to a computer or a mobile device, in order to steal data from an infected device or money from a victim’s account (the Trojans);
- Software designed to take advantage of vulnerabilities in the software installed on a victim’s computer (exploits);
- Databases of stolen credit card data and other valuable information;
- Internet traffic (a certain number of visits to a customer-selected site by users with a specific profile.)

The “services” include:

- Spam distribution;
- Organization of DDoS attacks (overloading sites with requests in order to make them unavailable to legitimate users);
- Testing malware for antivirus detection;
- “Packing” of malware (changing malicious software with the help of special software (packers) so that it is not detected by antivirus software);
- Renting out exploit packs;
- Renting out dedicated servers;
- VPN (providing anonymous access to web resources, protection of the data exchange);
- Renting out abuse-resistant hosting (hosting that does not respond to complaints about malicious content, and therefore does not disable the server);
- Renting out botnets;
- Evaluation of the stolen credit card data;
- Services to validate the data (fake calls, fake document scans);
- Promotion of malicious and advertising sites in search results (Black SEO);
- Mediation of transactions for the acquisition of “products” and “services”;
- Withdrawal of money and cashing.

Payments for such “products” and “services” on the cybercriminal market are generally made via an e-payment system such as WebMoney, Perfect Money,

Bitcoin and others.

All of these “products” and “services” are bought and sold in various combinations in order to enable four main types of crime. These types can also be combined in various ways depending on the criminal group:

- DDoS attacks (ordered or carried out for the purpose of extortion);
- Theft of personal information and data to access e-money (for the purpose of resale or money theft);
- Theft of money from the accounts of banks or other organizations;
- Domestic or corporate espionage;
- Blocking access to data on the infected computer for the purpose of extortion;

According to Kaspersky Lab experts, the theft of money is currently the most widespread type of crime. The rest of this report therefore focuses on this segment of the Russian-language cybercrime market.

The “labor market” of financial cybercrime

The variety of skills required for the creation of “products” and the provision of “services” has given rise to a unique labor market of professionals involved in financial cybercrime.

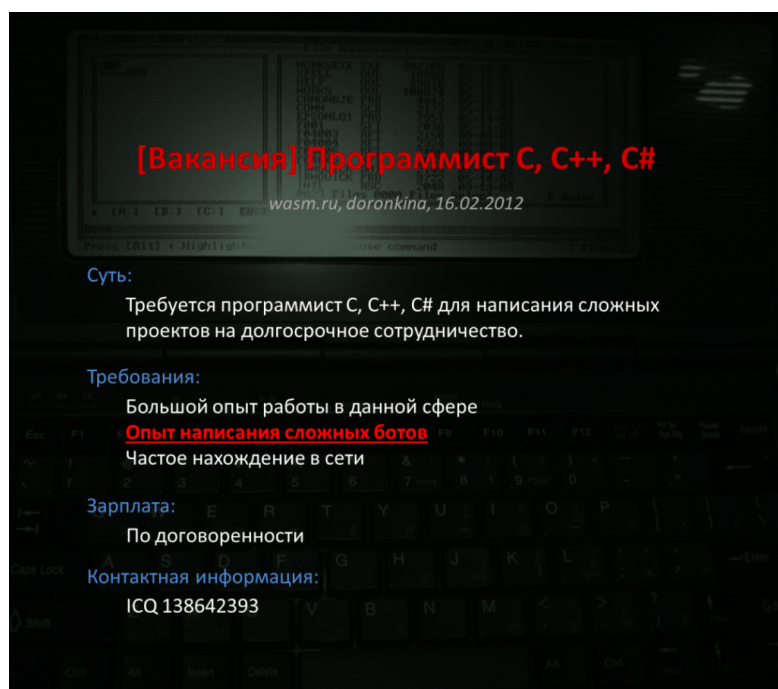
The list of key roles is almost exactly the same as that seen in any IT-related company:

- Programmers / encoders / virus writers (for the creation of new malicious software and modification of existing malware);
- Web designers (for the creation of phishing pages, emails, etc.);
- System administrators (for the construction and support of the IT infrastructure);
- Testers (to test the malicious software);
- “Cryptors” (responsible for the packing of malicious

code to bypass antivirus detection).

The list does not include the heads of the criminal groups, the money flow managers engaged in withdrawing money from compromised accounts, and the heads of money mules supervising the process of cashing the stolen money. This is because the relationship between these elements of the criminal groups is not an employer-employee one, but more of a partnership.

Depending on the type and extent of the criminal enterprise, the heads of the groups either employ “staff” and pay them a fixed salary or work with them on a freelance basis paying for a particular project.



The image is a screenshot of a job advertisement posted on a forum. The background is dark with faint, glowing text and symbols. The main title is in red: "[Вакансия] Программист С, С++, С#". Below it, in white, is the source and date: "wasm.ru, doronkina, 16.02.2012". The text is organized into sections with blue headers: "Суть:", "Требования:", "Зарплата:", and "Контактная информация:". The requirements section includes "Опыт написания сложных ботов" in red.

[Вакансия] Программист С, С++, С#
wasm.ru, doronkina, 16.02.2012

Суть:
Требуется программист С, С++, С# для написания сложных проектов на долгосрочное сотрудничество.

Требования:
Большой опыт работы в данной сфере
Опыт написания сложных ботов
Частое нахождение в сети

Зарплата:
По договоренности

Контактная информация:
ICQ 138642393

An offer of employment posted on a semi-closed forum inviting a programmer to join a cybercriminal group. The job requirements include experience in writing complex bots.

“Employees” are recruited either via sites where those involved in criminal activity traditionally gather or via resources for those interested in non-standard ways of making money online. In some cases, the ads are placed on mainstream job search sites or on the labor exchanges for remote employees.





Tweet

We can confirm
the activity of at
least 5 major
cybercriminal
groups
specializing in
financial crimes

In general, employees involved in cybercrime can be divided into two types: those who are aware of the illegality of the project or the work they are offered, and those who (at least in the beginning) know nothing about it. In the latter case, these are usually people performing relatively simple operations such as copying the interface of banking systems and sites.

By advertising “real” job vacancies, cybercriminals often expect to find employees from the remote regions of Russia and neighboring countries (mostly Ukraine) where problems with employment opportunities and salaries for IT specialists are quite severe.

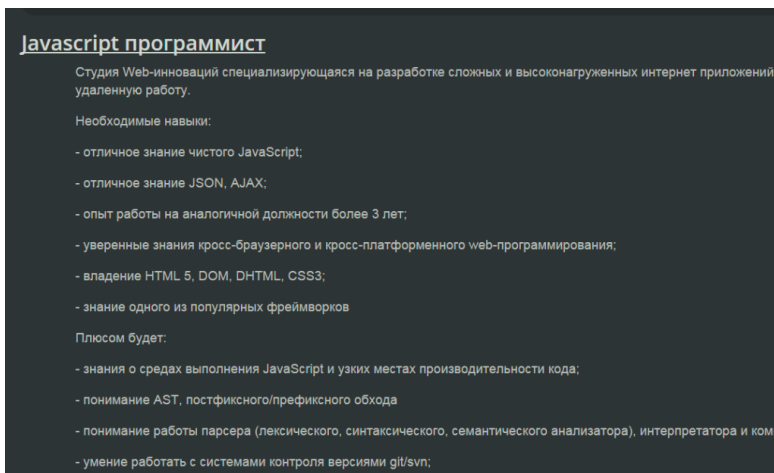
The screenshot shows the 'itMonsters' website interface. The main content area displays a job listing for a specialist in Java/Flash. The listing includes the following details:

- Section:** ТРЕБУЕТСЯ СПЕЦИАЛИСТ ПО JAVA/FLASH
- Date:** 23.10.2014
- Salary:** Зарплата от: 2500 у.е
- Experience:** Опыт работы от 2 лет
- Location:** Город: работа в Одессе
- Requirements:**
 - хороший уровень программирования java (только SE, никаких серверных разработок)
 - хороший уровень на flash (action script 3)
 - уверенное знание спецификаций JVM/AVM, т.е. — формат файлов, умение читать и понимать байткод, умение восстанавливать алгоритмы по байткоду, умение работать с программными фреймворками по модификации форматов спецификаций, умение работать с обфусцированными файлами форматов
 - опционально — программирование python, хотя бы начальный уровень
- Conditions of work:**
 - удаленная работа на постоянной основе;
 - полная занятость;
 - Заработная плата 2500\$.

A fraudster has advertised a job vacancy for java / flash specialists on a popular Ukrainian website. The job requirements include a good level of programming skills in Java, Flash, knowledge of JVM / AVM specifications, and others. The organizer offers remote work and full employment with a salary of \$2,500.

The idea of searching for “employees” in these regions is simple – they carry a saving because staff can be paid less than employees based in large cities. Criminals also often give preference to candidates who have not previously been involved in cybercrime activity.

Often, such job offers are presented as legitimate work, with the true purpose of the work only becoming clear once the task is received.



JavaScript программист

Студия Web-инноваций специализирующаяся на разработке сложных и высоконагруженных интернет приложений с удаленную работу.

Необходимые навыки:

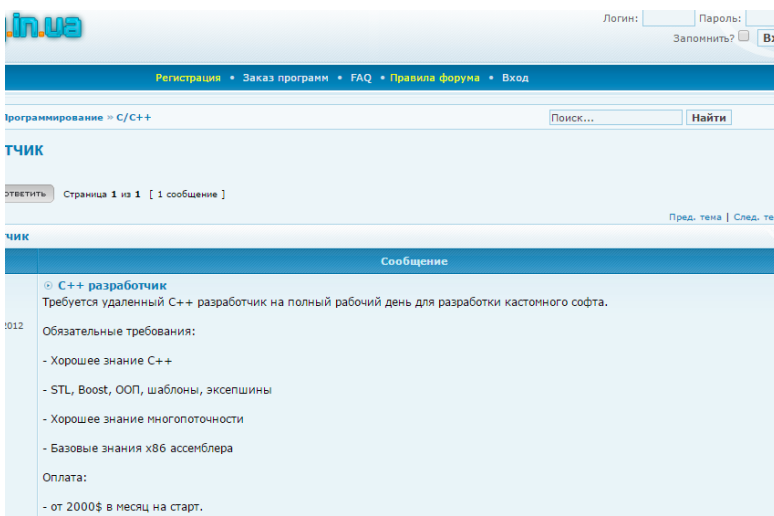
- отличное знание чистого JavaScript;
- отличное знание JSON, AJAX;
- опыт работы на аналогичной должности более 3 лет;
- уверенные знания кросс-браузерного и кросс-платформенного web-программирования;
- владение HTML 5, DOM, DHTML, CSS3;
- знание одного из популярных фреймворков

Плюсом будет:

- знания о средах выполнения JavaScript и узких местах производительности кода;
- понимание AST, постфиксного/префиксного обхода
- понимание работы парсера (лексического, синтаксического, семантического анализатора), интерпретатора и компилятора
- умение работать с системами контроля версиями git/svn;

In this example, the organizer of the criminal group offers a job to a javascript programmer, masking it under a vacancy at a “Web-innovation studio specializing in the development of highly sophisticated Internet applications.”

In the case of illegal job search sites, less-experienced candidates are expected.



in.ua

Логин: Пароль:
 Запомнить?

[Регистрация](#) • [Заказ программ](#) • [FAQ](#) • [Правила форума](#) • [Вход](#)

Программирование » C/C++

ТЧИК

Страница 1 из 1 [1 сообщение] Пред. тема | След. тема

Сообщение

012 **C++ разработчик**
 Требуется удаленный C++ разработчик на полный рабочий день для разработки кастомного софта.

Обязательные требования:

- Хорошее знание C++
- STL, Boost, ООП, шаблоны, экспецины
- Хорошее знание многопоточности
- Базовые знания x86 ассемблера

Оплата:

- от 2000\$ в месяц на старт.

This vacancy invites a C ++ developer to develop “custom” software. In this context “custom” software means malicious software.

The second reason in favor of remote “personnel” is the organizer’s aim of making the activity of the group as anonymous as possible, and to ensure that no single contractor possesses complete information about the group.

Options for organizing a criminal group

Criminal groups involved in stealing money or financial information that will enable them to get access to money, differ in the number of participants and scope of activities. There are three main types of involvement:

- Affiliate programs
- Single dealers, small and middle-sized groups (up to ten members)
- Large organized groups (ten or more participants)

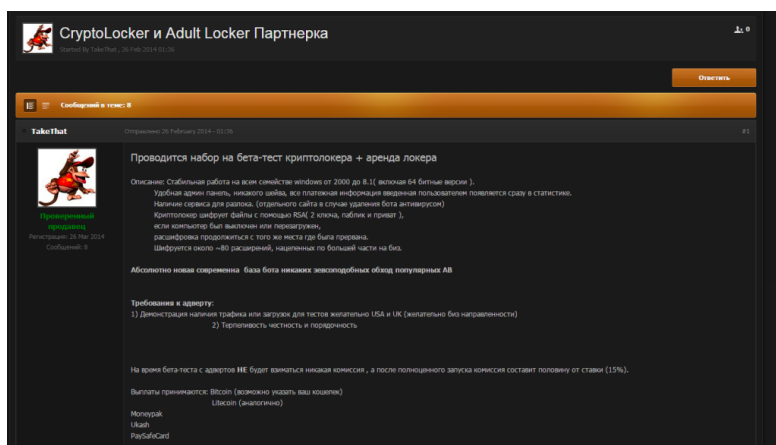
This division is nominal. The scale of the group’s activity depends on the skillfulness of its participants, their ambition and the overall level of organizational abilities. In some cases, Kaspersky Lab experts came across relatively small criminal groups performing tasks that usually require a greater number of participants.

Affiliate programs

Affiliate programs are the easiest and least expensive method of getting involved in cybercrime activities. The idea behind an affiliate program is that the organizers provide their “affiliates” with almost all the tools they need to commit a crime. The task of the “affiliates” is to generate as many successful malware infections as possible. In return, the owner or owners of the affiliate program share the income received as a result of these infections with the affiliates. Depending on the type of fraudulent scheme this could be a share of:

- The sums stolen from the accounts of Internet banking users;
- The money paid by the user as a ransom when cybercriminals use ransomware Trojans;
- The money stolen from the “prepaid” accounts of mobile device users by sending out SMS messages to premium mobile numbers with the help of a malicious program.

Creating and supporting an affiliate program for the purpose of stealing money is a cybercrime committed, as a rule, by a group of users. However, such projects are often carried out by large organized groups whose activity is analyzed later in this document.



This advertisement announces the launch of the beta testing of an affiliate program used to distribute encrypting ransomware. Judging by its characteristics, the group's activity is focused on companies located in the US and the UK. This is indicated by the comment saying that the malware distributed via the partner network is able to encrypt files with 80 different extensions, many of which are files of applications used in companies. The text on requirements for candidates to participate in testing includes a demonstration of the presence of traffic or downloads from the United States and the United Kingdom.

According to Kaspersky Lab experts, affiliate programs are becoming less popular with Russian-language cybercriminals. The main driver of their popularity had been fraudulent schemes used to infect users' mobile devices with malicious programs which then sent out SMS messages to premium numbers. However, in the spring of 2014, the Russian regulator introduced new requirements

for the organization of such services, which included a need to secure additional confirmation of subscription to a particular paid mobile service. This change was instrumental in reducing the number of malicious mobile partner programs to practically zero. Nevertheless, this type of joint cybercriminal activity is still used by groups specializing in the distribution of encrypting ransomware.

Small Groups

What distinguishes this form of cybercriminal activity from an affiliate program is that in this instance the criminal or criminals organize their own fraudulent scheme. Most of the components needed for the attack, such as malware and its modifications (“re-packed” malware), the traffic, the servers, etc., are bought on the black market. Often, members of such groups are not experts in the field of computer and network technologies; they learn about the components and organization of financial attacks from public sources, usually forums. The abilities of such groups can be restricted by a number of factors. Specifically, the use of widely-available malware results in rapid detection by security solutions. This, in turn, makes cybercriminals invest more money in the distribution of malware and in its “re-packing” to bypass detection. The end result is a significant drop in profits for the attacker.

Mistakes made by this type of cybercriminal often result in their identification and arrest. However, as a relatively low cost entry into the world of cybercriminal activity (from \$ 200), this “amateur” format continues to attract new dealers.

An example of such an “amateur” criminal organization is the group that in 2012 was convicted by the Russian court for stealing more than 13 million rubles (then worth about \$422,000) from a Russian bank’s online customers. During a comprehensive investigation Kaspersky Lab experts were able to collect the information that allowed law enforcement authorities to identify those behind the theft.

The court sentenced two members of the criminal group,

giving each a suspended sentence of four and a half years. However, this verdict did not stop the criminals, and they continued to commit crimes, stealing almost as much again over the next two and a half years. They were re-arrested in May 2015.

Large organized criminal groups

Large criminal groups differ from the other players, both through a larger scale of activity and through a more thorough approach to the organization and operation of criminal schemes. Such groups can comprise up to several dozen people (not including money mules used for cashing and “laundering” money.) The targets of their attacks are not limited to individual online banking customers: they also attack small and medium-sized companies, while the largest and most sophisticated of them, such as Carbanak focus mostly on banks and e-payment systems.

The operational structure of large groups differs significantly from smaller groups. To a certain extent, the structure reflects that of an ordinary, average-sized company engaged in software development.

In particular, large groups have some form of regular staff – a group of associates who perform organizational tasks in return for a regular, fixed payment. However, even in these large, professional groups some of the tasks are passed to third-party contractors. For example, the “re-packing” of malware can be performed by the staff or hired virus writers or via third-party services where the process is automated with the help of special software. The same is true for many other elements of the IT infrastructure required for committing crime.

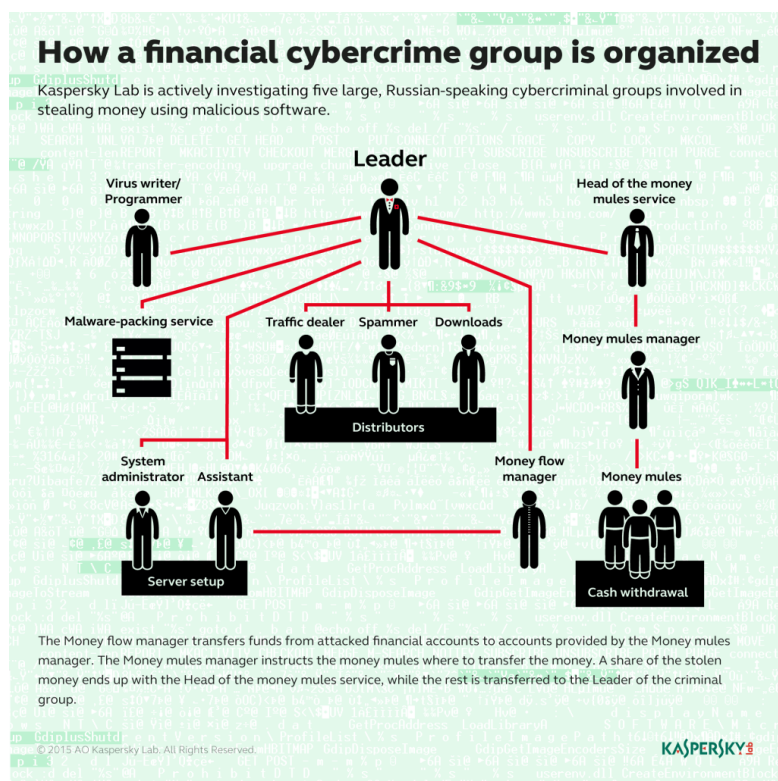
Examples of large, organized criminal groups are Carberp, whose members were arrested in Russia and Ukraine in 2012 and 2013 respectively, and Carbanak, unmasked by Kaspersky Lab in early 2015.

Although the damage from the activity of partner programs and small groups can run into hundreds of thousands of

dollars, the large criminal groups are the most dangerous and destructive. The estimated damage caused by Carberp reaches several hundred million dollars (up to a billion). In this regard, studying how these groups function and the tactics they use is extremely important, as it strengthens our ability to effectively investigate their activity and – ultimately – to suppress it.

Distribution of roles in a large cybercriminal group

A major financial cybercrime undertaken by criminal “experts” in security and the finance sector can result in multi-million dollar losses for attacked organizations. As a rule, such crimes are preceded by many months of preparation. This preparation includes constructing complex infrastructure, and selecting and developing malicious software, as well as a thorough study of the target organization in order to clarify the details of its internal operations and security vulnerabilities. Each member of the criminal group has their own responsibilities.



The following role distribution is typical for a criminal group involved in stealing money. The distribution of roles in groups that specialize in other types of cybercrime may be different.

Virus writer/Programmer

A virus writer or programmer is responsible for creating malicious programs, i.e. the programs that allow the attackers to gain a foothold in the corporate network of the target organization, download additional malware that will help to obtain the necessary information, and ultimately steal money.

The significance of this group member and the nature of their relationship with the organizers may vary from group to group. For example, if the group uses ready-made malware taken from open sources or bought from other virus writers, their functions may be limited to setting and modifying malicious programs to work in the infrastructure created specifically for a certain cybercrime, or to adapt it for attacks on specific institutions. The most advanced groups, however, tend to rely on their own “developments” since it makes a malicious program less visible to most security solutions and provides more opportunities for malware modification. Where this is the case, the virus writer’s role becomes more important as they are responsible for the architecture and feature set of a malicious program.

A virus writer can also take on responsibility for malware “re-packing”. But this happens only when the organizer wants to keep the maximum number of tasks within the group, and where original software is used for malware “re-packing”. In most cases, however, this procedure is shifted to third-party contractors or packing-services.

Testers

The function of testers in a criminal group is not that different from testers working in legal IT companies. In both cases, testers receive from their managers the

specifications for testing programs in different environments (different versions of operating systems, different sets of installed applications, etc.) and execute them. If a fraudulent scheme involves fake interfaces of remote banking or e-payment systems, the task of testers also includes monitoring the correct operation of these fakes.

Web designers and Web programmers

Typically, web designers and web programmers are remote employees, whose tasks include creating phishing pages and websites, fake application interfaces and web injects, all of which are used to steal data to get access to e-payment and e-banking system.

Distributors

Distributors aim to ensure the download of malicious software on as many devices as possible. The result is achieved by using several tools. Generally, the group organizer determines the profile of the users to be infected and buys the required type of traffic from the so-called traffic providers (services to attract users with certain characteristics to a particular website).



An advert offering to buy traffic. Cybercriminals are willing to pay only for the successful installation of malicious software at \$ 140 per 1000 “call-backs” (a message that is sent by the malware to the command server after a successful infection).

The organizer can choose and order a spam mailing that will contain either an infected attached file or a link taking a victim to a malicious website. The organizers can also choose the site with the necessary target audience; involve hackers in breaking into it and placing the exploit pack on it. Of course, all these tools can be used in combination with each other.

Hackers

Often, in the course of an attack, the exploits and other malicious software the organizer has to hand is not enough to infect all the computers necessary for the attack and to anchor in them. It may become necessary to hack into a specific computer or site. In such cases, the organizers involve hackers, people who have considerable skills in information security and are able to perform non-standard tasks. In many of the cases examined by Kaspersky Lab experts, hackers were occasionally involved and were paid on a fee-for-service basis. However, if hacking is required regularly (e.g., for targeted attacks on financial institutions), a hacker becomes a “team member” and is often one of the cybercriminal group’s key participants, along with the organizers and money flow managers.

System administrators

System administrators in cybercriminal groups perform near-identical tasks to their counterparts in legitimate businesses: they implement the IT infrastructure and maintain it in working condition. Cybercriminal system administrators configure management servers, buy abuse-resistant hostings for servers, ensure the availability of tools for anonymous connection to the servers (VPN) and resolve other technical challenges, including the interaction with remote system administrators hired to perform small tasks.

Call services

Social engineering is important for the success of the

cybercriminal business. Especially when it comes to attacks on organizations that result in the theft of huge sums of money. In most cases, even if the attackers are able to establish control over the computer from which the transaction could be performed, confirmation of its legitimacy is required to successfully complete the operation. This is what the “call service” is for. At the specified time, its “employees” play the role of an employee of the attacked organization or a bank with which the organization works, and confirm the legitimacy of the transaction.

“Call services” can participate in a particular cybercrime both as a subdivision of the criminal group, or as a third-party organization, performing a specific task on a fee-for-service basis. The forums that users involved in cybercrime use to communicate with each carry plenty of ads offering such services.

Доброго времени суток господа!

Предлагаем услуги прозвона на:

- Английском (EN)
- Немецком (DE)
- Голландском (NL)
- Французском (FR)

Список языков будет расширяться! Опаса МЖ.

Продаваемое оружие, шоты, банки, и т.д.

Дайтинг на званки!

Оказываем услуги по приему СМС на номера в США

ПРИНИМАЕМ звонки как на свои, так и на предоставленные Вами номера.

Занимаемся быстрым изготовлением локальных и топфри номеров (преимущественно на взорядше звонки с моментальным форвардом на наш/ваш номер) в разных странах от 15\$, присутствуют выборы по странам/штатам/адреса соде, ставим войсы, форварды и тд.

Изготовление локальных и топфри ФАКСОВ с редиректом на ваше место и возможность отправки факса с этого номера.

Попробуйте, и Вам понравится с нами работать!!!

Цены:

- EN - 10\$ за звонок
- DE, NL, FR - 12\$ за звонок
- Отправка факса - 5\$
- Изготовление локальных/топфри номеров - от 15\$
- Изготовление локальных/топфри факсов - от 15\$
- Прием СМС в США/Канаде - 10\$

This advertisement offers “call services” in English, German, Dutch and French. The group specializes in calls to Internet stores and banks, as well to duped mules. Also, the group offers the quick creation of local toll-free numbers used to imitate support services in fraudulent schemes, receiving SMS messages, and receiving and sending faxes. The criminals ask from \$10 to \$12 for one call, \$ 10 for receiving SMS and from \$ 15 for creating toll-free numbers.

According to Kaspersky Lab, large cybercriminal groups prefer to have their own “call services” so they hardly ever turn to third-party providers.

Money flow managers

Money flow managers are members of the cybercriminal group who come into play when all the technical tasks for organizing the attack (choosing and infecting the target and anchoring in its infrastructure) are fulfilled, and everything is ready to commit the theft. Money flow managers are the people who withdraw money from compromised accounts. However, their participation is not limited to pressing the keys; they play a key role in the whole process.



Tweet

The list of key roles in financial cyber gangs almost mirrors IT-companies

Money flow managers usually thoroughly understand the internal rules of the attacked organization (they even know the lunch hours of the employee from whose computer the fraudulent transaction will be made). They know how the automated anti-fraud systems operate and how to bypass them. In other words, in addition to their criminal role of thieves, money flow managers perform “expert” tasks that are difficult or impossible to automate. Perhaps because of this special status, money flow managers are one of the few members of the criminal group who receive a percentage of the stolen money rather than a fixed “salary”.

Money flow managers often perform as botnet operators. i.e. members of the criminal group who analyze and classify the information obtained from infected computers (the access to the remote banking services, availability of money on the accounts which could be accessed, the organization where the infected computer is located, etc.).

Besides money loaders, these “working conditions” are only shared by the leaders of mule projects.

Head of Mules (Mule “project”

leader)

Head of mules is a representative of the criminal group working closely with the people involved in the process of stealing money. The function of the mules is to get the stolen money, cash it and transfer to the criminal group its due share. To do this, the head of mules builds their own infrastructure, which consists of legal entities and individuals with their own bank accounts, to which the stolen money is transferred and from which it is later withdrawn and moved into the pockets of the fraudsters. The mule project leader cooperates with the organizer of the criminal group, and provides them with the numbers of the accounts to which the money loader sends the stolen money. Both mule project leaders and money flow managers work on commission which, according to the information obtained by Kaspersky Lab during the course of investigation, can amount to half the sum stolen.

Mule “projects”

Mule projects are a vital component of any financial cybercrime. Such groups comprise one or more organizers and up to several dozen individual mules.

A mule (or drop) is a holder of a means of payment who, on command from the money mules manager, cashes the money received into their/an account, or transfers it to another account as specified by the money mules manager.

Mules can be divided into two types: duped and non-duped. Duped mules are people who, at least at the beginning of their cooperation with the money mules manager, do not realize they are involved in a criminal scheme. As a rule, the task of getting and transferring money is presented to them under some plausible pretext. For example, the money mules manager can establish a legal entity and appoint to an executive position (the general or financial director, for example) a person who will perform the functions of the duped mule: such as signing corporate documents which will, in fact serve as a legal screen for withdrawing stolen money.

Non-duped mules are well aware of the real purpose of the money mules manager's tasks.

The options used by the mule projects to withdraw money are manifold. Depending on the amount of money stolen, they may include individual credit card holders ready to cash money and give it to the representative of the money mules manager for a small fee, or specially created legal entities, whose representatives open "salary projects" (credit cards for transferring the salaries of company employees) at their corporate bank.

Yet another common method for constructing a mule scheme is for non-duped mules to open dozens of accounts at different banks.



На протяжении 3 лет успешной работы, мы НЕ позволяем совершать краж с наших карт! Предоставляем подробный мануал разработанный нашим сервисом по использованию деб. карт оформленных на дропов.

- В нашем сервисе работают **более 40 продавцов**. Не составит труда найдем и подобрали в вашем регионе или ближайшем от вас. Большинство из них сейчас онлайн, готовы ответить и предоставить бесплатную консультацию.
- Огромный ассортимент банков** нашей необъятной страны и за ее пределами, в странах ближнего зарубежья СНГ, Европы, Азия и дальнего за океанского партнера Америки(USA).
- Можем и **предоставляем редкий товар**.
- Обеспечиваем анонимность и безопасность в проведение сделки**(гарант приветствуется!)

категории и цены

- Карта momentum любой банк от 3.000р. (за комплект)**
- Карта classic любой банк от 4.000р. (за комплект)**
- Карта gold любой банк от 6.000р. (за комплект)**
- Карта platinum любой банк от 8.000р. (за комплект)**

Памятка для покупателя! **Что в себя включает полный комплект**

- На руки вы получите полный пакет документов с привязанной симкой и секретным словом для связи с банком.
- Копию паспорта, бонусер с банком, заявление на выпуск карты, банк клиенту, смена, on-line банком, счета привязанные к карте, по желанию мультивалютные счета.
- Наша цель предоставляем продавцам все подконтрольные, подбираем под разные нужды(обслуживаем). В случае возникновения проблем вопросы решаем в максимально краткие сроки!

Доставка

- осуществляется любым удобным способом, будь это поезд, автобус, курьерские службы и т.п. (условия оговариваются).

This advert offers sets of payment cards (the card, the documents based on which the card was authorized, the SIM card with which the bank account of the card is associated) that can be used for cashing stolen money. For sale is the card issued by Russian banks and banks from neighboring countries, as well as banks from the countries of Europe, Asia and the United States. The Momentum-type set is costs 3000 rubles (less than \$50), the set with the Platinum card – eight thousand rubles (about \$120).

When the theft occurs outside of Russia, the role of the non-duped mules is performed by a citizen or group of citizens of an Eastern Europe country, who within a short period of time visit several countries on the continent and in each of them open accounts in their names. Then the non-dupe mules provide the money mules manager with

the data to access all these accounts. These accounts are used later to withdraw the stolen money.

Готовые фирмы ООО, ИП,
так же фирмы в офшорных зонах.
С кэш картой, под любой вид деятельности, оказываю в наличии и под заказ.
по цене:
с рсч ИП 37т.р., ООО 50т.р.
без рсч ИП 27т.р., ООО 40т.р.

Доставка в любой город сдэк или ссе.ги, действует курьерская доставка до дома или вашего офиса.
Оплата через гарант форума.

Дражон, v

Продажа дебетовых карт, эк.кош, фирмы офшор, помощь в обнале.
контакты ЛС форума и по запросу

An example of an ad offering for sale a list of companies registered in the Russian Federation and in the offshore zone. The services of cybercriminals cost from \$560 to \$750.

Stuffers

The word “stuffer” comes from the word “stuff” (a colloquial word for “goods”). One way to withdraw stolen money is by buying goods in e-stores with the stolen money, reselling them and returning to the fraudsters their due percent. This is done by the stuffers, members of the cybercriminal groups engaged in spending money from compromised accounts on purchasing goods in online stores.

In fact, a stuffer is a variation of the money flow manager. Withdrawing money by purchasing goods is generally practiced if the stolen sums are relatively small. As a rule, the stuffers work in a team with the fences. Working “in tandem” often involves purchasing a certain type of goods, sometimes from a specific manufacturer or a clearly-defined model.

Organizer

If we consider cybercrime as a project, the organizer of the criminal group is its general manager. Their duties usually include financing the preparatory phase of the attack, allocating tasks to executors, monitoring their performance and interacting with third-party agents such

as mule projects and call services (if the group does not have its own). The organizer determines the targets for attacks, selects the necessary “specialists” and negotiates with them.

Stages of the attacks

It should be noted that the above classifications are not set in stone. In some cases, a single member of the criminal group can combine several roles. Nevertheless, regardless of how many people execute them, each of the roles described can be found when investigating almost every money-related cybercriminal incident. Here’s how they work in “real time.”

1. **Exploration.** When it comes to targeted attacks on a specific company, the organizer first instructs the contractors to collect information about the company, which will help to develop a plausible social engineering scheme for the first stage of attack. If we are talking about an attack on individual users, the preliminary exploration stage is skipped or limited to choosing a “target audience” for the attack (for example, the users of the online banking service of a specific bank) and creating phishing emails and phishing sites with relevant content.
2. **Infection.** Penetration of the corporate network is performed by spear-phishing or a phishing mass-mailing that contains an attachment with the special document or a malicious web-link. Opening the attachment or following the link leads to malware infection. Often, infection occurs automatically without the user’s awareness or participation – after clicking on the link, a malicious program is automatically downloaded on the user’s computer (drive-by download) and runs on it.

In other cases, infection is carried out via compromised popular sites on which a tool is placed that invisibly redirects users to a third-party site containing a set of exploits. Once on this site, the user

will be infected with malware.

Once inside the system cybercriminals use a number of malicious tools to consolidate their presence. For example, to ensure that internal sites of compromised organizations have the malware reinstalled when the organization's security software deletes the previous version. In addition, attackers are often set up within the infrastructure software of the attacked organization, enabling easy access to the internal corporate network from outside.

- 3. Exploration and implementation.** The programs for remote, hidden administration and management are downloaded onto compromised computers. They are used by cybercriminals to gain system administrators' credentials. Legal programs for remote management and administration whose functionality is known to many users are often used for this.
- 4. Money theft.** In the final stage, cybercriminals access the financial systems of the targeted organization and transfer money from its accounts to the accounts of the mule projects or [withdraw money directly at ATMs](#).

Conclusion

Financial cybercrime backed by Russian-speaking criminals has become widespread in recent years and this growth is due to a number of causes. The main ones are:

- Not enough qualified staff in law enforcement agencies;
- Inadequate legislation allowing criminals in many cases to avoid responsibility or to receive a lighter sentence;
- A lack of established procedures for international cooperation between law enforcement agencies and expert organizations in different countries.

Unlike the real world, a robbery in cyberspace usually goes unnoticed and there is a very small window for

collecting digital evidence after the crime. Further, criminals have no need to stay in the country where the crime is committed.

Unfortunately, for Russian-speaking cybercriminals current conditions are more than favorable: the risk of prosecution is low while the potential rewards are high. As a result, the number of crimes and the damage caused by them is growing, and the market for cybercriminal services is increasing momentum.



Tweet

A relatively low cost of entry (\$200) to cybercrime attracts new dealers

The lack of established mechanisms for international cooperation also plays into the hands of criminals: for example, Kaspersky Lab experts know that the members of some criminal groups permanently reside and work in Russia's neighbors, while the citizens of the neighboring states involved in criminal activity often live and operate in the territory of the Russian Federation.

Kaspersky Lab is doing everything possible to terminate the activity of cybercriminal groups and encourages other companies and law enforcement agencies in all countries to cooperate.

The international investigation of Carbanak's activity, initiated by Kaspersky Lab, is the first example of successful international cooperation. If the world is to see a serious and positive change there should be more such cases.

Reference. What is Kaspersky

Lab Computer Incidents Investigation?

Kaspersky Lab is a well-known developer of anti-malware security solutions. But the company provides comprehensive protection, and this also includes services for computer incidents investigation.

Evidence of an incident, mainly presented in the form of digital data, needs to be collected and recorded so that there are no grounds for doubt in the investigation and trial when a victim makes a court application.

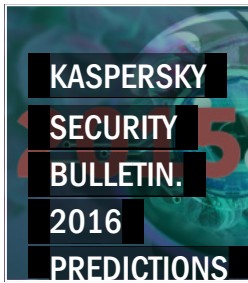
Kaspersky Lab Computer Incidents Investigation is responsible for:

- Responding to IT security incidents and providing a quick analysis of the situation;
- Collecting digital evidence and determining the circumstances of IT security incidents in accordance with established procedures;
- Analyzing the evidence collected, searching the information related to the circumstances of the incident on the Internet and fixing them;
- Preparing materials for the victim's application to law enforcement agencies;
- Providing expert support to investigative operations.

A huge amount of data is processed when responding to IT security incidents and supporting investigative operations. The analysis of this data, in combination with statistics on malicious objects detected identifies the trends of criminal behavior in cyberspace.

The Kaspersky Lab Computer Incidents Investigation Department was established in 2011 and involves six forensic experts.

Related Articles



THERE IS 1 COMMENT

If you would like to comment on this article you must first [login](#)



John

Posted on November 19, 2015. 2:00 pm

Superb article which nicely sets out the structure and operation of these criminal networks.

I have distributed a link to this article to several of my clients in the UK.

Keep up the good work.

[Reply](#)
