Trend Micro Incorporated
Research Paper
2012

# Russian Underground 101

Max Goncharov

# Contents

## Introduction

This research paper intends to provide a brief summary of the cybercriminal underground and shed light on the basic types of hacker activity in Russia. The bulk of the information in this paper was based on data gathered from online forums and services used by Russian cybercriminals. We also relied on articles written by hackers on their activities, the computer threats they create, and the kind of information they post on forums' shopping sites.

Online fraud has long since moved from being a mere hobby to a means for cybercriminals to earn a living. This paper examines what is being sold on the most popular cybercrime forums like antichat.ru, xeka.ru, and carding-cc.com; which items are in demand; and what services professional fraudsters offer.

The fraudsters consider the Internet a playing field. It has many vulnerable sites and a great deal of unprotected data. While "protected" data do exist, the places they are stored in can still be hacked. Some cybercriminals shared their experience in hacking; generating traffic; and writing code for Trojans, exploits, and other malware via online articles.

This paper discusses fundamental concepts that Russian hackers follow and the information they share with their peers. It also examines prices charged for various types of services, along with how prevalent the given services are in advertisements. The primary features of each type of activity and examples of associated service offerings are discussed as well.

Each section of this paper focuses on a specific type of criminal activity, good, or service in the Russian underground market.

## File Encryption and Crypting Services

File crypting is primarily employed to conceal infected files or malware from security software. The offerings in the crypting market can be categorized into two—actual service provision to encrypt individual files (e.g., .EXE and .DLL files) and crypter sales. To hide a malicious file or malware from security software, cybercriminals use various crypting techniques. The more effective the technique used, the more expensive a file is.

One of the most important things to be aware of in this sphere is the crypter stub, a piece of code used to decode an encrypted piece of malicious code. A particular crypter stub is attached to and used in conjunction with a certain encrypted file, somewhat increasing the final file's size.

Crypters can be classified as either statistical or polymorphic. A statistical crypter's stub is a separate program to which the encrypted file is tied. When launched, the file is extracted, decoded, and executed. Some crypters do not write the file to the hard disk, they instead launch the file from memory. This crypting method, however, is not effective.

Statistical crypters use different stubs to make each encrypted file unique. That is the reason why authors usually create a separate stub for each client. A stub that has been detected by security software has to be modified or, in hacking terms, "cleaned."

Polymorphic crypters are considered more advanced. They use state-of-the-art algorithms that utilize random variables, data, keys, decoders, and so on. As such, one input source file never produces an output file that is identical to the output of another source file. This can be achieved by using several algorithms, including:

- **Shuffling blocks of code while preserving a malicious file's ability to run:** Blocks of code are encrypted using a specific technique. Several decoders are then created for the malware body, which is randomly decoded. This applies also to variables and other data.

- **Creating macros:** A macro is created during preprocessing. When invoked, it repeatedly performs an instruction.

- **Inserting garbage code:** Blocks are split into sections, in-between which garbage instructions are inserted. These instructions do not affect the code but force an emulator to "sweat." Not only are garbage instructions used in code blocks, these are also used to execute helpful actions that complicate the work of an anti-malware analyzer in every possible way.

- **Combining all of the above-mentioned methods:** All of the aforementioned methods, along with dynamically generating algorithms after encrypting a specific block of code based on random conditions, may also be used.

Joiners [Склейка] refer to a variation of crypters. A joiner, aka a "binder," is a program used to stitch several files (e.g., a .JPG file and a malicious .EXE file) together and put them in a single container. When launched, the container extracts the files from the container and executes them. As a result, the composite file will have the extension name .exe, .bat, .cmd, .scr, .com, or .pif. Malware are most commonly made compatible with highly popular programs to ensure that these will affect as many users as possible.

On average, crypting services cost US$10–15. Offerings costing US$6 and US$50 can, however, also be found, depending on what kind of crypting service is required and how complicated the service is. Polymorphic crypters, which usually encrypt .EXE and .DLL files, cost more.

Crypting services that use infamous malware such as ZeuS, Pinch, and other bots and Trojans are also most frequently sold online. ZeuS encryption services, for instance, cost US$30–50. These can, however, also be bought at lower prices. Crypting and obfuscation services are also available for exploits at US$10–30. The more complex the service is, the more expensive it is. A one-time exploit crypting service bundle costs approximately US$50–150 per subscription, which includes five crypters in a span of one month. File-stitching services cost US$10–15. In general, regular and wholesale customers can get special offers for file encryption and other services.

## Crypter Prices

| Offering | Price |
|---|---|
| Basic statistical crypter | US$10–30 |
| Stub crypter with various add-ons | US$30–80 |
| Polymorphic crypter | US$100+ |
| Joiner | US$10–30 |

*Table 1: File encryption and crytping service prices*

Some exotic offerings are also available such as a service that stitches a .PDF file and an .EXE file into a .PDF file.

Here's a sample cybercriminal post offering crypting services (translated from Russian):

*"You give me an .EXE and any ordinary .PDF file (if you don't have one, I can use a blank .PDF or my own) that should be shown to the user. I will stitch them together and give you a toxic .PDF file. When it's opened, the .EXE and .PDF are extracted and the toxic .PDF is replaced by the ordinary .PDF and displayed to the user. This service costs US$420."*

## Dedicated Servers

A dedicated server [Дедики] is one that a user does not share with others. It can be used for various malicious activities, ranging from brute forcing to carding, that a hacker would prefer not to do on his own machine. Hackers typically connect to a dedicated server via VPN, which provides them anonymity. Dedicated servers are among the most popular goods in the underground market. These are considered unique consumables with more or less constant demand. Dedicated servers are usually sold by the tens or hundreds with prices depending on their processing power and, to a larger extent, Internet access speed.

Servers are a must in a cybercriminal operation, particularly for brute force attacks on wide ranges of IP addresses. Hackers also offer brute-forcing services because dedicated servers have so-called "lifetimes," depending on several factors, the most important of which are what measures an administrator implements to ensure server security.

Bulletproof-hosting services [абузоустойчивые], which allow cybercriminals to host any kind of material on a site or page without worrying about it being taken down due to abuse complaints, are also widely available in the underground market.

### Dedicated Server Prices

| Offering | Price |
|---|---|
| Dedicated server | US$0.50-1 |
| Powerful server | US$10-20 |
| Bulletproof-hosting service (i.e., VPS/virtual dedicated server [VDS]) | US$15-250 per month |
| Bulletproof-hosting service with distributed denial-of-service (DDoS) protection, a 1Gb Internet connection, and other extra features | US$2,000 per month |

*Table 2: Dedicated server prices*

## Proxy Servers

A proxy server [Прокся] is an intermediate computer that acts as a "proxy" or mediator between a computer and the Internet. Proxy servers are used for various purposes like accelerating data transmission and filtering traffic but their main purpose, which makes them popular among hackers, is to ensure anonymity. Anonymity, in this case, comes from the fact that the destination server sees the IP address of the proxy server and not that of the hacker's computer. Even hackers, however, frequently noted that despite the assurance of proxy server operators, all such servers, even paid ones, keep logs and cannot provide complete anonymity.

The main types of proxy servers are:

- **HTTP proxy server:** The most prevalent form of proxy server. In fact, a proxy server most often refers to this type of server. In the past, this kind of server only allowed users to view web pages and images as well as to download files. The latest versions of applications (e.g., ICQ, etc.) can run via an HTTP proxy server. Any browser version also runs via this type of proxy server.

- **SOCKS proxy server:** This kind of proxy server works with practically every kind of information available on the Internet (i.e., TCP/IP). To use SOCKS proxy servers, however, programs must explicitly be made able to work with them. Additional programs are required for a browser to use a SOCKS proxy server. Browsers cannot work on SOCKS proxy servers on their own but any version of ICQ and several other popular programs work very well on them. When working with SOCKS proxy servers, their versions (i.e., SOCKS4 or SOCKS5) must be specified.

- **CGIProxy server, aka "anonymizer":** This type of proxy server can only be used for browsers. Using it for other applications is difficult and unnecessary given HTTP proxy servers. Since this type of proxy server is expected to inherently work for browsers, using them is exceptionally easy. It is easy to enable an anonymizer to work. One can also create a CGIProxy chain without any trouble.

- **FTP proxy server:** This type of proxy server is quite rare and hardly used except in corporate networks. FTP proxy servers are commonly used by organizations that put up firewalls—systems that protect computers from external intrusion—which prevents direct access to the Internet. These are supported by many popular file managers (e.g., File and ARchive [FAR] and Windows Commander), download managers (e.g., GetRight and ReGet), and browsers.

Like dedicated servers, proxy servers must also be acquired. Various methods to do so exist, ranging from doing a simple Google search to using assorted scanners, including those that hackers write themselves. Some special Trojans also transform Internet-connected computers into proxy servers. Like dedicated servers, proxy servers are also frequently sold in bulk by the tens and hundreds and are in constant demand.

Here are sample cybercriminal posts offering proxy services (translated from Russian):

*"SOCKS service (online ~1,500 servers); price: US$2/day, US$7/week, US$13/2 weeks, US$25/3 weeks"*

*"List of proxy servers: On average, US$1.50–3 for a list of 300, US$2–4 for 500, US$3.50–5 for 1,000"*

*"List of SOCKS4/5 servers: US$3 for 100 servers"*

*"Proxy service: HTTP, HTTPS, SOCKS4, SOCKS5; prices: 5 days = US$4; 10 days = US$8; 30 days = US$20; 90 days = US$55"*

## SOCKS Bots

A SOCKS bot is embedded in a system, resides in the explorer.exe process, gets around firewalls through a driver, is recorded in stats, and opens SOCKS on a chosen port. It stores information about itself in a script, which tells it when to access a server. If a SOCKS connection succeeds, the bot writes itself to the database of valid SOCKS bots. Its processes remain invisible as it runs in the explorer.exe process. Apart from bypassing firewalls through a driver, it also bypasses proactive security measures by pinching and poking using buttons. It is easy to administer; displays all possible information about a captured machine, including the contents of protected storage; can download and execute .EXE files from any URL; self-destructs when found; has the kamikaze function; can issue commands to individual bots or bots in different countries; has two backup administrative programs in addition to a primary program for bot management; supports SOCKS5; when compressed, is only 56kb in size, which is essentially unimportant if a loader is used; is written purely in C++; and is sold for US$100.

# VPN Services

VPN technology is used to create a secure and encrypted tunnel on a computer when connecting to the Internet through which data is then transmitted. This allows a hacker to use all kinds of conventional programs (e.g., ICQ, Skype, email, or website administration) while ensuring that data remains encrypted even when transmitted. In addition, the data appears to be transferred not from the hacker's IP address but from that of the VPN service provider.

In other words, one who does not use a VPN does everything online with the aid of his chosen ISP, including opening websites and performing other services upon request. Using a VPN—an intermediary—allows hackers to encrypt all requests issued to and incoming data from the Internet. VPNs protect data and preserve their anonymity by sending requests for online resources and transmitting data using their IP addresses and not those of the users, making them valuable to hackers.

A VPN protects data by encrypting all incoming and outgoing traffic to and from the computers connected to it. It preserves anonymity, meanwhile, by allowing hackers to access websites using the unique IP address attached to it. It also allows the use of dual IP addresses, making it impossible for a provider to log traffic that comes from and goes to it.

## VPN Service Prices

| Offering | Price |
|---|---|
| 1-day service | US$1-5 |
| 7-day service | US$8-9 |
| 1-month service | US$11-40 |
| 3-month service | US$50-55 |
| 6-month service | US$105-125 |
| 1-year service | US$190-240 |

*Table 3: VPN service prices*

Here are sample cybercriminal posts offering VPN services (translated from Russian):

*"PPTP VPN, open VPN, double VPN service, price: US$11/ month"*

*"VIP72.com prices: Proxy/SOCKS service—unlimited/month US$33 proxy/SOCKS service—250 SOCKS/month US$25 proxy/SOCKS service—90 SOCKS/10 days US$10, VPN: Day—US$3, week—US$9, month—US$30, 6 months—US$125, year—US$235"*

*"US—US$15/month; France—US$15/month; Brazil—US$20/ month; Mexico—US$20/month"*

* Note that VPN service prices for Mexico and Brazil cost more because they are less developed technically compared with other countries.

# Pay-per-Install Services

In the pay-per-install (PPI) service [Залив с отстуком] business model, advertisers pay publishers a commission every time a user installs usually free applications bundled with adware. In a PPI attack, an install refers to downloading and launching a file on a victim's computer. Downloads can come in the form of an exploit bundle or from a botnet. In such an attack, a user who visits an exploit-hosting site using a vulnerable browser downloads and runs a malicious script and gets his computer infected. This is one of the most popular means to distribute malware (i.e., most often Trojans).

## Pay-per-Install Service Prices

Offering download services is a widespread practice. In this business model, a customer provides the malicious file for a service provider to distribute. Download services are usually offered based on the target country.

| Offering | Price per 1,000 Downloads |
|---|---|
| Australia (AU) | US$300–550 |
| Great Britain (UK) | US$220–300 |
| Italy (IT) | US$200–350 |
| New Zealand (NZ) | US$200–250 |
| Spain (ES), Germany (DE), or France (FR) | US$170–250 |
| United States (US) | US$100–150 |
| Global mix | US$12–15 |
| European mix | US$80 |
| Russia (RU) | US$100 |

*Table 4: PPI service prices*

Mixed-traffic download services (e.g., European, Asian, or global mix) are also frequently sold.

The value of traffic is primarily based on how important its owner is. The bigger the organization it belongs to, the more expensive it is. Most of the business traffic sold come from the United States and Australia. Since most of the U.S. traffic, however, are porn related, Australian traffic is considered of higher quality and, thus, more frequently used for carding activities.

In other words, a country's rating is determined by the likelihood that a malicious file will be downloaded and opened by some businessman or firm in it, which will allow cybercriminals to gain access to all sorts of confidential information (e.g., credit card numbers) and maybe even root access to corporate sites or networks.

Two basic types of activity take place in the download service market—either a customer offers a malicious file to download service providers or a download service provider offers services to customers. Partner programs for both download- and traffic-related services also exist.

Traffic partner programs [партнерки] convert traffic to downloads. Download partner programs, meanwhile, are sold per 1,000 installs. Download partner programs usually require two components—traffic and an exploit bundle. Traffic, by itself, has no value. It must first be converted into downloads to be of any use. For instance, 1,000 unique visitors in a 24-hour period can yield up to 50 downloads.

To obtain downloads, hackers use exploits [сплоиты], which are scripts that permit the execution of a desired action through a vulnerability in some program (e.g., a browser), or exploit bundles, which are collections of exploits that have been stitched into a single script for better reach. An exploit bundle's reach is equal to the amount of traffic it turns into downloads. It is, however, impossible to precisely ascertain reach based on traffic from only 1,000 hosts; typically, at least 20,000 hosts need to be put up to enable measurement.

Maintaining an exploit bundle also requires a host. Hackers generally use dedicated servers [дедики] or bulletproof-hosting services [абузоустойчивый] in order to direct traffic [залить] to an exploit-laden web page in order to obtain downloads. The "ingredients" for getting downloads (i.e., traffic, exploits, and bulletproof hosts) are sold separately.

Here's a sample cybercriminal post offering download software, which is occasionally found online as well (translated from Russian):

*"Download bot! -=UA-BOT=- Check out my next development—a bot with simple and convenient administrative controls in PHP. It downloads and launches different programs. As a bonus, it includes the ability to execute HTTP GET requests; very similar to a DDoS (makes sense only with a large number of bots or, alternatively, for wildly cranking up counters and other such pranks, or for creating a wrapper for sensitive scripts, etc.). Contact ICQ 9490610 for all the details. As part of my testing, I'm giving away a bot configured using test administrative controls. A bot costs US$30, stitching costs US$5."*

## Programming Services

Programming services refer to those required to write computer programs. Programmers who want to make a living offer their services to write customized programs using languages that range from assembly to Python. The offerings can also be very diverse, including spammers, Trojans, and worms.

## Software Sales

Selling off-the-shelf programs constitutes a large portion of the underground market. The most popular wares include different kinds of malware, Winlockers, Trojans, spammers, brute-forcing applications, crypters, and DDoS bots. Licenses for ZeuS, Pinch, SpyEye, and other popular toolkits are also sold. Note, however, that some program vendors are not necessarily the actual programmers. The most prevalent wares available are web applications (i.e., PHP + MySQL) and programs written in C++ and C#.

## Programming Service Prices

Service prices may depend on who the programmer is. Prices are usually results of negotiations between a buyer and a programmer, depending on feature complexity, timeline, and other such factors.

Here are sample cybercriminal posts offering programming services (translated from Russian):

*"Programming service; Perl, PHP, C, Java, etc. Prices: From US$100; injects writing: From US$200; web server hacking: From US$250"*

*"Writing and selling Trojans and other malware; available: Trojan for bank account stealing—US$1,300, Trojan for web page data replacement in a client's browser—US$850, WebMoney Keeper Trojan—US$450, DDoS bot—US$350, credit card checker—US$70, backdoor—US$400, LiveJournal spammer—US$70, fakes of different programs—US$15-25"*

# Distributed Denial-of-Service Attack Services

Denial-of-service (DoS) [ДДоС] and DDoS attacks are types of hacker attacks on computers. These attacks create conditions in which legitimate computer users are denied access to system resources. Hackers who instigate these are not trying to illegally break into protected computers to steal or destroy data. They just want to paralyze websites or computers.

Schematically, a DDoS attack involves an enormous number of spurious requests from a large number of computers worldwide that flood a target server. As a result, the target server spends all of its resources serving requests and becomes virtually unavailable to ordinary users. The users of the computers that are sending the fake requests may not even suspect that their machines have been hacked.

DDoS software were initially created for nonmalicious purposes like experiments to study the throughput capacity of networks and their tolerance to external loads. In such a case, using an improperly structured ICMP packet is most effective because this requires a great deal of processing. A packet is dispatched to the sender after determining what is wrong with it. Consequently, the main objective—choking network traffic—is achieved.

The following are the different types of DDoS attack:

- **UDP flood attack:** Involves sending a large number of UDP packets to a target computer. This was more frequently used in the past but is now considered the least dangerous type of DDoS attack. This kind of attack is easy to detect because unencrypted protocols such as TCP and UDP are used during the exchange between a master controller and agents.
- **TCP flood attack:** Involves sending a large number of TCP packets to a target computer, which uses a lot of network resources.
- **TCP SYN flood attack:** Involves dispatching a huge number of requests to initialize TCP connections with a target site, which is consequently forced to expend all of its resources to keep track of the partially open connections made. In this attack, the hacker sends synchronization packets to a target. After receiving the first packet, a victim's computer sends a response (i.e., SYN ACK) and waits for an ACK packet that will never come, causing a DDoS.
- **Smurf attack:** Involves sending ICMP ping requests to a target broadcast address using a fake source address via IP address spoofing.
- **ICMP flood:** Similar to a Smurf attack minus the broadcasting part.

DDoS attacks usually require the use of specially crafted bots and botnets. To instigate a DDoS attack, a hacker must first gain access to a target computer. He then installs a daemon in it using his DDoS bot kit. He then does the same thing to several other machines, turning them all into zombies. The hacker then starts the master program, which also comes from the DDoS bot kit, on his own or on a remote system and orders it to launch an attack on a chosen IP address. The master program then commands all of the daemons to attack the chosen victim for purposes like taking down a particular website.

## Distributed Denial-of-Service Service Prices

| Offering | Price |
|---|---|
| 1-day DDoS service | US$30–70 |
| 1-hour DDoS service | US$10 |
| 1-week DDoS service | US$150 |
| 1-month DDoS service | US$1,200 |

*Table 5: DDoS service prices*

Here are sample cybercriminal posts offering DDoS services (translated from Russian):

*"Optima DDoS bot: The file name on the system isn't numbers and it isn't just a set of random letters. Rather, it is a perfectly fitting word or abbreviation, albeit randomly generated.*

- *Bypasses Windows Firewall: The administrative panel shows not only the version of the bot and the OS but it also shows the account type (e.g., administrator or standard user).*
- *A/U correspondingly*
- *Ability to overwrite: A file can be installed on top of other versions of the bot; the older copies are removed. Updating Optima requires an overwrite. The command, exe=url, is used to perform an update. An entire team has worked on the bot: Testers, coders, vendors, and promoters. This means that every day, the bot is getting better. Bugs are being found and fixed quickly. The bot features four types of DDoS attack: HTTP, ICMP (ping), SYN, and UDP. Our bot places virtually no load on a system, which will allow it to remain undetected for a long time. Our bot installs in a system almost instantaneously, which avoids any suspicion from the victim. The bot is lightweight and behaves well on a system. The convenient and intuitive control panel is highly optimized, which reduces the load on the server.*
- *In two languages (RU, EN): The bot runs on 100 (!) threads; a timeout can be set. Furthermore, the threads are nearly perfectly synchronized with each other, making it possible to generate the greatest amount of HTTP traffic.*
- *Able to simultaneously attack several URLs on a single server*
- *Attack individual servers (e.g., a forum, a news block, or file storage): During this type of attack, each bot instance selects targets independently, which results in a manifold increase in the server load because the responses cannot be cached.*
- *Able to transfer and launch your .EXE files*
- *SOCKS5 proxy support: The standard port is 1080 but it can be changed when a build is created. Note that this is ordinary proxying—it doesn't work over NAT. The bot is compatible with the entire Windows family: Microsoft Windows 95–Windows7. There's no reason not to install.*
- *Works correctly on 64-bit systems*
- *Works correctly under both an administrator's account and a standard user's account*
- *Protects against unfair downloads (if a bot is downloaded on a PC that is already infected, the word "FAIL" is displayed in the administrative panel). In individual cases, it may be possible to arrange for shutting down a process or processes and other light tweaking.*
- *Fabulous performance*
- *Advanced system for issuing user agents and referrals: It's randomly generated for each call.*
- *Continuous technical support*
- *Regulates the strength of the attack*
- *A command can be followed by a parameter that indicates a delay for each thread (e.g., | 5): The values range from 0 to 9; "0" means "no delay." The default is "1." See the FAQ for more information. This change increases the bots' ability to survive.*
- *Supported by the dd1 and dd2 commands*
- *Support for certain features to bypass certain anti-DDoS protection measures: The bot emulates a browser.*
- *Modularity: You can buy bot add-ons (i.e., general purpose and custom).*
- *Minimal: The DDoS bot with no free advertising is US$450.*
- *Standard: The DDoS bot plus one month of free advertising is US$499."*

*"Smoke DDoS bot; HTTP GET/POST flood, UDP flood, SYN flood; price: US$300; rebuild: US$30"*

*"DDoS bot 'ibot'; price: US$350 (for the first five customers)"*

*"DARKNESS (OPTIMA) DDoS bot HTTP, ICMP (ping), trash, SYN 100 threads price—pack: US$350, updates: US$85, rebuild: US$35"*

*"DDos bot G-Bot; price: US$150; builder: US$1,500"*

## Spamming Services

Spamming [Спам] refers to the mass distribution of messages online. Spam can be themed or unthemed. Themed spam are meant for a specific target audience (i.e., dating, job search, business, and pornographic site frequenters). A database of bulk message recipients plays a key role in distributing themed spam.

Unthemed spam, on the other hand, are sent to virtually anyone in a particular order. What is most important to this kind of spam is that they get to as many users as possible.

Spam can also be categorized in terms of distribution medium—email, ICQ, social network, or forum spam. Each medium requires its own set of recipients and distribution resources.

## Spamming Service Prices

The spamming service market is quite diverse. Databases and forum and social networking accounts are most in demand. Databases are usually sold in bulk, depending on the target audience (e.g., date or job seekers).

Social networking account credentials, which are required for spam distribution, are also available in the market. Spam distribution tools and/or programs via ICQ and email can likewise be bought. Tools to spam forums and social networks, however, are less commonly seen. Their prices depend on features, distribution speed, and the like.

Private spamming services, which are used to distribute messages using a customer or proprietary user database, are more expensive.

Several flooding services, particularly call and SMS flooding services, are also available in the market though they are not that commonly seen. If at all, the main goal of their users is to annoy victims.

| Offering | Price |
|---|---|
| Cheap email spamming service | US$10 per 1,000,000 emails |
| Expensive email spamming service using a customer database | US$50–500 per 50,000–1,000,000 emails |
| SMS spamming service | US$3–150 per 100–10,000 text messages |
| ICQ spamming service | US$3–20 per 50,000–1,000,000 messages |
| 1-hour ICQ flooding service | US$2 |
| 24-hour ICQ flooding service | US$30 |
| Email flooding service | US$3 for 1,000 emails |
| 1-hour call flooding service (i.e., typically takes call center services down) | US$2–5 |
| 1-day call flooding service | US$20–50 |
| 1-week call flooding service | US$100 |
| SMS flooding service | US$15 for 1,000 text messages |
| Vkontante.ru account database | US$5–10 for 500 accounts |
| Mail.ru address database | US$1.30–19.47 per 100–5,000 addresses |
| Yandex.ru address database | US$7–500 per 1,000–100,000 addresses |
| Skype SMS spamming tool | US$40 |
| Email spamming and flooding tool | US$30 |

*Table 6: Spamming and related service prices*

## Botnets

A botnet is a network of computers that are somehow controlled from a single control center—a command-and-control (C&C) server. A standard botnet comprises a C&C server and bots or zombies. Botnets can, however, exist without a C&C server. In this case, a botnet uses a peer-to-peer (P2P) architecture. Commands are transmitted from one bot to another, making botnet takedown substantially more complicated to perform. Certain chat protocols such as IRC can also be used to control the bots in such a botnet. A botnet command center can also take the form of a web server—the most prevalent method at present, an instant-messaging (IM) medium (e.g., ICQ or Jabber), an IRC channel, or other more exotic methods.

To add a machine to a botnet, a special program must be installed in it. This program allows hackers to remotely execute certain actions on a compromised machine. A computer can get infected in various ways (e.g., drive-by downloads and vulnerability exploitation).

Botnets are rather versatile resources as they can be used for spamming, launching DDoS attacks, and instigating mass downloads. Botnet owners, aka "botnet masters," can also rummage through the logs bots send. These logs can contain all sorts of information valuable to fraudsters like victims' social networking account passwords and credit card numbers.

## ZeuS

One of the most infamous botnet toolkits is ZeuS, which created botnets that remotely stole personal information from victims' computers. ZeuS botnets intercept WinAPIs in UserMode (Ring 3), which means that a bot does not need drivers or calls in Ring 0, the level with the most number of privileges. This feature allows the bot to run regardless of a user's access rights to an infected computer (i.e., administrator, user, or guest). It also guarantees stability and adaptability to any Windows OS version.

A bot can do the following:

- Sniff TCP traffic
- Intercept FTP logins via any port
- Intercept POP3 logins via any port

- Intercept any type of data in transit

Everything that a user lets his system "remember" for him (e.g., user names, passwords, and other form data) becomes accessible to ZeuS. Even if a victim does not save such information in an infected computer, however, a bot can still keep track of what keys he pressed and in what order they were pressed when logging in to a certain site via keylogging. All of this information is then sent to the botnet master.

Some sites use virtual keyboards to help users avoid being spied on. ZeuS, however, can also come with a mechanism that allows hackers to intercept data via screen captures. As such, it can be said that ZeuS allows control of all kinds of data that pass through bots' browsers. It has, for instance, the ability to change the contents of a web page whose address is in its configuration file without the victim's knowledge. It generally adds fields for confidential data. Some sites create special digital signatures or certificates in computers upon registration. These are validated on every subsequent visit. If a user's browser does not present the appropriate certificate to a site, that site will not grant it full access. Even these certificates, however, are not safe from ZeuS as it also has the ability to find such certificates in an infected computer, steal them, and send them off to a hacker.

Hackers who use compromised computers for malicious purposes like distributing spam utilize ZeuS to install all of the necessary software in a bot as well. As such, even computers that do not have confidential information saved in them can still prove useful for a variety of malicious activities, hence, ZeuS's infamy.

## Botnet Prices

| Offering | Price |
|---|---|
| Bots (i.e., consistently online 40% of the time) | US$200 for 2,000 bots |
| DDoS botnet | US$700 |
| DDoS botnet update | US$100 per update |

*Table 7: Botnet prices*

* Note, however, that botnets are rarely sold in the underground market. Hackers normally operate their own botnets because selling them is less profitable.

Here are sample cybercriminal posts offering ZeuS services (translated from Russian):

*"I'll sell ZeuS 2.0.8.9 source code. Private sale of source code. Price: US$400–500; bargaining (swapping) is possible."*

*"Selling ZeuS 2.1.0.1 bin + set up on your hosting for US$200 escrow is accepted."*

*"I'll sell a Zeus 2.0.8.9 builder + administration controls. I also do builds. Price: US$300. Build price: US$100."*

*"LOGS-ZeuS logs (2.4Gb) DE FR IT GB, price: US$250."*

*"Installation of ZeuS in your host: US$35. Installation of ZeuS in my host: US$40."*

*"Setup of ZeuS: US$100, support for botnet: US$200/month, consulting: US$30."*

## Security Software Checks

Some hackers offer security software checks [AV Проверка] or services to check a malicious file against various security software. The more security software a file is checked against, the more expensive the service is. In such cases, customers get reports at very little cost.

Even if various online file-checking services exist, hackers tend to be wary of them because some can be set up by security companies to obtain information about the malicious files that have been tested.

### Security Software Checking Prices

| Offering | Price |
|---|---|
| 1-time security software checking | US$0.15–0.20 |
| 1-week subscription | US$10 |
| 1-month subscription | US$25–30 |

*Table 8: Security software checking prices*

## Trojans

A Trojan [Трояны], short for a "Trojan horse," is a malware masquerading as a legitimate computer program or application. Trojan spyware, malware specifically designed to steal user data, are also available. The kinds of data Trojan spyware steal include ICQ passwords, contact lists, confidential documents, bank account numbers, and the like. Forum and social networking account credentials do not come cheap.

ICQ numbers are used to distribute spam or for flooding purposes. FTP account credentials are sold and used for blackhat search engine optimization (SEO) purposes.

Trojans can also include keyloggers and other spyware that track various user actions. The best known Trojans include the following:

- Limbo
- Adrenalin
- Agent DQ
- Pinch
- ZeuS
- SpyEye

### Trojan Prices

Here are sample cybercriminal posts offering Trojans (translated from Russian):

*"Spider Keylogger Pro v. 1.2.4. FUD 100%. Price: US$50."*

*"Trojan (steals passwords from Opera, Mozilla Firefox, Chrome, Safari, Mail.ru agent, qip). Price: US$8."*

*"Backdoor for sale (software for remote access to computers); price: US$25; price of source code: US$50."*

*"Keylogger Detective 2.3.2 (Trojan with hidden installation); price: US$3."*

*"Trojan emulates WebMoney Keeper Classic; price: US$500."*

*"Check out my private version, which was designed to intercept keys for the widespread iBank banking system. iBank is used by major banks in the CIS such as AlfaBank, UkrSotsBank, Bank of Moscow... For details, review the list of banks (Russia). The main functionality is implemented in a DLL and begins working automatically as soon as the library is loaded to memory (i.e., you can easily add the functionality to your tools). This is how it works:*

- *The Trojan searches for the bank's client window, captures all key presses, and calls to files in the Java virtual machine (i.e., THERE ARE NO FAKE WINDOWS that can easily give away the Trojan's presence on the machine due to the absence of the bank's logo).*

- *After the bank's client window has been closed, the Trojan creates a session file based on the captured data that contains all the pressed keys and the bank key in an encoded form!!! The Trojan is suited to both online and local versions of the bank's client application."*

*"I also offer an ICQ bot that gives command-line access to a machine and has an integrated CONNECTED-DEVICE DETECTOR (i.e., you'll know when the bank token has been inserted!!)!!! Size: 15kb uncompressed; developed in assembly (FASM). For eavesdropping, the Trojan alters the export list of one of the Java DLLs. This ensures STABLE system operation as opposed to the INJECTION method. I'll consider selling the Trojan and source code (US$3,000)."*

*"I'm selling a program to intercept SMS. The program is based on a mobile SMS spy. It works using alarms. The program's functionality lies in its simultaneous transmission of SMS.*

- *You send an SMS from Skype to the victim's phone. An MMS arrives. When the MMS is opened, the program is automatically installed on the phone.*

- *Now, everything that comes to the victim's phone will come to you at the same time.*

- *SMS Spy lets you catch others' SMS in flight.*

*Would you like to do some spying? Do you want to be sure of your partner? Or would you like to laugh at your friends? Then you've come to the right place! Be in the know! This is the service for you! Does your girlfriend constantly send SMS and say that they are to her girlfriend? When she dials a number you can't see, does she go into another room and say that she called her girlfriend? Would you like to find out?*

- *Instant access to all services: Ability to read all of a subscriber's incoming and outgoing SMS.*

- *Function to view the sender/recipient, including his name as it is (as recorded in the address book of the phone on which the program is installed)*

- *Full stealth mode, that is, there are no external signs of the program's operation*

- *Completely anonymous, nobody will ever be able to figure out who installed the program in the phone*

- *The application works when roaming*

- *A version has been implemented that runs in complete invisible mode*

- *The mobile phone begins transmitting messages only when in standby mode, that is, when its menu is off and no buttons are being pressed*

- *Consequently, the user won't suspect a thing*

*The program costs US$350."*

*"I'm selling Limbo source code. If you don't know, this is a Trojan that has been around for two years. The price is US$300. Contact the author via PM."*

*"I'm selling three administrative controls for SpyEye 1.3 (client, main, and form grabber); plug-ins for the new version of SpyEye; collector from the new version; database dump from the new version; the most detailed manual on configuring and installing SpyEye 1.3. Each line in the settings is spelled out: What, where, how, and why. That is, all the modules from the new version. No publicity! I'm ready to show you screenshots of the administrative controls and whatever you want. The suite costs US$300."*

# Rootkits

A rootkit [Руткиты] is a program that conceals certain elements (e.g., files, processes, Windows registry entries, memory locations, network connections, etc.) from other programs or a computer's OS. Rootkits can hide processes, registry keys, and other evidence of the existence of malicious software in a computer. On Windows, all applications run in Ring 3. The system and drivers, on the other hand, operate in Ring 0. Programs that run in Ring 0 naturally have significantly greater abilities. Note, however, that it is not always possible to move from Ring 3 to Ring 0. This the reason why there are two types of rootkit—those that work at the application level and those that work at the kernel level.

Application programming interface (API) functions exist to allow communication between programs and a computer. An API is a set of functions designed so the user can access a computer's kernel at the application level. If a program wants to view a list of files in a directory, it must call a number of API functions. One of the ways by which malware conceal files is to intercept and change API function calls.

Rootkits are quite a rare commodity in the underground market. Occasionally though, threads related to rootkit sales can still be found.

## Rootkit Prices

| Offering | Price |
|---|---|
| Linux rootkit that replaces ls, find, grep, and other commands | US$500 |
| Windows rootkit that operates at the driver level and that allows the download of specially assembled drivers | US$292 |

*Table 9: Rootkit prices*

Bootkits, which are more effective than rootkits, are also available but are expensive. A boot loader for drivers makes it possible to download specially assembled drivers as soon as the OS starts.

Here's a sample cybercriminal post offering rootkits (translated from Russian):

*"The drivers are loaded before the NT kernel is initialized, which means they are loaded before PatchGuard is started. The driver's digital signature is not required. All versions of the Windows OS are supported from XP to 7 SP1, inclusive. Two architectures are supported—x86 and AMD64 (EM64T). The loader's code changes. It consists of a certain number of blocks that are randomly shifted each time the project is built. Thus, the binary image of each newly compiled loader differs from the previous one. The project is built using MS Visual Studio 2005 and MS Windows XP DDK. It is built for x86 first and AMD64. The price is US$292."*

## Social Engineering Services

Social engineering is a term crackers and hackers use to denote unauthorized access to information by means of something other than software usage. The objective is to outsmart people in order to get their passwords or other confidential information that can help cybercriminals breach their computer's security. Classic fraud types include making telephone calls to a company to ascertain who has the necessary information then calling its administrator using an employee with an urgent system access problem's identity.

In its pure form, social engineering does not attract fraudsters. Social engineering training services can, however, be found though they are quite rare. Social engineering primarily allows fraudsters to hack victims' email or social networking accounts. It also effectively lures people to visit exploit-laden and phishing web pages.

## Hacking Services

Account hacking [Взлом акков] is very popular among cybercriminals. The demand for such a service is enormous so advertisements for this abound in underground markets. The most common hacking targets are email and social networking accounts. Hacked site and forum accounts are less commonly seen. In fact, each concrete order is usually handled separately in a private conversation.

### Brute Forcing

Brute forcing [Брут] is one of the oldest means by which cybercriminals hack email and other accounts (e.g., FTP, Telnet, and ICQ). Brute forcing is simply "guessing someone's password." Special programs that automate this process are available in the underground market. All it requires is to compile a good dictionary feed. It will then try each password one at a time and report which one works.

The most popular brute-forcing programs are Brutus and Hydra. Hacking accounts via brute forcing is very difficult because the required password may not be in a program's dictionary. Besides, trying every password can take a considerable amount of time. The growth of computing power, however, is allowing brute forcing to once again gain relevance. Some cybercriminals even offer services to decrypt hashes.

### Guessing Answers to Secret Questions

Guessing answers to so-called "secret questions" is relevant to hacking email accounts. Because people frequently set questions such as "Where do I live?" or "What is your favorite food?" as prompts to access their accounts should they forget their user names or passwords, it is not so difficult for cybercriminals to hack these.

## Exploiting Website Vulnerabilities

Sites are most commonly vulnerable to SQL injection and cross-site scripting (XSS).

### SQL Injection

SQL injection occurs when a user enters data to form SQL queries without verification and a hacker inserts data that allows him to obtain any kind of information from a SQL database. The request using the query, SELECT login, password FROM members where email='$email';'', where the value of $email is entered by the user into a table, is processed on a web page. The results for such a query are also displayed on a web page. A hacker can modify this data and enter, 'my@mail.ru'OR login LIKE '%admin%'' to the form. The SQL request will then become SELECT login, password FROM members where email='my@mail.ru' OR login LIKE '%admin%';, which will then allow a hacker to obtain the passwords of users whose user names have 'admin'.

### Cross-Site Scripting

XSS is commonly used to hack email accounts. It allows JavaScript to run on a victim's browser, making it possible for bad guys to steal cookies or to hijack open sessions. XSS is, however, not easy to perform. To hack a victim's email account, an XSS vulnerability in the site that stores his account credentials must first be found. It is possible though to find and buy exploits for common vulnerabilities in Mail.ru and Yandex.ru in various forums.

### SQL Injection Cross-Site Scripting

SQL injection XSS (SiXSS) is a combination of SQL injection and XSS—instigating an XSS attack via a SQL injection vulnerability using a script.

One of the most exploited vulnerabilities via SiXSS is the so-called "include bug." To simplify the process of adding new pages to a website or other such tasks, site administrators use the include($file) function in scripts where $file is set by the user or is specified in a URL (e.g., <a href=http://victim.com/news.php?file=somefiletarget="_blank"> http://victim.com/news.php?file=somefile</a>). Instead of the include() function, the contents of somefile is inserted. This may be very convenient but if the value of the user-entered data is not verified, sooner or later, a malicious user can easily enter <a href="http://victim.com/news.php?file=/etc/passwd" target="_blank">http://victim.com/news.php?file=/etc/passwd</a> to obtain a page's contents.

The PHP include bug is quite an interesting vulnerability that can be considered a subspecies of the include bug. Unlike the include bug, the PHP include bug does not aim to get data from some file but to insert PHP code to a page and subsequently execute this code on the page's server. Those familiar with PHP know that code fragments wrapped in <? ... ?> or <?php ... ?>) are simply inserted to a web page. When processed by a server line by line, these fragments are executed. In other words, chunks of code can be inserted to a web page by exploiting a PHP include bug.

A web page with the code 'include($file)''s contents where the value of $file is set by a user can be exploited. A hacker can prepare a file in advance with the PHP code he wants to execute on a vulnerable server. He then uploads the file to his own web server and inputs the request, <a href="http://victim.com/news.php?file=http://attacker.host.com/php_code.php" target="_blank">http://victim.com/news.php?file=http://att...om/php_code.php</a>. This inserts the hacker's PHP code to the vulnerable page, which is then executed by its server.

## Using Sniffers, Trojans, Phishing Sites, and Social Engineering

To hack accounts, using sniffers, Trojans, phishing sites, and social engineering is a common practice.

A sniffer is a program that intercepts network traffic. A huge number of sniffers have already been specifically customized to capture passwords from email accounts. Account passwords can, however, be obtained by infecting victims' computers with Trojans via drive-by downloads, for instance.

As one of the oldest means by which cybercriminals steal passwords, phishing remains effective to this day. Bad guys create fake copies of login pages, which gather user credentials. Users who scrutinize URLs and pages, however, are more likely to fall for more sophisticated means of data stealing, hence the rise of social engineering.

## Hacking Service Prices

The most popular email domains cybercriminals hack in Russia are Mail.ru, Yandex.ru, and Rambler.ru. Social networks, Vkontakte and Odnoklassniki, are also popular targets. Services and tools for hacking Gmail, Hotmail, and Yahoo! Mail are also somewhat available but at premium prices. Offerings for hacking ICQ, Skype, Twitter, and Facebook accounts as well as other services are not very popular but may also be found.

| Offering | Price |
|---|---|
| Mail.ru, Yandex.ru, and Rambler.ru accounts | US$16–97 |
| Vkontakte and Odnoklassniki known accounts (no guarantees) | US$97–130 |
| Vkontakte and Odnoklassniki unknown accounts (no guarantees) | US$325+ |

*Table 10: Hacking service prices*

Here are sample cybercriminal posts offering hacking services (translated from Russian):

*"Mail.ru (@BK.ru, @inbox.ru, @list.ru): US$41; Mail.ru, Bk.ru, Inbox.ru, List.ru: US$100; Yandex, Rambler: US$150; Gmail, Googlemail.com: US$180; Yahoo.com: US$350; Hotmail.com: US$350; Odnoklassniki: US$100; Vkontakte: US$100"*

*"Mail.ru, Bk.ru, Inbox.ru, List.ru: US$97; Mail.qip.ru: US$97; Gmail.ru: US$97; Yandex, Rambler: US$130; Ngs.ru, Inbox.lv, @gmx.de, AOL.com: US$130; @i.ua (UA.fm, Email.ua), @ukr.net, @ukrpost.net, Bigmir.net: US$130; Gmail.com, Googlemail.com: US$162; Yahoo.com: US$162; Hotmail.com: US$162; if the email address for social networks, ICQ, and Skype is unknown, the cost amounts to US$325; if the email is known, then: Odnoklassniki: US$130, Vkontakte: US$130, Mamba.ru: US$130, Facebook.com: US$130, Twitter.com: US$130; IM services: Skype.com: US$130, ICQ.com: US$130; acquiring the IP address of the target: US$65; corporate email: US$500 per mailbox"*

*"Mail.ru (List.ru, BK.ru, Inbox.ru): US$70; Yandex.ru: US$70; Rambler.ru: US$70; Gmail.com: US$85; Pochta.ru: US$60; UKR.net: US$60; Odnoklassniki.ru (given an email address): US$85; Vkontakte.ru (given an email address): US$85"*

## Scanned Document Copy Sales

To confirm a user's identity, some cybercriminals require scanned document (e.g., passport, driver's license, etc.) copies. If, for instance, a hacker needs to verify a PayPal account, he needs to submit a scanned copy of the owner's passport or driver's license. Scanned document copies sell very well in the underground market. Some also offer services to rework scanned documents using a template. Scanned database copies are hard to find but do exist in the underground market as well.

## Scanned Document Copy Prices

| Offering | Price |
|---|---|
| Russian and other Commonwealth of Independent States (CIS) country passport | US$2–5 |
| European passport | US$5 |
| Document rework service | US$15–20 |
| Credit card rework service | US$25 |

*Table 11: Scanned document copy prices*

Here's a sample cybercriminal post offering a database of documents (translated from Russian):

*"Database of documents (passport, cc, driver's license, utility bill, bank statement) price: US$195; more than 500 documents and templates"*

## SMS Fraud Services

SMS fraud services are fairly rare largely due to the development of the Internet and the emergence of simpler ways to make money. Sometimes though, services to send SMS using fake numbers or to activate other services via SMS can be found.

## SMS Fraud Service Prices

| Offering | Price |
|---|---|
| SMS activation service for:<br>1–10 devices<br>11–20 devices<br>21+ devices | <br>US$0.40<br>US$0.45<br>US$0.50 |
| SMS spamming service (all Russian operators) | US$3 for 100 text messages<br>US$20 for 1,000 text messages<br>US$150 for 10,000 text messages |
| SMS spamming service (with phone number replacement) for:<br>1 text message<br>3 text messages<br>5 text messages<br>8 text messages<br>15 text messages<br>20 text messages<br>30 text messages<br>50 text messages | <br><br>US$0.15<br>US$0.35<br>US$0.65<br>US$1.15<br>US$1.95<br>US$2.75<br>US$4.15<br>US$6.95 |

*Table 12: SMS fraud service prices*

SMS delivery software are also sold.

Here are sample cybercriminal posts offering SMS services (translated from Russian):

*"Sale of SMS delivery software: Price on the official website: US$160; my price: US$100"*

*"PHP SMS flooder; speed: 2 SMS per second; price: US$16"*

*"SMS flooder for sale; price: US$65"*

## Ransomware Services

The most widespread online extortion practice involves the use of a Windows blocker. A blocker such as Winlocker is a special type of malware designed to paralyze a computer's OS. Its execution spurs the appearance of a prompt urging a user to deposit a certain amount of money to the hacker's account in order to unblock his system. Winlockers are sometimes sold in the underground market, albeit rarely.

### Ransomware Service Prices

| Offering | Price |
|---|---|
| Winlocker | US$10–20 |
| Winlocker builder | US$20–25 |
| Winlocker source code | US$8 |

*Table 13: Online extortion service prices*

## Serial Key Sales

Selling software activation keys is common in the underground market. In fact, serial keys can easily be obtained at low prices.

Here are sample cybercriminal posts offering serial keys (translated from Russian):

*"Windows 7 Ultimate: US$7, Windows 7 Professional: US$5, Windows 7 Home Premium: US$3, WinServer 2008: US$5; MS Office 2010: US$4; MS Office 2011 for Mac: US$4"*

*"Kaspersky Internet Security 2010/2011 activation keys: 1 year: US$4, 2 years: US$$7"*

# Exploits

Exploits [Сплоиты], aka "sploits," are programs, more often scripts that exploit vulnerabilities in other programs or applications. The most prevalent type are browser exploits, which enable the download of malicious files. Exploits introduce code that download and launch executable files on a victim's computer.

An example of an exploit attack is causing an integer buffer overflow in the setSlice() method in the WebViewFolderIcon ActiveX component. Using a specially constructed webpage or email, a remote user can corrupt a computer's memory and execute arbitrary code. Arbitrary code execution occurs when a person using a vulnerable browser navigates to a web page embedded with an exploit.

Exploits are usually installed in hosting servers. An exploit bundle is a special script, most often written in PHP, which combines several exploits. Using a bundle is much more effective than using individual exploits. Conventionally, bundles are categorized as either "intelligent" or "unintelligent."

An unintelligent exploit bundle simply downloads all of the exploits in a bundle at one time, regardless of what browser a victim uses. As such, it is not a very efficient solution because running several exploits in a bundle may do more harm than good. One exploit's routines may interfere with those of another exploit. Unintelligent bundles are generally less expensive than intelligent ones.

Intelligent bundles determine a victim's browser and OS versions before downloading the appropriate exploits. If they do not have an exploit for the user's OS and browser, they do not download anything.

As a rule, bundled exploits are encrypted to avoid malware detection by security software. Bundle developers also try to obfuscate their exploits' source code to prevent victims from noticing them running on websites. Each bundle may also be able to obtain statistics (e.g., a mechanism for recording the number of visitors, their OS versions, their browser versions, etc.).

An exploit's reach is a measure of its efficiency–the ratio of users on whose computers the exploit worked to the total number of users who visited a page in which it was embedded. As such, if 1,000 users visited an exploit-laden page and the computers of 200 people were successfully infected with a Trojan, that exploit's reach is equal to (200 / 1,000) * 100 or 20%.

XSS exploits are also available in the underground market. XSS vulnerability exploitation occurs when a script that is usually malicious embedded in a site is able to communicate with content in a different site or in a local HTML page, hence its name. Unlike in other attacks, hackers use servers susceptible to XSS as intermediaries to attack the visitors of infected websites, forcing their browsers to execute malicious scripts.

In an XSS attack, after the execution of a malicious script, the script begins to receive commands from a remote resource, controlling a victim's browser without alerting him to what is happening and carrying out required actions. A script may be locally invoked on a system or may reside in an inactive state on a compromised web server until the affected user makes calls to an infected web page. The script then becomes active on the user's machine and begins to execute harmful operations.

Successful XSS attacks require the satisfaction of several criteria—the use of an insufficiently secured browser that does not compare a script's origin with the permissions it seeks and a carelessly written web page that lacks sufficient data entry verification. Social engineering is frequently employed to get a potential victim to click a link to a page that has been embedded with malicious code.

The majority of XSS attacks target users' session cookies—files saved in systems every time they visit a website. Stealing cookies allows hackers to impersonate users and perform actions in their name. Cookies are transmitted to attackers via the execution of commands in the malicious script. A successful XSS exploit can prevent its victims from accessing important data and can expose them to identity theft. Hijacking sessions allow a script's owner to engage in any kind of activity that the true owner of the account is capable of like reading and deleting emails, conducting financial transactions, and writing social networking posts.

XSS can also be used to steal data from forms. XSS exploits can conventionally be categorized as either active or passive. A passive XSS exploit requires a victim's direct participation, for instance, clicking a malicious link, which requires social engineering and trickery.

An active XSS exploit, on the other hand, does not require any additional action on a victim's part. All a victim needs to do is to open an XSS-laden web page to automatically execute malicious code. Because of its automated nature, active XSS exploits are more expensive.

## Exploit Prices

Exploits may be sold individually or as bundles. Some are also available for rent.

| Offering | Price |
|---|---|
| Exploit bundle rental:<br>24 hours<br>1 week<br>1 month | <br>US$25<br>US$125<br>US$400 |
| Styx Sploit Pack rental (affects Java and Adobe Acrobat and Flash Player) | US$3,000 per month |
| Eleonore Exploit Pack v. 1.6.2 (for Microsoft Data Access Components [MDAC], IEpeers, SnapShot, HCP, JDT, JWS, PDF collab,collectEmailInfo, PDF SING, and Java Invoke(chain) 1.5/1.6; average reach of 10–25%) | US$2,500–3,000 |
| Phoenix Exploits Kit v. 2.3.12 (for Internet Explorer [IE] 6 MDAC, Java Deserialize, Java GSB, PDF Collab/Printf, Adobe Flash Player 9 and 10, IEpeers, Java SMB, HCP, PDF/SWF, PDF Open, and PDF Lib TIFF) | US$2,200 per domain |
| Less popular and less effective bundle | US$25+ |
| XSS exploit for Mail.ru:<br>Active XSS exploit<br>Passive XSS exploit<br>Passive XSS exploit for Rambler.ru and Yandex.ru<br>XSS exploit for Gmail.com | <br>US$50–150<br>US$10–35<br>US$10–50<br><br>US$200 |
| SQL exploit for a site with 50,000 visitors a day | US$100 |
| Exploit bundle crypting service:<br>1-time<br>1-month subscription (5 times) | <br>US$50<br>US$150 |

*Table 14: Exploit service prices*

## Fakes

A fake is a program that copies the interface of another program or site to capture certain kinds of data, primarily passwords. The primary objective of using a fake is to trick a user into entering his user name and password or other kinds of confidential data to a form.

Fake ICQ clients as well as bank and social networking web pages are sold online. Fakes are closely related to phishing—one of the most common methods used to commit online fraud. Phishing basically refers to a set of actions to trick users into giving away personal or confidential information. Modern-day phishing can be broken down into three types—online, email, and hybrid. The oldest phishing means is accomplished via email.

Online phishing, meanwhile, relies on the use of fakes and involves copying official sites but using similar-looking domain names or URLs. This is also known as "site spoofing," wherein users who visit fake sites type personal information into forms, believing they are in official sites.

Finally, hybrid phishing involves creating a counterfeit version of a legitimate company's website. Hackers pester users with prompts to urge them to do something on these sites.

## Fake Prices

Fakes are no longer in high demand mostly due to increased computer literacy among users. As such, fakes are rather inexpensive.

| Offering | Price |
|---|---|
| Fake site | US$5-20 |
| Fake WebMoney Keeper | US$50 |
| 1-year prepaid phishing domain (e.g., vkOntakte.net.ua and vkontaktu.net.ua) | US$50 each |

*Table 15: Fake prices*

## Traffic

Traffic [Трафф] refers to the stream of visitors to a particular website. Traffic volume refers to the number of visitors (i.e., unique or otherwise) to a site over a certain period of time. The traffic cybercriminals use can be split into two categories—traffic for exploits to get downloads and traffic for blackhat SEO purposes. Several traffic sources exist, including hacked websites, white-listed sites, doorways, and spam distributors.

Iframe traffic though is most commonly used to obtain downloads. In order to get traffic, a website is hacked by inserting an iframe to one of its pages. An iframe, aka an "inline frame," is a "floating frame." Because it is concealed, visitors to hacked sites are unknowingly and automatically led to the hackers' web pages. As a result, the hackers get a lot of traffic, which they can either sell or use for their own malicious purposes.

Managing the contents of hacked websites can be accomplished via an FTP account or a web shell. A web shell is a special program or a script designed to remotely manage the contents of a website.

Traffic can be topical in nature, depending on the kind of website it came from. Business traffic is most valuable because business site visitors are generally serious people with money. As such, their downloads are likely to turn into profit for hackers. Adult traffic (e.g. traffic from porn sites) is also worth mentioning even if less valuable because porn sites receive many visitors.

Traffic is frequently classified according to the visitors' countries. Traffic from Australia, the United States, Great Britain, Germany, and Italy are most in demand. The traffic that comes from these countries is primarily business traffic. Traffic mixes are often sold as well.

Traffic for blackhat SEO purposes increases the number of visitors to a selected website. Traffic is managed via a traffic direction system (TDS).[1]

1 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_malware-distribution-tools.pdf

## Traffic Prices

As expected, traffic costs much less than downloads. Traffic from European countries and the United States is more expensive (i.e., US$7–15 for 1,000 visitors) than traffic from other countries. Overall, the country ranking in terms of price is the same as that for downloads. Ads for TDSs may sometimes be found though very rarely.

Here are sample cybercriminal posts offering traffic (translated from Russian):

*"U.S. stream of 50,000/day; iframe. I'll sell for US$9. 30% is adult traffic; the rest is related to movies, music, games, and dating."*

*"US$6 for 1,000 visitors (IT, PL, BR, AR, ES)."*

*"1,000 visitors: US$10 (RU); 1,000 visitors: US$4 (mix)"*

*"Portal TDS + unique redirect system, price: US$600. All updates are free."*

## Blackhat Search Engine Optimization Services

SEO uses various techniques to promote websites and optimize these for searches. It is a legitimate means by which organizations raise awareness for their sites, making them appear on top of search results pages.

An important concept frequently encountered in relation to SEO involves the Topical Citation Index (TCI). It is a method used by the Yandex search engine to ascertain the "authority" of an Internet resource based on the characteristics of the links to it from other websites. The TCI is computed using a specially developed algorithm in which special weight is given to the "topical proximity" of a resource and the websites that link to it. Only approximate values are specified, which helps roughly determine websites' authority.

Several ways to improve a site's TCI exist, including registering to catalogs and article directories, commenting on forums with links back to one's site, signing guest books with links back to one's site, posting on announcement boards, and exchanging links.

Blackhat SEO is the malicious way of using SEO. It often involves the use of doorways or websites generated by a program (i.e., doorway generator) whose pages are optimized (i.e., have a lot of search spam and crosslinks) for various search queries in order to redirect visitors, aka "drones," to a certain website.

Xrumer [Хрумер] is one of the most popular blackhat SEO tools available online. Several versions of the program, in fact, are sold with features like:

- **Direct posting:** A customer's text is distributed in forums, guest books, or blogs.
- **Aggressive posting:** Similar to direct posting, except for the fact that a topic is created in all of the sections of more than one forum.
- **Profile use:** Profiles with links to the customer's site are registered on home pages, resulting in "endless" back linking.

- **Ref spam method use:** Consists of sending ref requests to a website's pages with referer="your_website" set in the request. As a result, the address of a customer's website is displayed on all of the websites on a special page, primarily focusing on search engines.

## Blackhat Search Engine Optimization Service Prices

| Offering | Price |
|---|---|
| Xrumer database with 30,000 sites (mostly RU and EN):<br>Direct posting<br>Aggressive posting<br>Profile use<br>Ref spam method use | <br>US$20<br>US$25<br>US$20<br>US$7 |
| Xrumer 7 Elite (licensed) | US$295 |
| Xrumer 7 posting service:<br>With 9,000–10,000 profiles<br>For 30,000 posts | <br>US$20<br>US$7 |
| Xrumer posting on forums, blogs, and guest books | US$6 per 100,000 posts |

*Table 16: Blackhat SEO service prices*

Here's a sample cybercriminal post offering SEO services (translated from Russian):

*"SEO service in YouTube, MySpace, FaceBook, Twitter; prices: YouTube: 1,000 views for US$16; MySpace: 5,000 plays of track (views of page): US$50; 1,000 Facebook Likes: US$140; 1,000 Twitter followers: US$35"*

## Conclusion

As the Russian underground community continuously modifies targets and improves technologies, security companies and users must constantly face the challenge of effectively protecting their money and the information they store in their computers and other devices.

This paper covered only the most basic and fundamental tools and technologies cybercriminals create and use to enhance their business. It also contains pricing snapshots gleaned from underground forums in order to paint a comprehensive picture of the Russian underground economy and how much it resembles real-world business.

The Russian shadow economy is an economy of scale, one that is service oriented and that has become a kleptocracy wherein crony capitalism has obtained a new lease on life in cyberspace.

# Appendix

Based on ongoing research and monitoring of various Russian underground forums, we assessed the popularity of various malicious activities and/or services and ranked them below:

1. Programming services and software sales
2. Hacking services
3. Dedicated server sales and bulletproof-hosting services
4. Spam and flooding services, including call and SMS flooding services
5. Download sales
6. DDoS services
7. Traffic sales
8. File encryption services
9. Trojan sales
10. Exploit writing services and sales
11. Scanned document copy sales and reworking services
12. Ways to earn money online document sales
13. Proxy sales
14. Fake sales
15. Botnet and bot sales, particularly ZeuS botnets
16. VPN services
17. Blackhat SEO services
18. Serial number and activation code sales
19. SMS fraud services
20. Windows blocker sales and ransomware services
21. Security software checking services
22. FTP account and web shell sales
23. Malicious code obfuscation services
24. Rootkit sales

The top 10 forums where Russian cybercriminals buy and sell their wares were:

1. antichat.ru
2. xeka.ru
3. carding-cc.com
4. Exploit.IN
5. InAttack
6. XaKePoK.su
7. HACKER-PRO CLUB (HPC)
8. XAkNet.ru
9. zloy
10. HackForce.RU

## TREND MICRO™

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.


## TREND MICRO INC.

**10101 N. De Anza Blvd.**
**Cupertino, CA 95014**

**U.S. toll free:** 1 +800.228.5651
**Phone:** 1 +408.257.1500
**Fax:** 1 +408.257.2003
www.trendmicro.com


TREND MICRO™

Securing Your Journey to the Cloud