

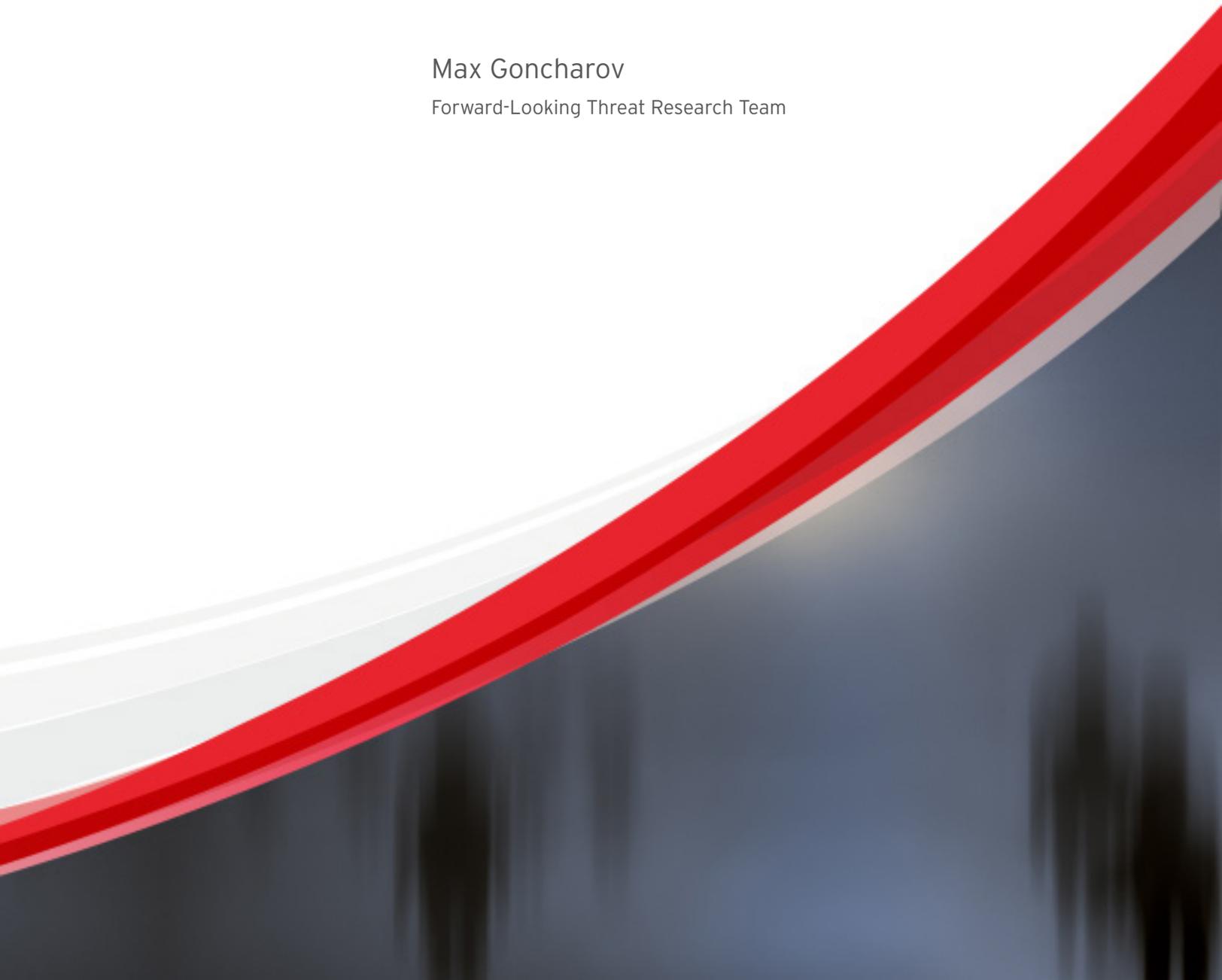
A Trend Micro Research Paper

CYBERCRIMINAL UNDERGROUND ECONOMY SERIES

# Russian Underground Revisited

Max Goncharov

Forward-Looking Threat Research Team



## Contents

Cybercriminal Underground Economy Series .....	1
Introduction.....	2
Methods Used to Gather Underground Market Data .....	3
Normalizing Prices.....	3
A Product or a Service? .....	3
What Characterizes the Russian Underground Market? .....	4
Products .....	5
Trojans .....	5
Exploits and Exploit Bundles .....	5
Rootkits.....	7
Traffic.....	7
Crypters .....	8
Fake Documents.....	9
Stolen Credit Card and Other Credentials .....	10
Services.....	10
Dedicated-Server-Hosting Services.....	10

### TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.



Proxy-Server-Hosting Services.....	11
VPN Services.....	11
Pay-per-Install Services.....	11
Denial-of-Service Attack Services.....	13
Spamming Services.....	13
Flooding Services .....	14
Malware Checking Against Security Software Services .....	14
Social-Engineering and Account-Hacking Services.....	14
Account-Hacking Services .....	15
Brute-Forcing Services .....	15
Account Hacking via Social Engineering Services.....	15
Cybercriminal Wares Sold in the Russian Underground Market .....	16
Conclusion.....	19
Appendix.....	19
List of Cybercriminal Underground Wares Trend Micro Tracks and Monitors .....	19
Products.....	19
Services .....	20
Russian Underground Glossary.....	21

## Cybercriminal Underground Economy Series

Places in the Internet where cybercriminals converge to sell and buy different products and services exist. Instead of creating their own attack tools from scratch, they can instead purchase what they need from peers who offer competitive prices. Like any other market, the laws of supply and demand dictate prices and feature offerings. But what's more interesting to note is that recently, prices have been going down.

Over the years, we have been keeping tabs on major developments in the cybercriminal underground in an effort to stay true to our mission—to make the world safe for the exchange of digital information. Constant monitoring of cybercriminal activities for years has allowed us to gather intelligence to characterize the more advanced markets we have seen so far and come up with comprehensive lists of offerings in them.

In 2012, we published “Russian Underground 101,” which showcased what the Russian cybercriminal underground market had to offer.<sup>1</sup> That same year, we worked with the University of California Institute of Global Conflict and Cooperation to publish “Investigating China’s Online Underground Economy,” which featured the Chinese cybercriminal underground.<sup>2</sup> Last year, we revisited the Chinese underground and published “Beyond Online Gaming: Revisiting the Chinese Underground Market.”<sup>3</sup> We learned then that every country’s underground market has distinct characteristics. So this year, we will add another market to our growing list, that of Brazil.

The barriers to launching cybercriminal operations lessened in number than ever. Toolkits are becoming more available and cheaper; some are even offered free of charge. Prices are lower and features are richer. Underground forums are thriving worldwide, particularly in Russia, China, and Brazil. These have become popular means to sell products and services to cybercriminals in the said countries. Cybercriminals are also making use of the Deep Web to sell products and services outside the indexed or searchable World Wide Web, making their online “shops” harder for law enforcement to find and take down.

All of these developments mean that the computing public is at risk of being victimized more than ever and must completely reconsider how big a part security should play in their everyday computing behaviors.

---

1 Max Goncharov. (2012). “Russian Underground 101.” Last accessed February 27, 2014, <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf>.

2 Zhuge Jianwei, Gu Liang, and Duan Haixin. (July 2012). “Investigating China’s Online Underground Economy.” Last accessed February 27, 2014, [http://igcc.ucsd.edu/publications/igcc-in-the-news/news\\_20120731.htm](http://igcc.ucsd.edu/publications/igcc-in-the-news/news_20120731.htm).

3 Lion Gu. (2013). “Beyond Online Gaming Cybercrime: Revisiting the Chinese Underground Market.” Last accessed February 27, 2014, <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-beyond-online-gaming-cybercrime.pdf>.

## Introduction

In 2012, we published “Russian Underground 101,” which provided a brief summary of the cybercriminal underground and shed light on the basic types of hacker activity in the region. This year, we revisited the Russian cybercriminal underground market to update the information we provided then. As in the 2012 paper, the bulk of the information in this paper was based on data gathered from online forums and services used by cybercriminals in the region. 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. It also discusses fundamental concepts that hackers follow and the information they share with their peers and compares product and service prices from 2011 to 2013. Primary features of each product or service and examples are also provided.

This paper is divided into five main sections—introduction, what characterizes the Russian underground market unique, products, services, and cybercriminal ware offerings in the market. This section discusses how we gathered data, normalized prices, and classified an offering as either a product or a service to answer questions we received when we published the 2012 paper. The second section characterizes the Russian underground market. It differentiates the region’s underground market from others. The third and fourth sections, meanwhile, provide detailed descriptions of the most common products and services, respectively, offered in the Russian underground market. The last section provides pricing information on the products and services sold in the market.

The cybercriminal underground economy, much like any other type of business economy, experiences pricing highs and lows, depending on demand and supply. In the Russian cybercriminal underground market’s case, the huge demand for credit card credentials drives prices up. Then again, incidents such as the massive breaches involving popular retailers a few months ago, which increased the supply of such credentials, drive prices down.

Unlike legitimate businesspeople, however, cybercriminals need to keep their identities secret and, as much as possible, hide all traces of their “business” transactions. Factors like this make real-time transactions almost impossible to do in the underground market. That said, business dealings in cybercriminal underground markets are much slower than in the legitimate business world.

Even though the prices of most products and services sold in the Russian underground market have been decreasing, that does not mean that business is not doing well for cybercriminals. It can even mean that the market is growing, as we see more and more product and service offerings as time passes. Cybercriminals, like legitimate businesspeople, are also automating processes, resulting in lower product and service prices. Of course, “boutique” products and services remain expensive because these involve specialized knowledge and skills to develop that only a few bad guys have. What we all need to keep in mind is that as long as profit can be made, cybercriminals will continue to offer products and services that can make life easier for themselves and their peers. And as long as customers exist, the cybercriminal underground will thrive. As users and potential victims, we all need to keep an eye out for the latest misdeeds to stay safe from all kinds of digital threats.

## Methods Used to Gather Underground Market Data

Trend Micro has been collecting underground market product and service data since 2009. We have also been continuously improving the gathering process by using in-house-designed and -developed tools. As such, our data collection has become fully automated though post-processing is manually done if, for instance, we want to normalize information such as product or service prices. Apart from this data, we also collect nicknames, email addresses, ICQ numbers, and Skype handles for possible forensic investigation.

At present, we categorize the data we collect into 33 groups (see Appendix). We find similarities among the bits of information we collect and combine related data together because cybercriminals often post details on their product or service offerings on several forums at the same time. Note, however, that some wares can fit in more than one category. Malicious traffic, for instance, is categorized under pay-per-install (PPI) services, traffic (i.e., for reselling purposes), and blackhat search engine optimization (SEO) services. Not limiting products and services this way allows greater flexibility in terms of data correlation.

## Normalizing Prices

The Trend Micro 2012 paper on the Russian underground market spurred several discussions in the security industry regarding inconsistencies with pricing. Based on experience, price gaps occur not only because of the wide range of available product and service options in the market but also because of differences in terms of quality and quantity.

Let us compare underground market wares with cars. A car can cost between thousands and millions of dollars. Of course, how much a car costs depends a great deal on its quality. The rarer the car is and the better its quality, the more expensive it often is. The same is true for underground market wares. If the most inexpensive bulletproof virtual private network (VPN) service offered in 2013 costs around US\$15 and the most expensive costs around US\$135, then the average price would be around US\$75. The prices featured in this paper are based on analyses of the data we collected.

## A Product or a Service?

Like the 2012 paper, this paper will also present a wide range of underground market product and service offerings. We classify a ware as a “product” if the buyer needs to do everything on his own after buying the tool to carry out an attack. In the case of botnet attacks, for instance, he can buy a botnet kit (i.e., a product), which can come with different modules, plug-ins, and so on. Renting a botnet, however, is classified under “services” because the customer does not have to worry about running or maintaining the botnet. He can simply gather the information he needs from its owner for use in his attacks. In the legitimate computing market, an example of a product would be Microsoft™ Office® while that of a service would be Office 365. To use the former, you need to install the software and buy a license for it. You cannot use it if you do not have it installed on your computer. You can, however, use the latter on any device as long as you have access to the service.

## What Characterizes the Russian Underground Market?

The Russian cybercriminal underground has been around since 2004. It then served as a place wherein cybercriminals exchanged information with their peers. Its biggest players included zloy.org, DaMaGeLaB, and XaKePoK.NeT. As the trade volume increased, underground forums became ideal places for closing deals and a platform to advertise malicious wares. They served as marketing instruments to monetize crimeware. The underground market slowly transformed into a marketplace of all sorts of products and services that aid cybercriminals in crafting and implementing malicious schemes.

The Russian underground market adheres to common trading and information exchange principles. As a pioneer, it was the first market to offer crimeware to cybercriminals. They no longer had to create their own tools for use in attacks, they had the option to buy from peers instead. The Russian underground market is also characterized by specialized offerings. As such, an individual or a group may solely offer file crypting services, distributed denial-of-service (DDoS) tools, or traffic direction systems (TDSs). Individuals or groups earned money by only selling products or services they excelled in producing or doing. They did not offer everything; they specialized instead.

As with the specialization that goes on in the Russian underground market, every market has its own specialty. The Russian market, for instance, specializes in selling TDSs and offering traffic direction and PPI services. In fact, traffic-related products and services are becoming the cornerstone of the entire Russian malware industry, as buying Web traffic can not only increase the cybercriminal victim base, sifting through the traffic stored in botnet command-and-control (C&C) servers can also help threat actors find useful information for targeted attacks.

As has been said, most of the time, sellers and buyers meet in underground forums. Buyers go to forums to check a seller's reputation (i.e., if he sells quality products and services), what products and services are offered, and how some deals went. To ensure both of their safety, sellers and buyers use escrows or "garants"—third parties who get and keep the buyers' money until the purchase is finalized. This protects the sellers because escrows make sure the buyers have the money to pay for the products or services sold. Escrows also test the products or services sold by the sellers to make sure the buyers get what they paid for and will not become victims of false advertising. When buying and selling stolen credit card credentials, for instance, an escrow checks several numbers to confirm their legitimacy before handing the payment the buyer gave him for safekeeping to the seller. Escrows usually get 2–15% of the sales price for their services, depending on the agreement between buyers and sellers and other circumstances.

The number of Russian underground forums has been growing each year. Even though some forums come and go, the most popular ones just change hosting service providers and domain names every so often but keep their loyal members. The most popular Russian underground forums such as verified.su and ploy.org can have 20,000 to several hundreds of unique members.

Forum members use all kinds of tricks (e.g., use VPNs, SOCKS proxies, or the TOR network) to hide their GeolIPs but they still need to be identified by unique nicknames and ICQ numbers, as that is how they can be distinguished from others. This allows them to stay anonymous but somewhat recognizable.

## Products

### Trojans

A Trojan [Трояны], short for a “Trojan horse,” is a piece of malware masquerading as a legitimate computer program or application.<sup>4</sup> Trojan spyware, a variant of such, are malware specifically designed to steal user data. Spyware steal information such as ICQ passwords, contact lists, confidential documents, bank account numbers, and so on. They can also come in the form of keyloggers that track victims’ keystrokes to obtain their online account credentials.<sup>5</sup> Note that forum and social networking account credentials are some of the most in-demand goods underground. This is most likely due to the fact that people reveal practically everything about themselves on social media. So, obtaining access to their social media accounts can mean getting access to their other accounts as well, especially if the victims use the same credentials across accounts.

Cybercriminals use stolen ICQ numbers to distribute spam or flood systems. Stolen File Transfer Protocol (FTP) account credentials, on the other hand, are sold and used for blackhat SEO purposes.<sup>6</sup>

### Exploits and Exploit Bundles

Exploits [Сплоиты], also known as “spoits,” are programs or, more often, scripts that exploit vulnerabilities in programs or applications.<sup>7</sup> The most prevalent exploits are browser exploits, which enable the download of malicious files. Exploits introduce code to a victim’s computer that then downloads and executes a malicious file.

An example of an exploit attack is causing an integer buffer overflow in the *setSlice( )* method in the *WebViewFolderIcon ActiveX®* component.<sup>8</sup> Using a specially constructed Web page 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 on 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.”

---

4 Trend Micro Incorporated. (2014). *Threat Encyclopedia*. “Trojan.” Last accessed February 6, 2014, <http://about-threats.trendmicro.com/us/malware/trojan>.

5 Trend Micro Incorporated. (2014). *Threat Encyclopedia*. “Keyloggers.” Last accessed February 6, 2014, <http://about-threats.trendmicro.com/us/glossary/k>.

6 Ryan Flores. (November 2010). “How Blackhat SEO Became Big.” Last accessed February 17, 2014, <http://www.trendmicro.co.uk/media/misc/blackhat-seo-became-big-research-paper-en.pdf>.

7 Trend Micro Incorporated. (2014). *Threat Encyclopedia*. “Exploit.” Last accessed February 6, 2014, <http://about-threats.trendmicro.com/us/glossary/e>.

8 MITRE Corporation. (2014). *CVE Details*. “Vulnerability Details : CVE-2006-3730.” Last accessed February 26, 2014, <http://www.cvedetails.com/cve/CVE-2006-3730/>.

An unintelligent exploit bundle simply downloads all of the exploits in a bundle at one time, regardless of which 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 another's. Unintelligent bundles are generally less expensive than intelligent ones though.

Intelligent bundles determine a victim's browser and operating system (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 evade 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 on which it was embedded. As such, if 1,000 users visit an exploit-laden page and the computers of 200 people are successfully infected with a Trojan, that exploit's reach is equal to  $(200 / 1,000) * 100$  or 20%.

Cross-site scripting (XSS) exploits are also available in the underground market. XSS vulnerability exploitation occurs when a usually malicious-site-embedded script 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.

After the execution of a malicious script in an XSS attack, the script begins to receive commands from a remote source to control an unknowing victim's browser while carrying out required actions. A script may be locally invoked on a system or reside in an inactive state on a compromised Web server until the affected machine makes calls to an infected Web page. The script then becomes active on the user's machine and begins to execute harmful activities.

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 induce 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 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 such as reading and deleting emails, conducting financial transactions, and writing social media posts.

XSS exploits can also be used to steal data from forms. They can conventionally be categorized as either “active” or “passive.” A passive XSS exploit requires a victim’s direct participation such as clicking a malicious link. This involves social engineering and trickery.

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

## 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.<sup>9</sup> 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 have significantly greater abilities. Note, however, that it is not always possible to move from Ring 3 to Ring 0.<sup>10</sup> This is the reason why there are two rootkit types—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.

## Traffic

Traffic [Траф] 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. Several traffic sources exist, including hacked websites, white-listed sites, and spam distributors.

In order to get traffic, a website can be hacked by inserting an iframe into one of its pages. An iframe, also known as an “inline frame,” is a “floating frame.” Because it is concealed, visitors to hacked sites are unknowingly and automatically led to hackers’ Web pages. As a result, hackers get a lot of traffic, which they can either sell or use for their own malicious purposes. Buying traffic allows cybercriminals to increase their sites’ SEO ranking. This allows the sites to end up as top search results, which can mean more visitors or potential victims.

---

9 Trend Micro Incorporated. (2014). *Threat Encyclopedia*. “Rootkits.” Last accessed February 6, 2014, <http://about-threats.trendmicro.com/us/glossary/r>.

10 Wikimedia Foundation, Inc. (February 14, 2014). *Wikipedia*. “Ring (Computer Security).” Last accessed February 17, 2014, [http://en.wikipedia.org/wiki/Ring\\_\(computer\\_security\)](http://en.wikipedia.org/wiki/Ring_(computer_security)).

Traffic can be topical in nature, depending on the type of website from which it originated. Business traffic is most valuable, however, because business site visitors generally have money. As such, their downloads are likely to be more profitable for hackers. Adult traffic (e.g., traffic from porn sites) is also worth mentioning even if it is 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 because it 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 TDS.<sup>11</sup> Cybercriminals use TDSs to determine traffic type, which will aid them in directing users to certain malicious sites and serving the right malicious payloads for particular systems.

## Crypters

File encryption is primarily employed to conceal infected files or malware from security software. To hide a malicious file or a piece of malware from security software, cybercriminals use various crypting tools and techniques. The more effective the encryption technique, the more expensive it is. One of the most important components of a crypter is the so-called "crypter stub," a piece of code used to decrypt an encrypted piece of malicious code.

Crypters can be classified as either "static" or "polymorphic." A static crypter stub is sold as 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 it from memory. This encryption method, however, is not effective. Static 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."

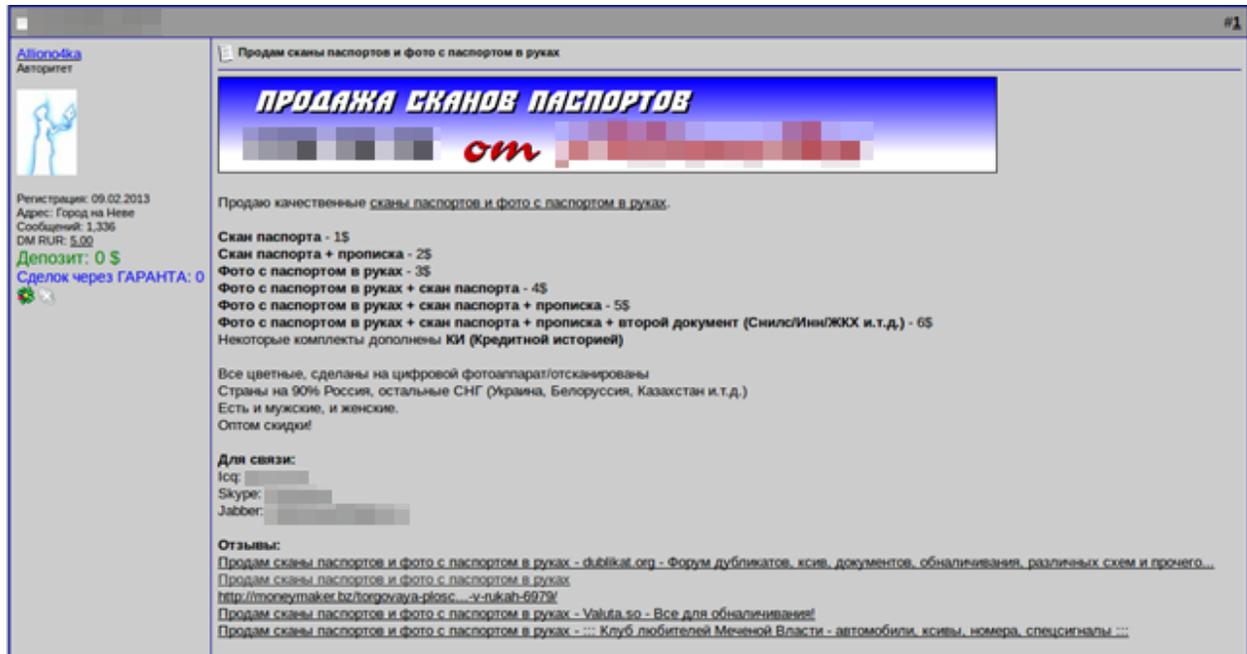
Polymorphic crypters are considered more advanced. They use state-of-the-art algorithms that utilize random variables, data, keys, decoders, and so on. As such, one input source file never produces an output file that is identical to the output of another source file. This can be achieved by using several algorithms, including shuffling blocks of code while preserving a malicious file's ability to run and creating macros.

---

<sup>11</sup> Max Goncharov. (2011). "Traffic Direction Systems as Malware Distribution Tools." Last accessed February 6, 2014, [http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt\\_malware-distribution-tools.pdf](http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_malware-distribution-tools.pdf).

## Fake Documents

Providers of fake passports and other documents can also be found in the Russian underground market.

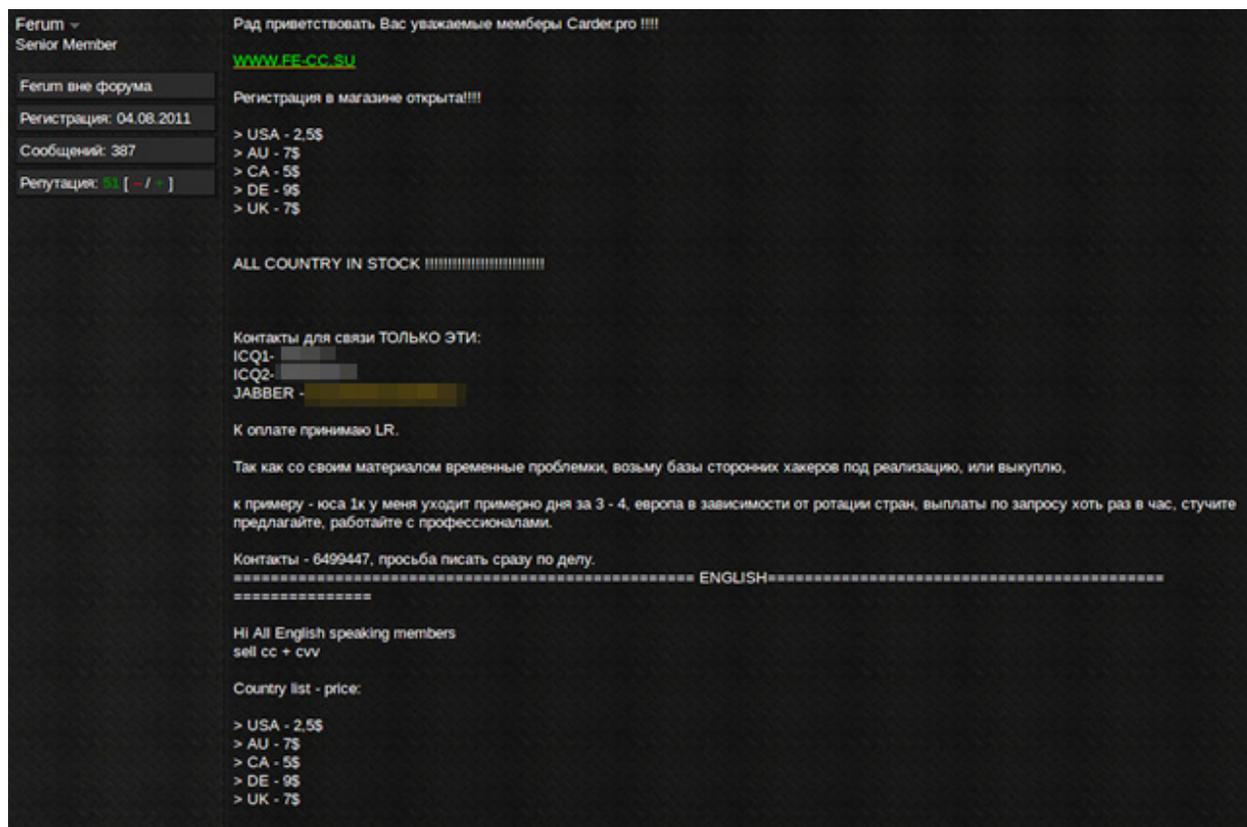


Scanned passport - \$1  
Scanned passport with registered postal address - \$2  
Picture of a person holding a passport - \$3  
Picture of a person holding a passport and scanned copy of the passport - \$4  
Picture of a person holding a passport with registered postal address - \$5  
Picture of a person holding a passport with registered postal address and tax ID document - \$6  
All document copies and pictures (taken with a digital camera) are in full color. Countries: 90%, Russia; 10%, CIS countries. We have documents for both males and females. Wholesale discounts!

Figure 1: Site that sells fake Russian and Commonwealth of Independent States (CIS) member-country passports

## Stolen Credit Card and Other Credentials

Stolen credit card and other credentials are also sold in the market.



**Figure 2:** Site selling stolen credit card credentials but only to registered members; it even has member testimonials

## Services

### Dedicated-Server-Hosting Services

A dedicated server [Дедики] is one that a user rents but does not share with others. It can be used for various malicious activities, ranging from brute forcing to carding; in most cases, however, it is used as a C&C server, a C&C proxy interface, or a drop zone for malicious files that infected machines upload.<sup>12</sup> Hackers typically access dedicated servers via a VPN, which provides anonymity with the aid of data transfer encryption. Dedicated-server-hosting services rank among the most in-demand underground market offerings. Dedicated servers are usually rented out at varying prices, depending on which country they are in, how fast they are, what their hardware specifications are, and whether or not they are bulletproof.

<sup>12</sup> U.S. Department of Justice. (June 26, 2012). *The FBI: Federal Bureau of Investigation*. "International Cyber Crime Takedown Targets 'Carding.'" Last accessed February 17, 2014, [http://www.fbi.gov/news/news\\_blog/international-cyber-crime-takedown-targets-carding](http://www.fbi.gov/news/news_blog/international-cyber-crime-takedown-targets-carding).

## Proxy-Server-Hosting Services

A proxy server [Прокся] is an intermediate computer that serves as a “proxy” or a mediator between a computer and the Internet. Proxy servers are used for various purposes such as accelerating data transmission and filtering traffic but their main purpose, which makes them popular among hackers, is to ensure anonymity. Anonymity, in this case, is achieved because the destination server sees the Internet Protocol (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 proxy server types include HTTP/S; SOCKS; and Common Gateway Interface Proxy (CGIProxy), also known as an “anonymizer.”<sup>13</sup>

## 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 software) to ensure 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, not using a VPN means doing everything online with the aid of a chosen Internet service provider (ISP), including opening websites and performing other tasks. Using a VPN—an intermediary—allows hackers to encrypt all requests issued to and incoming data coming 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 their 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.

## Pay-per-Install Services

In the PPI service [Залив с отступом] business model, advertisers pay publishers a commission every time a user installs usually free applications bundled with adware.<sup>14</sup> In a PPI attack, an “installation” 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’s computer is infected when he visits an exploit-hosting site using a vulnerable browser that downloads and runs a malicious script. This is one of the most popular methods to distribute malware (i.e., most often Trojans).

---

13 Wikimedia Foundation, Inc. (February 12, 2014). *Wikipedia*. “Proxy Server.” Last accessed February 17, 2014, [http://en.wikipedia.org/wiki/Proxy\\_server](http://en.wikipedia.org/wiki/Proxy_server).

14 Kyle Wilhoit. (February 19, 2013). *TrendLabs Security Intelligence Blog*. “Business Models Behind Information Theft.” Last accessed February 17, 2014, <http://blog.trendmicro.com/trendlabs-security-intelligence/business-models-behind-information-theft/>.

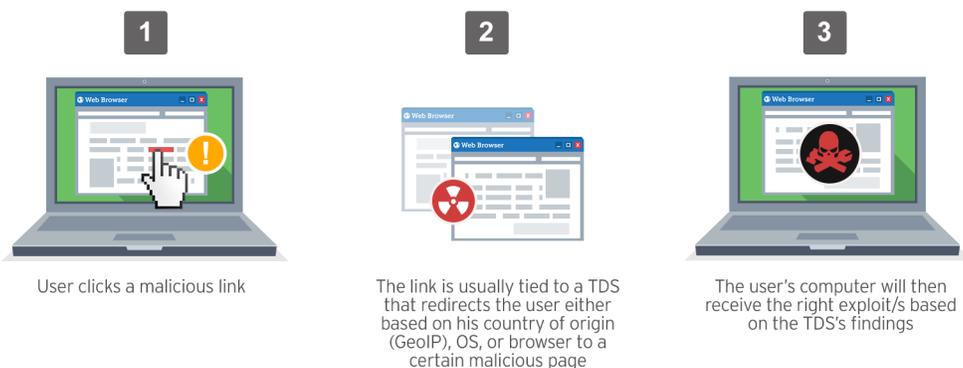
Offering download services is a widespread practice. In the PPI business model, a customer provides the malicious file for a service provider to distribute. Download services are usually offered based on the target country.

In other words, the PII rating of a country is determined by the likelihood that a malicious file will be downloaded and opened by a resident person or company. This 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 activity types take place in the download services market—either a customer can give a download service provider a malicious file for distribution or a download service provider offers services to interested parties. Partner programs for both download- and traffic-related services also exist.<sup>15</sup>

Traffic converters convert traffic into downloads. Downloads, meanwhile, are sold per 1,000 installations. Download packages usually have 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] or scripts that permit the execution of a desired action through a vulnerability in some program (e.g., a browser) or exploit bundles or 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.



**Figure 3:** How TDSs work

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 and obtain downloads. The “ingredients” for getting downloads (i.e., traffic, exploits, and bulletproof hosts) are separately sold.

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

<sup>15</sup> Paul Ferguson. (October 27, 2009). *TrendLabs Security Intelligence Blog*. “What the Experts Still Don't Know”—The Thriving Cybercrime Underground.” Last accessed February 17, 2014, <http://blog.trendmicro.com/trendlabs-security-intelligence/what-the-experts-still-dont-know-the-thriving-cyber-crime-underground/>.

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 comes from the United States and Australia. Since most of the U.S. traffic, however, is porn-related, Australian traffic is considered of higher quality and more frequently used for carding activities.

## Denial-of-Service Attack Services

Denial-of-service (DoS) [ДДoC] and DDoS attacks are hacking attack types on computers. These attacks create conditions in which legitimate computer users are denied access to their own systems' resources. Hackers who instigate these are not trying to illegally break in to protected computers to steal or destroy data; they just want to paralyze websites or computers.

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 send fake requests may not even suspect that their machines have been hacked. DDoS software were initially created for nonmalicious purposes such as to study the throughput capacity of networks and their tolerance to external loads. In such a case, using an improperly structured Internet Control Message Protocol (ICMP) packet is most effective because it 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.

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 on 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 such as taking down a particular website.

## Spamming Services

Spamming [Спам] refers to the mass distribution of emails. Spam can be themed or unthemed. Themed spam are meant to target a specific audience type (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 no particular order. They do not have specific targets. What is most important for this kind of spam is that they are sent to as many users as possible.

Spam can also be categorized in terms of distribution medium—email, instant-messaging (IM), social network, or Short Message Service (SMS) spam. Each medium requires its own set of recipients and distribution resources.

The spamming services market is quite diverse. Databases and forum and social networking accounts are most in demand. These are filtered by interest, age, social status, and so on, allowing spammers to obtain more information on the people in the databases so they would not have to resort to so-called “blind spam sending.” They can more easily identify the right targets for each spam run or campaign. Databases are usually sold in bulk, depending on the target audience (e.g., date or job seekers).

Email account credentials, which are required for spam distribution, are also available in the market. Spam distribution tools and/or programs for instant- and text-message spamming can likewise be bought. Tools to spam forums and social networks, however, are less commonly seen. Their prices depend on features, distribution speed, and so on.

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

## Flooding Services

Flooding is a simple routing technique in computer networks where a source or node sends packets through every outgoing link. It is used for DoS attacks to bring down a network service. The service is flooded with many incomplete server connection requests. Due to the flood of requests, the server or host is not able to process genuine requests at the same time. A flooding attack fills the server or host memory buffer; once full, further connections cannot be made, which results in DoS. 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.

## Malware Checking Against Security Software Services

Malware-checking services allow cybercriminals to anonymously see if their malicious files are being detected by popular security products. They do not use free or publicly available services such as VirusTotal or VirSCAN because these are affiliated with security vendors. Trend Micro, for instance, gets sample sets from anti-malware-checking service providers, which are then processed to create new patterns in order to protect our customers.

One of the popular underground anti-malware-checking service providers, Scan4You.net, in fact, even boasts on its About Us page that, “You can be fully sure that your files will not be sent to antivirus databases. All reporting systems in our version of antivirus engines were disabled.”

## Social-Engineering and Account-Hacking Services

Hacking refers to unauthorized access to information by any means other than through use of software. Cybercriminals often social engineer or outsmart users to get their passwords or other confidential information in order to breach their computers. Classic examples of social-engineering tactics include making telephone calls to a company to ascertain who has the necessary information then calling its administrator using the identity of an employee with an urgent system access problem.

In its pure form, social-engineering services do not attract much demand. As such, though these are offered underground, they are quite rare. Social engineering primarily allows fraudsters to hack victims' email or social media accounts. It also effectively lures people to visit exploit-laden and phishing pages.

Three types of hacking services, meanwhile, are offered in the Russian cybercriminal underground market.

### Account-Hacking Services

Account hacking [Взлом акков] is a very popular skill among cybercriminals. The demand for such a service is also enormous, so advertisements for it abound in underground markets. The most common hacking targets are email and social media accounts. Site- and forum-account-hacking services are less commonly seen. In fact, concrete orders are usually handled separately in private conversations.

### Brute-Forcing Services

Brute forcing [Брут] is one of the oldest methods cybercriminals use to 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 to carry out because the required password may not be in a program's dictionary. Besides, trying every password can take a considerable amount of time. The continuous growth of computing power, however, is allowing brute forcing to once again gain relevance. The faster a computer is, after all, the more passwords it can try to hack a victim's system. Some cybercriminals even offer services to decrypt hashes.

### Account Hacking via Social Engineering Services

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.

## Cybercriminal Wares Sold in the Russian Underground Market

The following tables show the various products and services sold in the Russian underground market.

Russian Cybercriminal Underground Market Product Offerings			
Product	2011 Price	2012 Price	2013 Price
Trojan: <ul style="list-style-type: none"> <li>• Phoenix</li> <li>• Adrenalin</li> <li>• Limbo</li> <li>• ZeuS (detected by Trend Micro as “ZBOT”)</li> <li>• SpyEye</li> </ul>	US\$500 US\$790 US\$350  US\$120 US\$500	US\$150 No data No data  US\$0 US\$0	US\$0–35 No data No data  US\$0 US\$0
Exploit kit: <ul style="list-style-type: none"> <li>• Eleonore Browser Exploit Kit</li> <li>• Phoenix Exploit Kit</li> <li>• eCore Exploit Pack</li> </ul>	US\$700 US\$600 US\$1,000	No data US\$250 No data	No data US\$0 No data
Traffic: <ul style="list-style-type: none"> <li>• PPI/1,000 installations USA</li> <li>• PPI/1,000 installations Europe</li> <li>• PPI/1,000 installations Asia</li> </ul>	US\$190–400  US\$240–340  US\$220–400	US\$120–340  US\$100–400  US\$120–190	US\$50–130  US\$40–170  US\$90–200
Crypter: <ul style="list-style-type: none"> <li>• Basic static</li> <li>• Static with stub and add-ons</li> <li>• Polymorphic</li> </ul>	US\$10–30  US\$30–80 US\$100	US\$4–10  US\$15–25 US\$80	No data  US\$10–30 US\$65
Proxy server host list per 300 IP addresses	US\$3	US\$4	US\$6
Scanned fake document: <ul style="list-style-type: none"> <li>• European passport</li> <li>• Russian and other CIS passports</li> </ul>	US\$2.50  US\$2–5	US\$1  US\$1–5	US\$1  US\$1–2

Russian Cybercriminal Underground Market Product Offerings			
Product	2011 Price	2012 Price	2013 Price
Credit card credentials (per card):			
• American	US\$2.50	US\$1	US\$1
• Australian	US\$7	US\$5	US\$4
• Canadian	US\$5	US\$5	US\$4
• German	US\$9	US\$7	US\$6
• British	US\$7	US\$6–8	US\$5

\* Proxy server host lists became more expensive over time because proxy-hosting services were supplied less than VPN-hosting services.

Russian Cybercriminal Underground Service Offerings			
Service	2011 Price	2012 Price	2013 Price
Dedicated-/Bulletproof-server hosting			
• Low-end	US\$160	US\$100	US\$50
• High-end	US\$450	US\$160	US\$190
• Virtual private server (VPS)	US\$70	US\$40	US\$12+
Proxy-server hosting (per day):			
• HTTP/S	US\$2	US\$1	US\$1
• SOCKS	US\$2	US\$2	US\$2
VPN-server hosting:			
• With one exit point	US\$8–12	No data	No data
• With an unlimited number of exit points and traffic	US\$40	US\$38	US\$24
• Average price	US\$22	US\$20	US\$15
Traffic-to-download conversion (PPI per 1,000 installations):			
• Australia traffic	US\$300–500	US\$200–500	US\$120–600
• U.K. traffic	US\$220–300	No data	US\$150–400
• U.S. traffic	US\$100–150	US\$100–250	US\$120–200
• Europe traffic	US\$90–250	US\$75–90	US\$50–110
• Mixed global traffic	US\$12–15	US\$10–17	US\$10–12
• Russia traffic	US\$100–500	US\$100–190	US\$140–400

Russian Cybercriminal Underground Service Offerings			
Service	2011 Price	2012 Price	2013 Price
DDoS attack: <ul style="list-style-type: none"> <li>• Lasts 1 hour</li> <li>• Lasts 24 hours</li> </ul>	US\$4–10 US\$30–70	US\$2–25 US\$15–60	US\$2–60 US\$13–200
Spamming (per 10,000 messages): <ul style="list-style-type: none"> <li>• Generic (uses a public database)</li> <li>• External-email-database-based</li> <li>• SMS</li> <li>• ICQ</li> <li>• Skype</li> </ul>	US\$13  US\$17 US\$600 US\$55 No data	US\$8  US\$14 US\$300 US\$15 US\$110	US\$4–5  US\$13 US\$100 US\$4–9 US\$86
Flooding: <ul style="list-style-type: none"> <li>• Email (per 10,000 messages)</li> <li>• Landline phone</li> <li>• SMS (per 1,000 text messages)</li> </ul>	US\$30 US\$32  US\$15	US\$3 US\$23  US\$10	US\$2 US\$25  US\$8
Malware checking against security software: <ul style="list-style-type: none"> <li>• Daily checking</li> <li>• Automatic reuploading in case a piece of malware is being detected by known anti-malware solutions</li> <li>• Checking against malicious URL blacklists</li> </ul>	US\$50  US\$50  US\$50	US\$30  US\$30  US\$30	US\$30  US\$30  US\$30
Hacking: <ul style="list-style-type: none"> <li>• Facebook account</li> <li>• VK account</li> <li>• Odnoklassniki account</li> <li>• Twitter account</li> <li>• Gmail account</li> <li>• Mail.ru account</li> <li>• Yandex.ru account</li> <li>• Hotmail account</li> </ul>	US\$200 US\$120–140  US\$94 US\$167 US\$117 US\$74 US\$74 US\$107	US\$160 US\$100  US\$90 US\$40 US\$120 US\$70 US\$70 US\$100	US\$100 US\$76  US\$94 No data US\$100 US\$50 US\$50 US\$100
Fake document rework	US\$15–20	US\$10–20	US\$5–28

## Conclusion

As the Russian underground community continuously shifts targets and gains access to better and leading-edge technologies, security companies must also continuously provide better and more effective solutions to help customers protect their money, assets and other valuable information resting in their computers and other devices.

As seen in this paper, the cybercriminal underground economy is much like any other type of business economy. It experiences pricing highs and lows, depending on demand and supply. Unlike legitimate businesspeople, however, cybercriminals need to keep their identities secret and, as much as possible, hide all traces of their “business” transactions.

Even though the prices of most products and services sold in the Russian underground market have been decreasing, that does not mean that business is not doing well for cybercriminals. It can even mean that the market is growing, as we see more and more product and service offerings as time passes. Cybercriminals, like legitimate businesspeople, are also automating processes, resulting in lower product and service prices. Of course, “boutique” products and services remain expensive because these involve specialized knowledge and skills to develop that only a few bad guys have.

This paper covered only the most basic and fundamental tools and technologies cybercriminals create and use to enhance their business. It also provides 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. We all need to keep in mind that as long as profit can be made, cybercriminals will continue to offer products and services that can make life easier for themselves and their peers. And as long as customers exist, the cybercriminal underground will thrive. As users and potential victims, we all need to keep an eye out for the latest misdeeds to stay safe from all kinds of digital threats.

## Appendix

### List of Cybercriminal Underground Wares Trend Micro Tracks and Monitors

#### Products

- Databases
- Exploits
- Fakes (e.g., currencies, etc.)
- FTP account credentials
- Online gaming account credentials
- Ransomware
- Remote access Trojans (RATs)

- Rootkits
- Scanned documents
- Serial numbers
- Traffic
- Trojans
- Web shells

### Services

- Abuse services
- Account-hacking services
- Blackhat SEO services
- C&C-server-activity-related services
- Carding services
- Crypting services
- DDoS services
- Dedicated-server-hosting services
- Electronic-payment-related services
- Laundering services
- Malware checking against security software services
- Money-laundering- and mule-related services
- Obfuscation services
- PPI services
- Programming services
- SMS-fraud-related services
- Social-engineering services
- SOCKS-proxy-server-hosting services
- Spamming services

- VPN services

#### Russian Underground Glossary

- **Account:** Акки [aki]
- **Botnet:** Ботнет [botnet]
- **Brute forcing:** Брут [brootforce or brutforce]
- **Cryptor:** Криптор [kriptor]
- **Dedicated server:** Дедики [Dediki]
- **DoS:** ДДoC [DDoS]
- **Exploit:** Сплоиты [sploiti]
- **Fraud:** Фрод [fraud] (i.e., any fraud kind: email, SMS, banking, etc.)
- **Joiner:** Склейка [skleyka]
- **Password brute forcing:** Подбор Паролей [podbor paroley]
- **PPI:** Залив [zaliv] or Пробив [probiv]
- **Proxy server:** Прокся [proksya]
- **Rootkit:** Руткиты [rootkit]
- **SOCKS 5:** Соксы [SOCKS 5]
- **Spam:** Спам [spam]
- **Traffic:** Траф [traf]
- **Trojan:** Трояны [Trojan]
- **Web inject:** Инжекты [inzhekti]

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit [www.trendmicro.com](http://www.trendmicro.com).

©2014 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.



Securing Your Journey  
to the Cloud

225 E. John Carpenter Freeway, Suite 1500  
Irving, Texas 75062 U.S.A.

Phone: +1.817.569,8900