Russian Underground 2.0

Max Goncharov
Forward-Looking Threat Research (FTR) Team

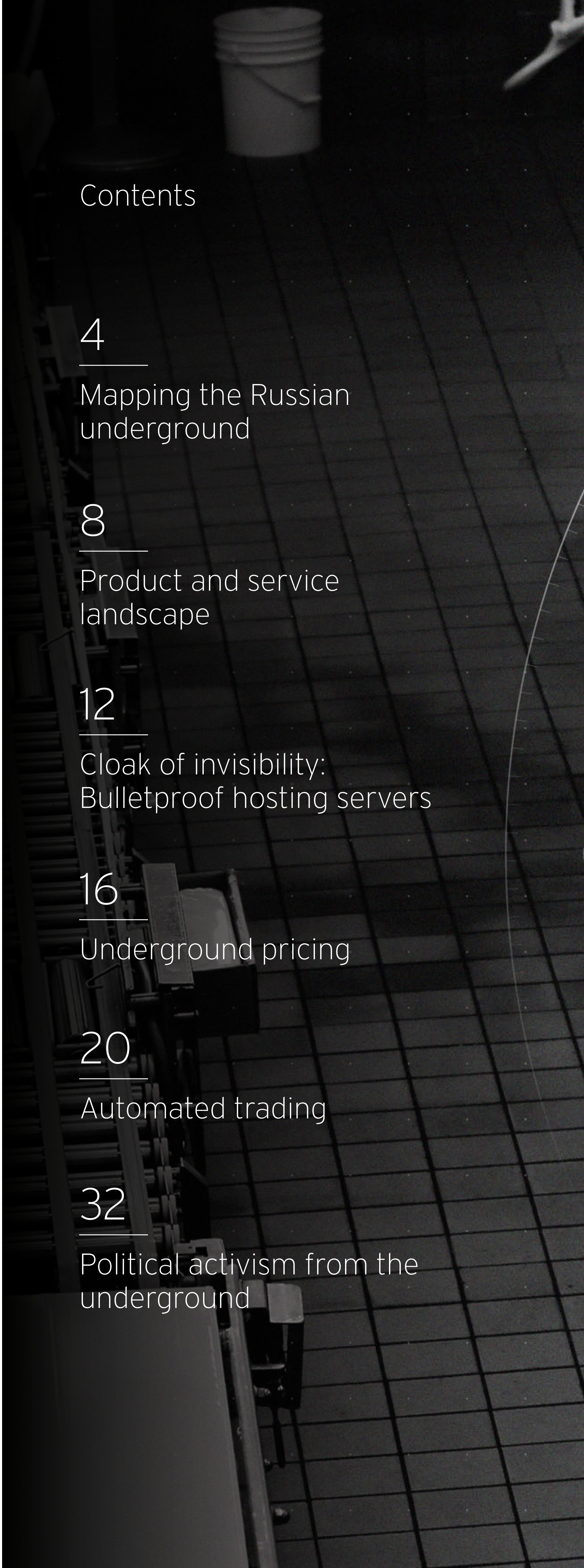
A TrendLabs℠ Research Paper

TREND MICRO LEGAL DISCLAIMER

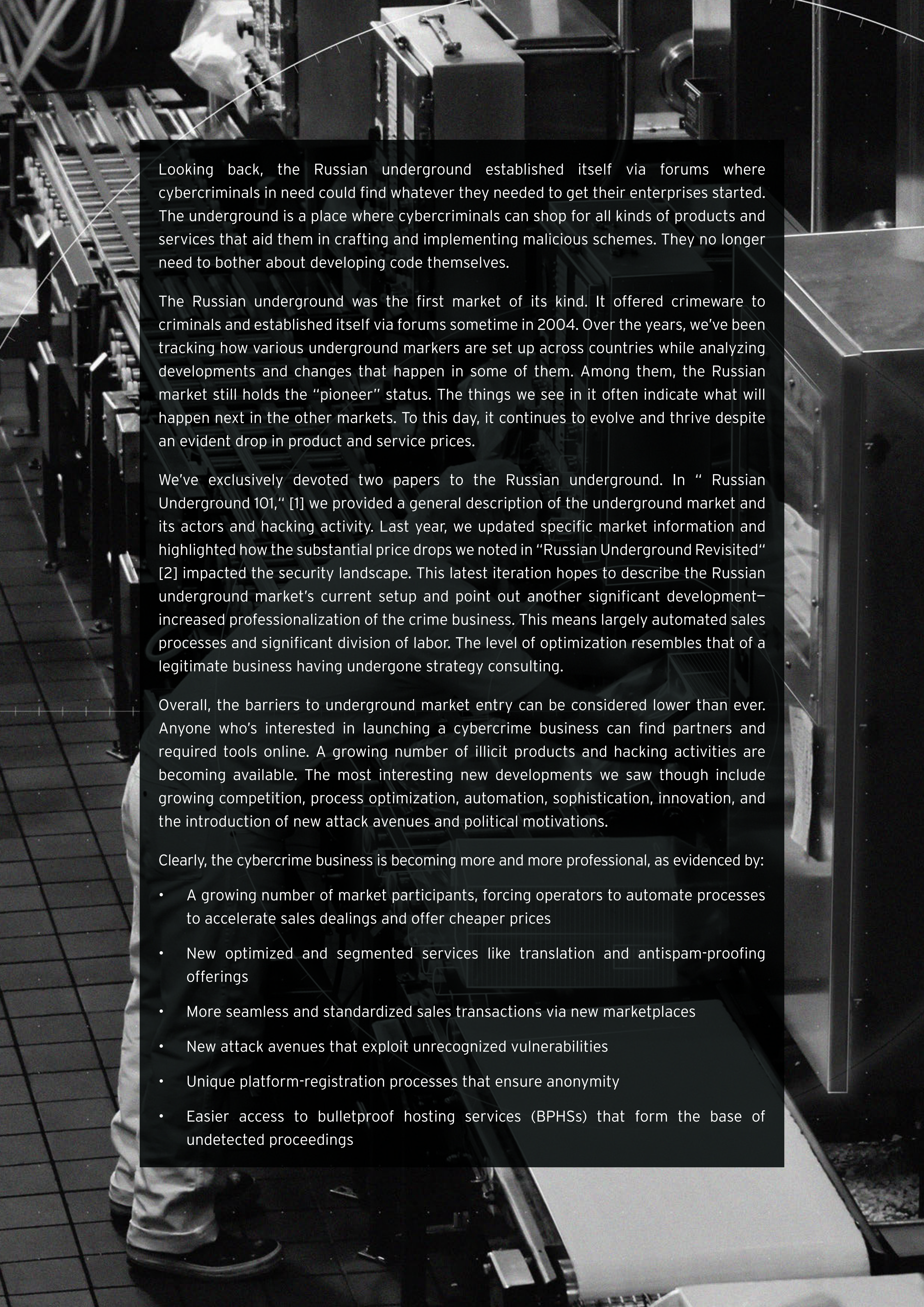
The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained 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.



Contents



Looking back, the Russian underground established itself via forums where cybercriminals in need could find whatever they needed to get their enterprises started. The underground is a place where cybercriminals can shop for all kinds of products and services that aid them in crafting and implementing malicious schemes. They no longer need to bother about developing code themselves.

The Russian underground was the first market of its kind. It offered crimeware to criminals and established itself via forums sometime in 2004. Over the years, we’ve been tracking how various underground markers are set up across countries while analyzing developments and changes that happen in some of them. Among them, the Russian market still holds the “pioneer” status. The things we see in it often indicate what will happen next in the other markets. To this day, it continues to evolve and thrive despite an evident drop in product and service prices.

We’ve exclusively devoted two papers to the Russian underground. In “ Russian Underground 101,“ [1] we provided a general description of the underground market and its actors and hacking activity. Last year, we updated specific market information and highlighted how the substantial price drops we noted in “Russian Underground Revisited“ [2] impacted the security landscape. This latest iteration hopes to describe the Russian underground market’s current setup and point out another significant development—increased professionalization of the crime business. This means largely automated sales processes and significant division of labor. The level of optimization resembles that of a legitimate business having undergone strategy consulting.

Overall, the barriers to underground market entry can be considered lower than ever. Anyone who’s interested in launching a cybercrime business can find partners and required tools online. A growing number of illicit products and hacking activities are becoming available. The most interesting new developments we saw though include growing competition, process optimization, automation, sophistication, innovation, and the introduction of new attack avenues and political motivations.

Clearly, the cybercrime business is becoming more and more professional, as evidenced by:

- A growing number of market participants, forcing operators to automate processes to accelerate sales dealings and offer cheaper prices
- New optimized and segmented services like translation and antispam-proofing offerings
- More seamless and standardized sales transactions via new marketplaces
- New attack avenues that exploit unrecognized vulnerabilities
- Unique platform-registration processes that ensure anonymity
- Easier access to bulletproof hosting services (BPHSs) that form the base of undetected proceedings

SECTION I

Mapping the Russian underground

Mapping the Russian underground

Data gathering and analysis

To gain a deeper insight into new developments in the underground community, we use certain tools and techniques to gather and analyze raw market data. Our current data-collection and -normalization process has been automated to a large extent. Language barriers and nuances brought about by the use of underground slang, however, still require careful manual analysis. Take the term "credit card," for example. In Russian, this is "кредитная карта." But cybercriminals use the term "картон" instead, which in English means "carton." The same issue applies to other terms like "Paypal," which translates to "palka" (палка) in slang, meaning "stick," and "bulletproof server" or "abuse free" (арбуз) in slang, meaning "watermelon."

We then group the information we collected into specific categories, usually by activity type like "traffic resale," "rootkit creation," or "distributed denial-of-service (DDoS) service provision." This categorization allowed us to aggregate activities and identify which were very common or popular at a given point in time as well as how trends shift and change (see the Appendix for more details).

This year, we added four categories to our existing 38—two for new attack avenues, one for an attack avenue that we believe we'll see more of in the near future, and one for interesting use of resources. These are described in more detail below.

- **Malicious code upload:** Using Web traffic (user clicks on certain sites), malware infect users' computers. In very simple terms, users access a site like *verypopularwebsite.omg* that a criminal has compromised and injected a malicious piece of code (invisible iframe) into. This iframe causes users to open another site—the criminal's—within the site they vistited (in this case, *verypopularwebsite.omg*). The site's content usually stays the same. Users can't see any of these movements but clicking the iframe opens a completely different domain. This domain usually executes a malicious JavaScript (an exploit kit) that checks if the users' browser is vulnerable then uploads the right exploit for the hole found, thus infecting their computers. This technique succeeds most in the case of new vulnerabilities (zero days) or as a result of missing updates. It's already well-known as well, but what we found novel is that this entire procedure is available for hire. Today, as a customer, users need not worry about the details of the mobile-code-uploading process—this procedure is taken care of by providers in the form of "malicious-code-installation-as-a-service" that can be bought at their convenience in underground forums.

- **Mobile traffic:** The global mobile data traffic volume grew 69% in 2014. In our 2014 predictions [3], we also stated that mobile devices will become the attack vector of choice, bringing in nastier threats and attacks. What drove this growth was a shift in device mix toward smart devices. As mobile traffic exponentially rises in the coming years, it will be increasingly used as a pathway for malware and exploits similar to Web traffic from computers. Criminals can filter traffic, depending on what kind of device they would like to infect. Targeting mobile devices is shaping up to become a big trend for fraud as well as malware distribution.

- **Router exploitation:** Home routers nowadays are no longer simply dummy boxes that can only emulate Point-to-Point Protocol over Ethernet (PPPOE), they now come with extended functionality, which can include proxying traffic, storing data, and rerouting Domain Name System (DNS) traffic, among others[1]. Today's home routers are practically small computers that allow for universal serial bus (USB) storage that run on any of the *nix operating systems (OSs) (Unix, Linux, and Android), which we think can theoretically be converted into infected boxes. For criminals, infecting home routers can prove more effective than infecting regular computers because routers are mostly kept online 24 x 7 unlike standard home computers. Routers are hardly ever checked and updated by their owners as well. We're already seeing growth in the stolen server access credentials and infected home routers market, which is a good indicator of what will trend in the underground market in the coming years.

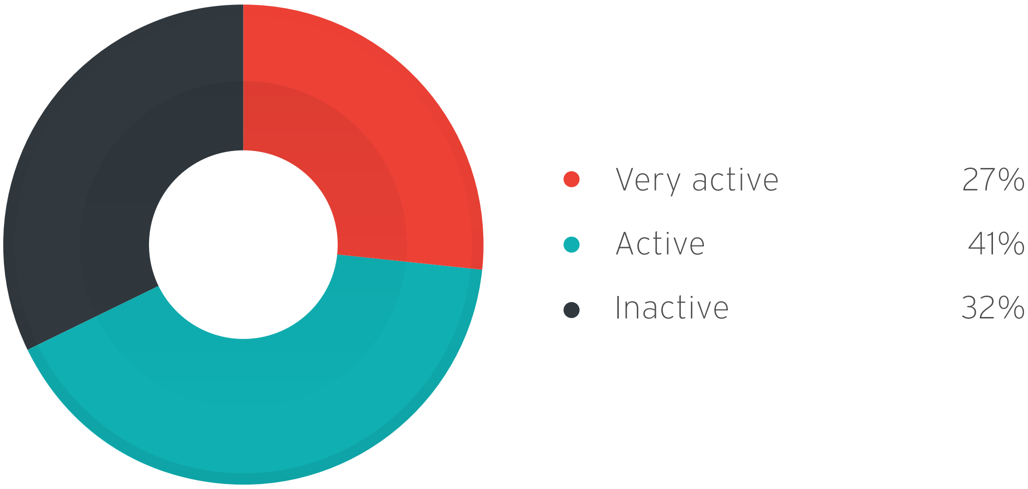
- **Hacktivism:** Between 2014 and 2015, we came across a number of groups that operate in the cyber-realm not for entrepreneurial purposes but in pursuit of political causes. Hacktivism used to be a means for the hacking community, with more or less liberal political ideas, to gain attention in cyberspace. We are increasingly observing hackers' partisanship with official authorities like nation states or separatist groups in real political conflicts. Through their actions in cyberspace, they try to participate in such conflicts. This doesn't, however, mean actual affiliation or state sponsorship. Many of these groups are self-proclaimed "cyberwarriors" or "cyber armies," and through a stated connection to a state, cause, or oppressed populace, try to gain legitimacy in the eyes of their supporters. It is difficult to tell who actually funds them.

Russian underground activities

Cybercrime has evolved in complexity and organizational capacity. Estimating the precise scale of the underground business is tricky. Statistics on underground economies are inherently speculative—the underground doesn't make annual disclosures or let auditors go over their books, which basically leaves us with back-of-the-envelope explorations.

[1] *Some models of advanced routers now even allow users to save fax messages received and answer calls.*

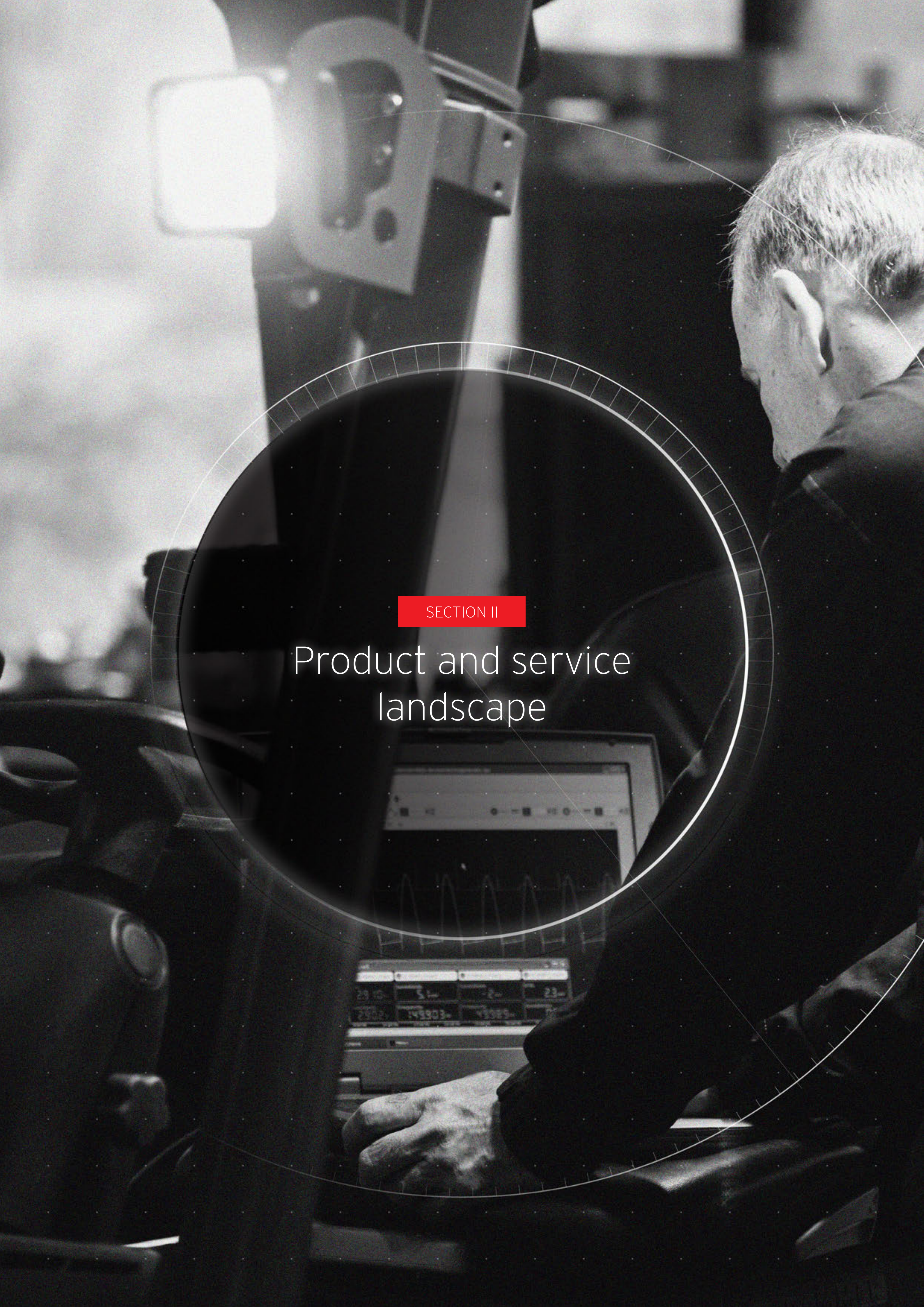
How then do we measure the extent of the Russian underground community? We base our estimates not only on the number of forums in it or how many threads per day each community member generates, but also on the volume of activities and cybertraffic that we see. The number of Russian underground forums grows every year. Even though some forums shut down, the more popular ones often just change their domain names every once in a while. At this moment, we consider 78 websites (underground forums) active, with varying degrees of activity.



Number of underground forums with varying levels of activity seen

We also track marketplaces and forum boards that don't necessarily focus on cybercriminal activities yet still have traces of cybercriminal posts. We track down individuals by the nicknames they use though this isn't very reliable, as some members of the cybercriminal community regularly change their nicknames to stay anonymous or avoid being identified due to having bad reputations. The popular forums we've seen can have 20,000 to several hundreds of unique members.

The underground market isn't very articulate about the ends toward which products sold should be used, but sometimes, users find a disclaimer stating that Russia shouldn't be a target of any malicious activity. The Russian underground is more conducive to blackhat activities targeting other countries (not part of the former Soviet Union).



SECTION II

Product and service landscape

Product and service landscape

Underground goods

The underground market is a place where criminals no longer have to worry about creating malware on their own. It has become one where they can shop for malicious tools to their hearts' content. The products and services offered in the underground pretty much stay the same with every passing year. The business model is pretty firm in terms of sales. The Russian market, for instance, specializes in selling traffic direction systems (TDSs) and offering traffic direction and pay-per-install (PPI) services. Traffic-related products and services are becoming the cornerstone of the entire Russian malware industry because 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.

While the products sold stay the same, we do see increasing changes within each category:

- In the carding business, we observe automation in the process of checking cards, seeing their balance, or checking their validity. Everything can be done with one click.
- Money-laundering schemes are now being offered as well. Criminals offer peers the option to launder money in various ways (buying flight tickets, booking hotels, or renting expensive villas).

Other cybercriminals can avail of services and lessen the effort required in earlier days. Back then, criminals had to steal card information, engage droppers' services to convert stolen credit cards into cash (buy a gadget with the card, send it to a dropper's address so the dropper can sell the gadget and keep 30% or more of the "revenue" as payment). Today, this process has evolved from using goods to buy tickets or pay for hotel stays. For example, criminal A buys a flight ticket with a stolen credit card for criminal B or a regular person in need of such good. The original ticket normally costs US$600, but because criminal A bought it with a stolen card, he only charges criminal B or the regular person US$300, thereby still keeping a 50% profit. In effect, criminal A not only saves time but also effort in laundering money.

New and optimized services

Automated shell script uploading

Challenges surrounding big data were tackled by the cybercommunity in a very efficient way. A good example of this is by providing automated shell-script-uploading and -selling services. Cybercriminals try to find and exploit vulnerable machines (Web servers) then scan these for known file names (*pleasehackme.php* on Wordpress, for example) so they can upload suitable shell codes or iframes that deliver the right exploits. Users who have access to log files on Web servers can see permanent attempts to open files that actually don't exist on the servers. This is a new development that we expect to see a lot more of in the near future.

Professional underground translation

For targeted email spamming and typing support, writing skills are required. If threat actors need to prepare for targeted attacks against selected individuals using emails as delivery vector, they need to know the individuals' background and use correctly written, credible-sounding emails. Underground forums keep special groups who can compose targeted attack emails on hand.

Fake identity-approval-call-receiving services

When cybercriminals launder money, they need to be fluent in the language of the country they are cheating in. Often, when money transfers or transactions don't conform to certain security templates, banks or online payment service providers make "proof-of-identity" calls to ensure that the purchasers are the real credit card or Paypal account owners. In such a case, it can come in handy for cybercriminals if they can approach service providers that can help them back up transactions.

Drop-as-a-service (Разводные незавидные) offerings

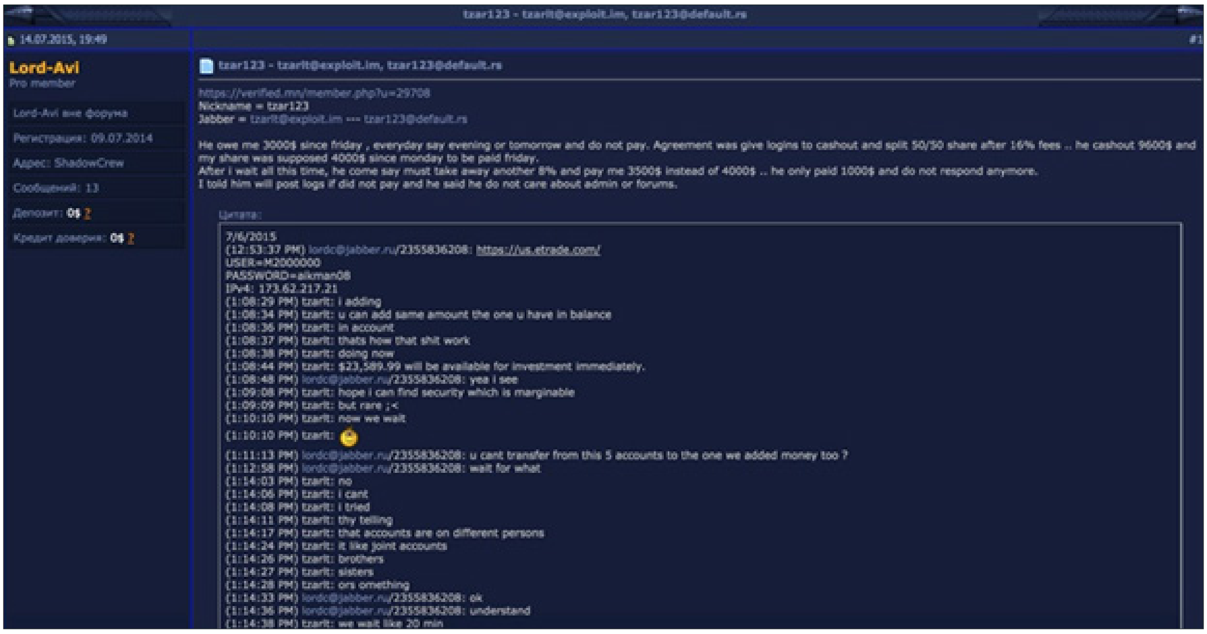
Cybercriminals who are in charge of cashing stolen credit cards and online payment system accounts are called "droppers." There are two types of droppers—those who aren't aware that they are "dropping" (*razvodnie*) and those that know exactly what they're doing (*nerazvodnie*). There's a huge market for dropping services and those who control them (drop controllers or *dropovod*) in the underground community. Drop controllers can control 10–1,000 droppers via so-called drop-as-a-service offerings (as rental).

Logs for sale

Within a botnet, users who have full access to big servers can also get access to log files and so extract information like passwords. Given that, they can find credit card information and even buy and/or sell log files (sometimes, even parse log files if they can). We've seen a trend where cybercriminals agree to process big data in order to extract interesting information. They usually buy logs 1GB (unpacked) in size or more at prices determined on a case-to-case basis. They also offer services to process logs on a regular basis (bundled packages) for a fixed price.

Corporate accounts for money laundering

Cybercriminals who need to launder their earnings can do so using corporate accounts (bank accounts owned by corporations). Such a service costs around 50% of the sum being laundered. The corporate accounts used for these mostly come from the United States (US), Germany, and the United Kingdom (UK), among others (destinations users would normally want to park laundered money in). Services of this sort cost US$50,000 or €50,000 or more.



Lord-Avi
Pro member
Lord-Avi вне форума
Регистрация: 09.07.2014
Адрес: ShadowCrew
Сообщений: 13
Депозит: 0$?
Кредит доверия: 0$?

tzar123 - tzarit@exploit.im, tzar123@default.rs

https://verified.mn/member.php?u=29708
Nickname = tzar123
Jabber = tzarit@exploit.im --- tzar123@default.rs

He owe me 3000$ since friday , everyday say evening or tomorrow and do not pay. Agreement was give logins to cashout and split 50/50 share after 16% fees .. he cashout 9600$ and my share was supposed 4000$ since monday to be paid friday.
After i wait all this time, he come say must take away another 8% and pay me 3500$ instead of 4000$ .. he only paid 1000$ and do not respond anymore.
I told him will post logs if did not pay and he said he do not care about admin or forums.

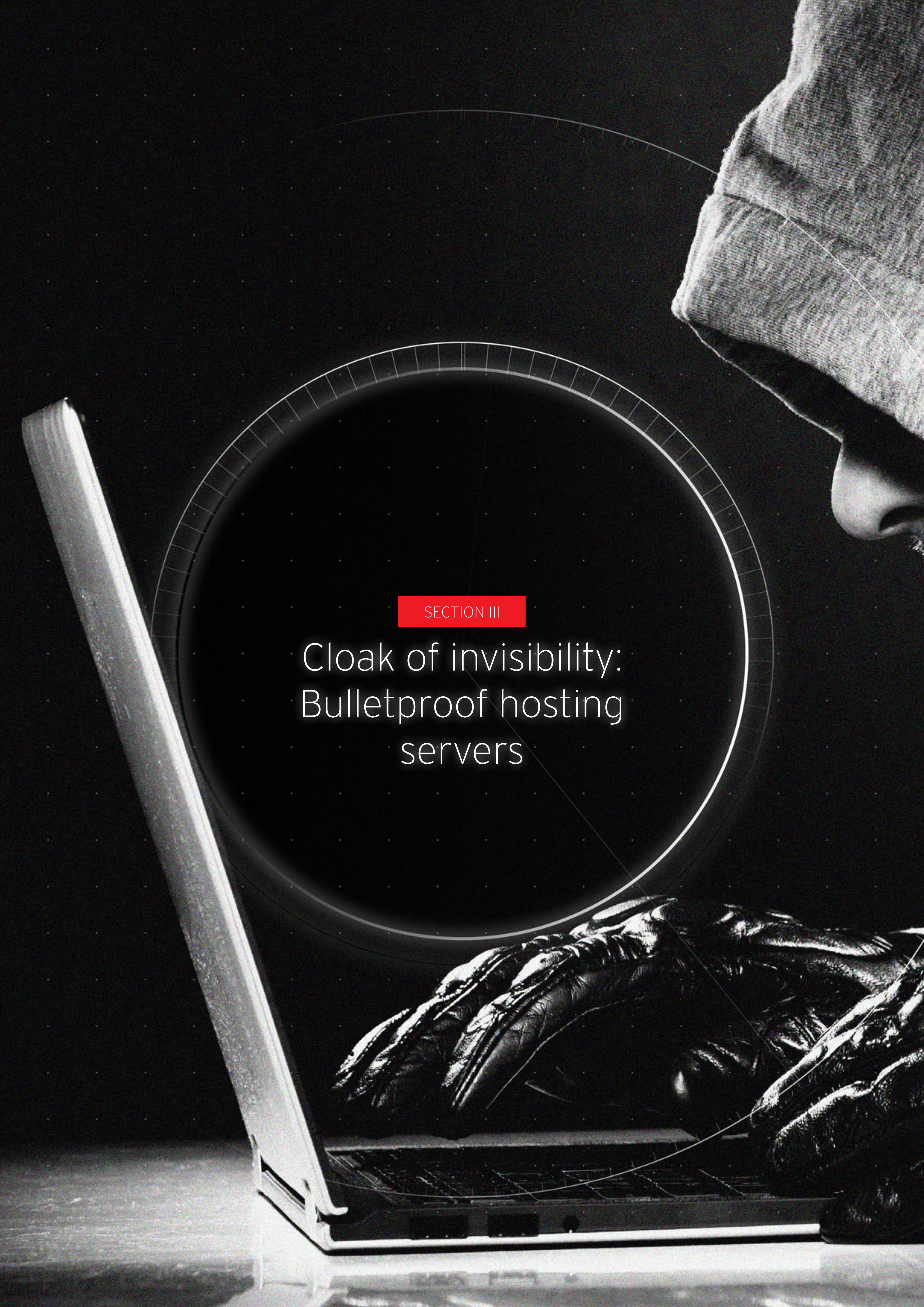
Цитата:

```
7/6/2015
(12:53:37 PM) lordc@jabber.ru/2355836208: https://us.etrade.com/
USER=M2000000
PASSWORD=aikman08
IPv4: 173.62.217.21
(1:08:29 PM) tzarit: i adding
(1:08:34 PM) tzarit: u can add same amount the one u have in balance
(1:08:36 PM) tzarit: in account
(1:08:37 PM) tzarit: thats how that shit work
(1:08:38 PM) tzarit: doing now
(1:08:44 PM) tzarit: $23,589.99 will be available for investment immediately.
(1:08:48 PM) lordc@jabber.ru/2355836208: yea i see
(1:09:08 PM) tzarit: hope i can find security which is marginable
(1:09:09 PM) tzarit: but rare ;<
(1:10:10 PM) tzarit: now we wait
(1:10:10 PM) tzarit:
(1:11:13 PM) lordc@jabber.ru/2355836208: u cant transfer from this 5 accounts to the one we added money too ?
(1:12:58 PM) lordc@jabber.ru/2355836208: wait for what
(1:14:03 PM) tzarit: no
(1:14:06 PM) tzarit: i cant
(1:14:08 PM) tzarit: i tried
(1:14:11 PM) tzarit: thy telling
(1:14:17 PM) tzarit: that accounts are on different persons
(1:14:24 PM) tzarit: it like joint accounts
(1:14:26 PM) tzarit: brothers
(1:14:27 PM) tzarit: sisters
(1:14:28 PM) tzarit: ors omething
(1:14:33 PM) lordc@jabber.ru/2355836208: ok
(1:14:36 PM) lordc@jabber.ru/2355836208: understand
(1:14:38 PM) tzarit: we wait like 20 min
```

Underground forum chat on money laundering

Antispam proofing

To bypass spam filters, the underground also has specialists who know how to bypass the email filters of big email service providers (Gmail, Yahoo Mail, MSN, Yonder, etc.). These specialists can help clients optimize the structure and/or content of their spam. They fully analyze spam content so these wouldn't be detected by spam filters.



SECTION III

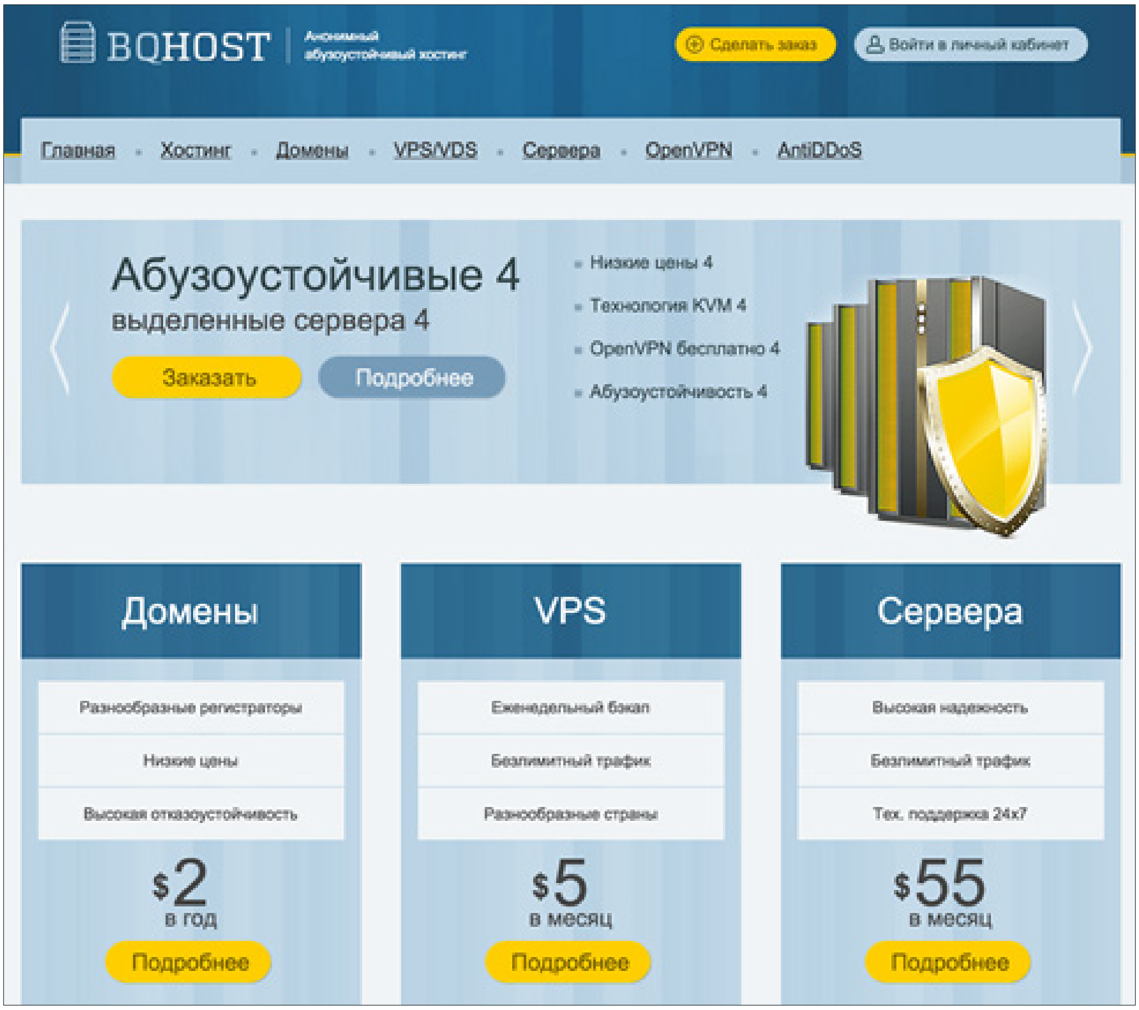
Cloak of invisibility: Bulletproof hosting servers

Cloak of invisibility: Bulletproof hosting servers

Bulletproof hosting servers represent the favorite hideouts for cybercriminals. These allow them to host malicious activities while putting on the appearance of legitimacy and operating out of countries with lax laws to avoid authorities [4]. As such, they have become essential for committing cybercrime under the radar. They seem to play a relatively smaller role in the grand scheme of things and so only pop up at the sidelines when cybercriminal operations are reported. But without the support of bulletproof hosting service (BPHS) providers to maintain and insulate criminal activities, criminal cybercommerce wouldn't exist.

Bulletproof hosts are used to store malware components and exploit kits, among others. They can serve as botnet command centers; stolen information repositories; and hosts for phishing sites, pornographic content, or scams. Nowadays, obtaining BPHSs has become easier, as users can make anonymous payments using Web money or Bitcoins. Such services have also become cheaper as a result of more affordable hosting facilities. We can even say that BPHS provision has become an industry on its own.

BPHS prices and locations largely depend on the risks involved in hosting certain content. Russia-based bulletproof servers can host both medium- and high-risk content for as low as US$70 (hardware) or US$20 (virtual private server [VPS]) per month. VPS hosting has become the industrial standard widely used by criminals due to easy maintenance.



Абузоустойчивые 4
выделенные сервера 4

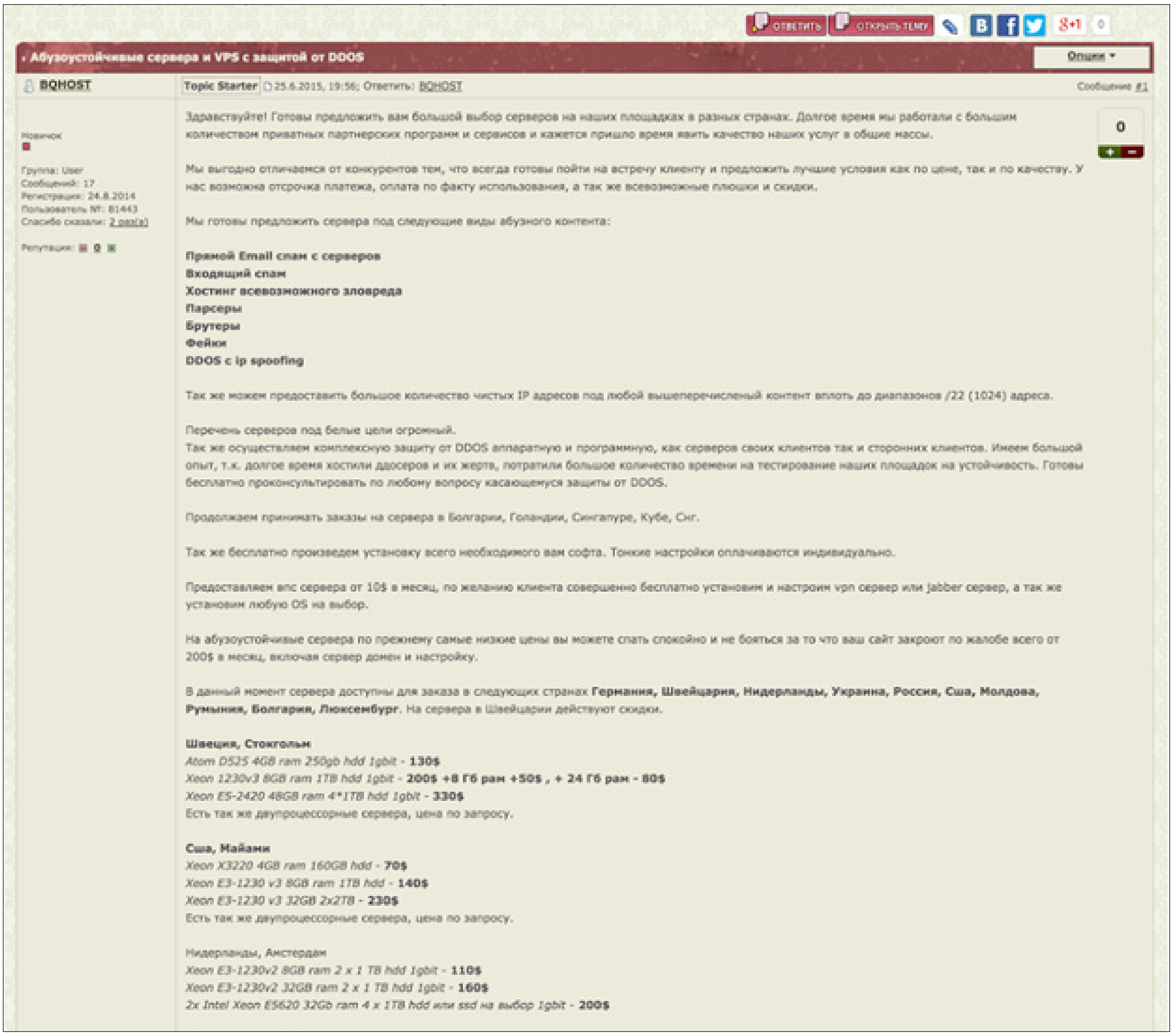
- Низкие цены 4
- Технология KVM 4
- OpenVPN бесплатно 4
- Абузоустойчивость 4

Домены	VPS	Сервера
Разнообразные регистраторы	Еженедельный бэкап	Высокая надежность
Низкие цены	Безлимитный трафик	Безлимитный трафик
Высокая отказоустойчивость	Разнообразные страны	Тех. поддержка 24x7
$2 в год	$5 в месяц	$55 в месяц

Sample BPHS provider ad (BQHOST offers "anonymous bulletproof hosting")

BQHOST offers bulletproof domains for US$2 per month)[2] , hardware servers for US$5 per month, and virtual servers for US$55 per month. It also offers various server locations, including Luxembourg, Germany, the Ukraine, and the US.

[2] *Prices were given in US$ for easier conversion into Web money or Bitcoins.*



› Абузоустойчивые сервера и VPS с защитой от DDOS

BQHOST

Topic Starter 25.6.2015, 19:56; Ответить: BQHOST

Сообщение #1

Новичок

Группа: User
Сообщений: 17
Регистрация: 24.8.2014
Пользователь №: 81443
Спасибо сказали: 2 раз(а)

Репутация: 0

0

Здравствуйте! Готовы предложить вам большой выбор серверов на наших площадках в разных странах. Долгое время мы работали с большим количеством приватных партнерских программ и сервисов и кажется пришло время явить качество наших услуг в общие массы.

Мы выгодно отличаемся от конкурентов тем, что всегда готовы пойти на встречу клиенту и предложить лучшие условия как по цене, так и по качеству. У нас возможна отсрочка платежа, оплата по факту использования, а так же всевозможные плюшки и скидки.

Мы готовы предложить сервера под следующие виды абузного контента:

Прямой Email спам с серверов
Входящий спам
Хостинг всевозможного зловреда
Парсеры
Брутеры
Фейки
DDOS с ip spoofing

Так же можем предоставить большое количество чистых IP адресов под любой вышеперечисленый контент вплоть до диапазонов /22 (1024) адреса.

Перечень серверов под белые цели огромный.
Так же осуществляем комплексную защиту от DDOS аппаратную и программную, как серверов своих клиентов так и сторонних клиентов. Имеем большой опыт, т.к. долгое время хостили ддосеров и их жертв, потратили большое количество времени на тестирование наших площадок на устойчивость. Готовы бесплатно проконсультировать по любому вопросу касающемуся защиты от DDOS.

Продолжаем принимать заказы на сервера в Болгарии, Голандии, Сингапуре, Кубе, Снг.

Так же бесплатно произведем установку всего необходимого вам софта. Тонкие настройки оплачиваются индивидуально.

Предоставляем впс сервера от 10$ в месяц, по желанию клиента совершенно бесплатно установим и настроим vpn сервер или jabber сервер, а так же установим любую OS на выбор.

На абузоустойчивые сервера по прежнему самые низкие цены вы можете спать спокойно и не бояться за то что ваш сайт закроют по жалобе всего от 200$ в месяц, включая сервер домен и настройку.

В данный момент сервера доступны для заказа в следующих странах **Германия, Швейцария, Нидерланды, Украина, Россия, Сша, Молдова, Румыния, Болгария, Люксембург**. На сервера в Швейцарии действуют скидки.

Швеция, Стокгольм
Atom D525 4GB ram 250gb hdd 1gbit - **130$**
Xeon 1230v3 8GB ram 1TB hdd 1gbit - **200$ +8 Гб рам +50$, + 24 Гб рам - 80$**
*Xeon E5-2420 48GB ram 4*1TB hdd 1gbit* - **330$**
Есть так же двупроцессорные сервера, цена по запросу.

Сша, Майами
Xeon X3220 4GB ram 160GB hdd - **70$**
Xeon E3-1230 v3 8GB ram 1TB hdd - **140$**
Xeon E3-1230 v3 32GB 2x2TB - **230$**
Есть так же двупроцессорные сервера, цена по запросу.

Нидерланды, Амстердам
Xeon E3-1230v2 8GB ram 2 x 1 TB hdd 1gbit - **110$**
Xeon E3-1230v2 32GB ram 2 x 1 TB hdd 1gbit - **160$**
2x Intel Xeon E5620 32Gb ram 4 x 1TB hdd или ssd на выбор 1gbit - **200$**

Underground forum BHPS advertisement (translated text: Прямой Email спам с серверов or direct spam; Хостинг всевозможного зловреда or hosting malware of all kinds; Парсеры or parsers; Брутеры or password brute forcing; Фейки or fakes)

SECTION IV

Underground pricing

Underground pricing

Constant monitoring of cybercriminal activities for years has allowed us to characterize the more advanced markets around and detect trends dominating the threat landscape for users in the next few years. One of the significant developments we saw, besides the entry of new products, had to do with pricing. In 2014, we already took note of a divide—while features are becoming more sophisticated and diverse, prices have been significantly dropping. And this trend continued on this year.

The decline in prices could be caused by a myriad of factors. Prices in the underground are regulated by supply and demand and so naturally experience fluctuations (a massive breach incident that brings an influx of new credit cards into the market causes prices to plummet). In addition to these regular dynamics, the market is becoming more competitive, as more and more vendors offer their products. Cybercriminals, as a result of growing demand and business expansion, have also taken to automate processes to quickly deal with all phases of a sale.

A clear price structure, of course, refers to goods and services that can be standardized and affixed with particular values (credit cards, personally identifiable information [PII], virtual private network [VPN] access, etc.). Other more sophisticated goods and services like exploits remain expensive or don't experience much fluctuation due to the specialized knowledge and skill needed to create them and the specific types buyers require.

Cheaper prices in the Russian underground are in no way a sign of a malfunctioning of the economy. It would even indicate that there's a lot of business due to low prices. If we compare the Russian underground market with new sales platforms in the Deep Web, it's still flourishing because entry into other Deep Web locations is very expensive and not every criminal requires the level of anonymity and invisibility it offers. The price of "buying" access to Deep Web cybercollaboration can cost US$1,000 or more.

The following tables show price developments for specific services and products within the last five years.

PPI (Cost per 1,000 installations)	2011	2012	2013	2014	2015
Australia	US$300–500	No data	No data	US$160–190	US$100–180
UK	US$220–$300	No data	US$150–400	US$150–350	US$90–130
US	US$100–150	US$100–250	US$120–200	US$90–150	US$40–100
Europe	US$90–250	US$75–90	US$50–110	US$90–240	US$80–130
Russia	US$100–500	No data	US$140–400	US$100–300	US$100–200
Asia	No data	No data	No data	No data	US$140
Global	US$12–15	US$10–20	US$10–12	US$8–15	US$10–12

PPI is the typical way of spreading malware; this table indicates prices of PPI per malware spread to 1,000 computers; installation comes with a guarantee; users find out via notifications of successful installation.

Proxy Service Type	2011	2012	2013	2014
Socket Secure (SOCKS)	US$2 per 24 hours	US$2 per 24 hours	US$2 per 24 hours	US$1 per 24 hours
Proxy list	US$3 per 300 IP addresses	US$4 per 300 IP addresses	US$6 per 300 IP addresses	US$4 per 300 IP addresses
HyperText Transfer Protocol (HTTP) or HTTP Secure (HTTPS)	US$2 per day	US$1 per day	US$1 per day	US$0.50 per day

A proxy refers to a computer that can proxy traffic; it can be a server, a home computer, or any other machine type.

VPN Service Type	2011	2012	2013	2014
With one exit point	US$8–12 per month	No data	No data	No data
Unlimited access	US$40 per month	US$38 per month	US$24 per month	US$15 per month
Average	US$22 per month	US$20 per month	US$15 per month	US$8 per month

There are different types of VPN service vendors, some are publicly searchable and accept Paypal and credit card payments while others are very stealthy in that users have to wait for the criminals to get in touch with them (they use compromised computers as exit points).

Antimalware-Checking Service Type	2011	2012	2013	2014
Daily checking	US$50	US$30	US$30	US$20
Automatic reuploading	US$50	US$30	US$30	US$20
Web checking	US$50	US$30	US$30	US$20

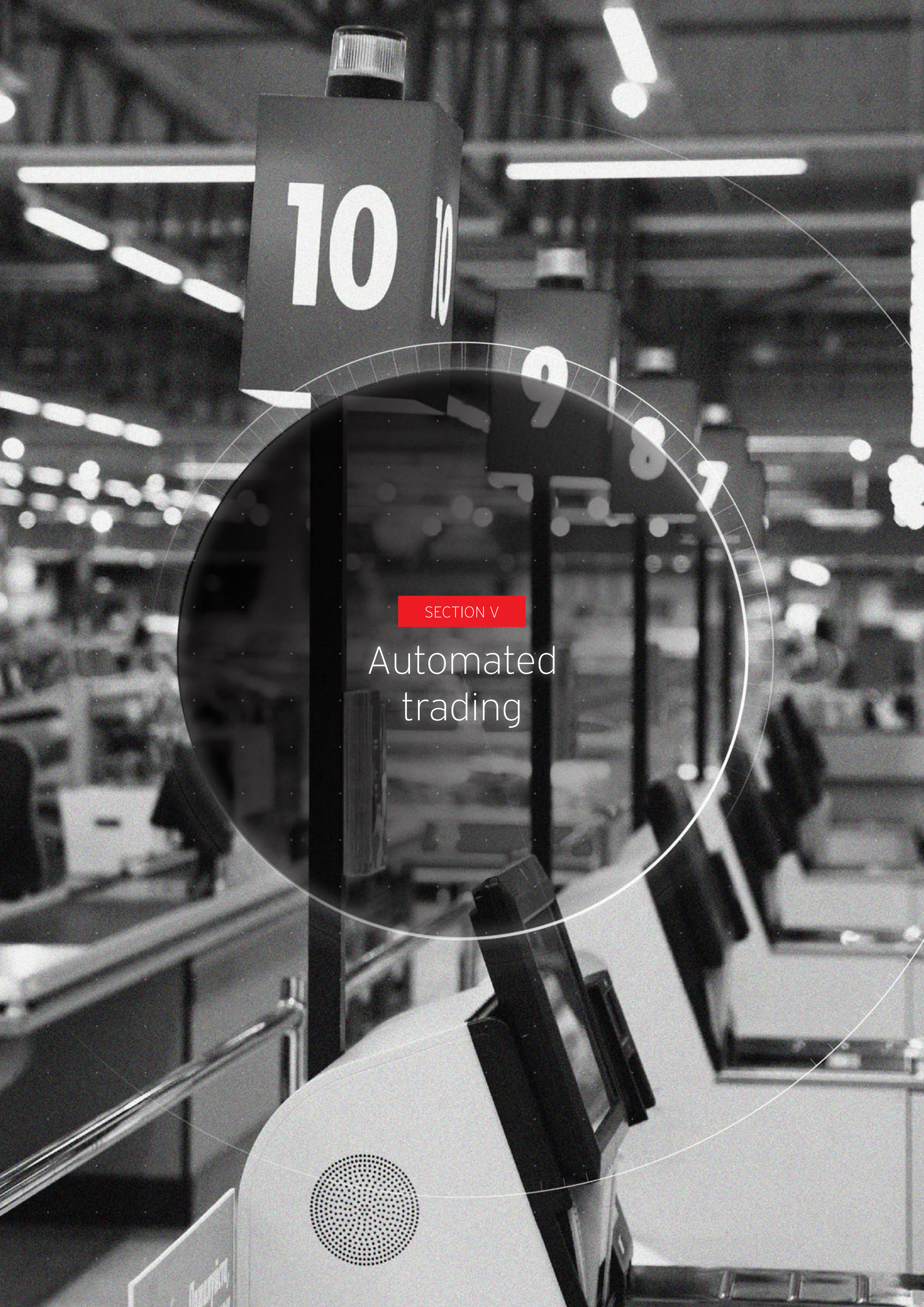
Users who have the malware with which they want to infect certain computers go to PPI service providers. They need to make sure that their malware aren't detected by typical antimalware. They won't run their Trojans or other malware on publicly available services like VirusTotal because the site will immediately share information on their malware with every security company. As such, other "companies" offer this discreet checking service.

DDoS Service Type	2011	2012	2013	2014
Lasts one hour	US$4–10	US$2–25	US$2–60	US$1–100
Lasts 24 hours	US$30–70	US$15–60	US$13–200	US$10–140

The wide range of DDoS services is due to many factors—kind of target, if the target is protected by special software or not, and if the target is a blackhat or a whitehat. Differences lie in the quality or volume of traffic used during a DDoS attack.

Spamming Service Type (Cost per 10,000 emails)	2011	2012	2013	2014
Generic (using publicly available databases)	US$13	US$8	US$4–5	US$1–3
Using external databases	US$17	US$14	US$13	US$10
Sent via Short Message Service (SMS)	US$600	US$300	US$100	US$40–100
Sent via ICQ	US$55	US$15	US$4–9	US$3–10
Sent via Skype	No data	US$110	US$86	US$49

Spamming service prices



SECTION V

Automated trading

Automated trading

Automated services

Automated garant or escrow services

All actors that operate in underground forums vigilantly hide their identities. In the event when deals go bad, there's no legal way to make claims as in the real world. As such, *garants* ("escrows" in English) were put in place to ensure smoother transactions. Garant and escrow agents process every transaction for a fee of 3–15% or higher, and upon receiving the goods and money in their accounts, then exchange the valuables after confirming that everything has been paid accordingly. Now, garant or escrow services are not completely new but we've discovered a significant change—some Russian underground forums like verified.mn offer automated garant services that allow quick sales or puchase processing. A lot of old business processes are being replaced by fully automated marketplaces.

Marketplaces and forums

Like any other market, underground markets have limitations and evolve with challenges, bringing forth new techniques, working conditions, and sometimes platforms for vendor-client deals. The pressure to ensure seamless and quick sales or purchases brought about marketplaces that, in part, are replacing forums as prime transaction places. Cybermarketplaces usually specialize in certain goods and services like credit cards, traffic (*partnerkas*), or dedicated servers.

Marketplaces are the new virtual shops for standardized goods—places for buyers and vendors to buy and sell under clear conditions. These have standard procedures and can more quickly process payments with technically enforced rules and are, therefore, more competitive than forums in terms of exchange. Forums are much slower because users would need to make contact, set deals, and then require garant or escrow services for transactions. This has to do with the nature and origin of forums. Forums were initially created for information exchange and later also used for transactions while marketplaces exclusively function as places of trade. But because of this, forums still have significance. They serve as information boards and first points of entry for anyone trying to enter a marketplace as well as places to trace bad market actors or vet the credibility of buyers and sellers and process more complicated deals. Marketplaces are restricted to selling standardized goods whose value can easily be measured like credit cards. It becomes more difficult to estimate the exact value of exploit kits or more sophisticated malware and so these still get sold via forums.

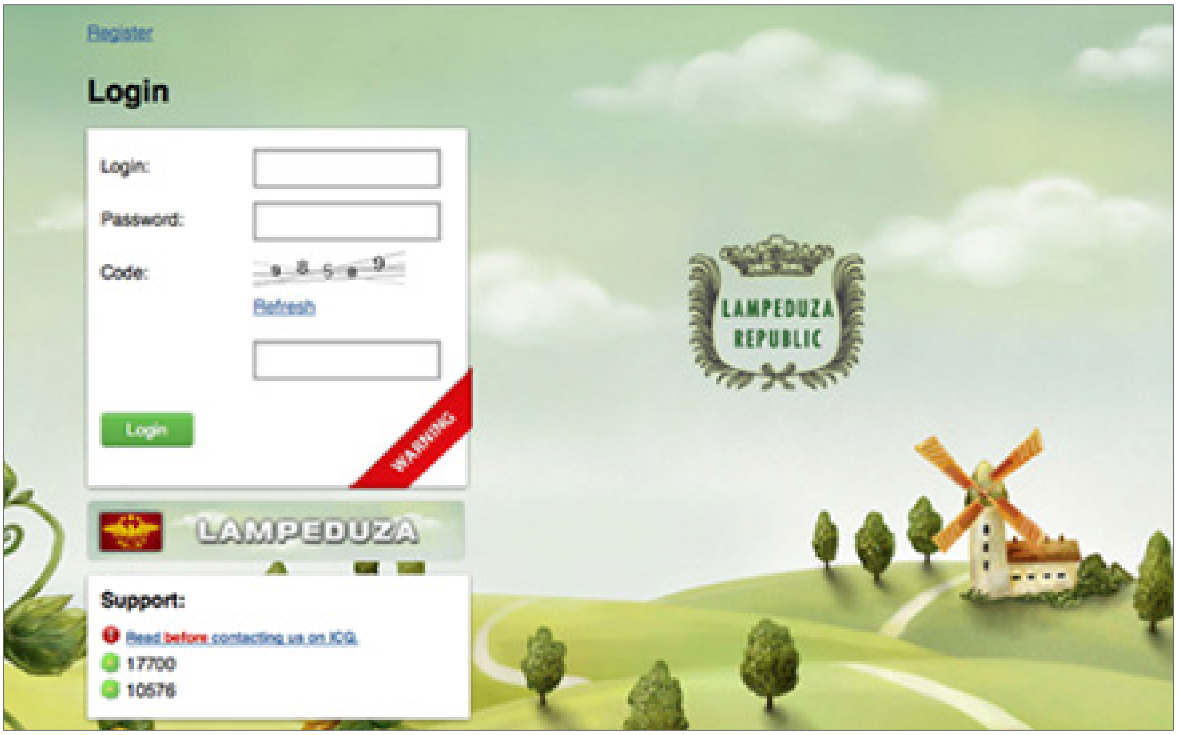
Such marketplaces in the Russian underground have been around since 2010 but they haven't been the mainstream trend until recently. 2013 and 2014 really marked a change due to the increase in stolen goods. After the significant data breaches seen in 2014 (Neimann Marcus, 350,000 credit and debit card holders; Home Depot, 56 million customers; JP Morgan, 76 million households and 7 million small businesses; and Sony, over 47,000 social security numbers), we saw the stolen credentials sold in the underground [5]. Products found in marketplaces usually include:

- Credit cards
- Stolen Secure Shell (SSH) and Remote Desktop Protocol (RDP) access to servers and private computers
- Web traffic (and, increasingly, mobile traffic)
- PPI services
- Stolen access to Paypal and other financial accounts

The most well-known examples for Russian marketplaces include:

- **fe-ccshop.su:** Marketplace to buy credit card information, including holder name, address, bank identification number (BIN), and card type. fe-ccshop.su is also involved in the business of selling fake international shipping labels (US Postal Service [USPS] or US Express Mail International) at a fraction of their actual cost. USPS labels that are purchased via fraudulent cards are known in the underground as "cc labels." These make it easy for reshipping scam operators to get hold of the required shipping labels. fe-ccshop.su has been operational for a substantial amount of time (since 2011).
- **Rescator:** This is well-known for running online credit card shops and as the administrator of the Russian carding forum, Lampeduza. We prefer to refer to the people behind this shop as the Lampeduza Gang, as Rescator is not the only person running this business. The "official" shops that Rescator runs include:
  - Octavian.su
  - Rescator.cc
  - Rescator.co
  - Rescator.cm
  - Rescator.so

This marketplace has become so famous that even fake versions of the Lampeduza shop have surfaced. Under false pretenses and disguised with the Lampeduza screen as front, unknowing cybercriminals are lured into accessing fake online credit card shops [6].

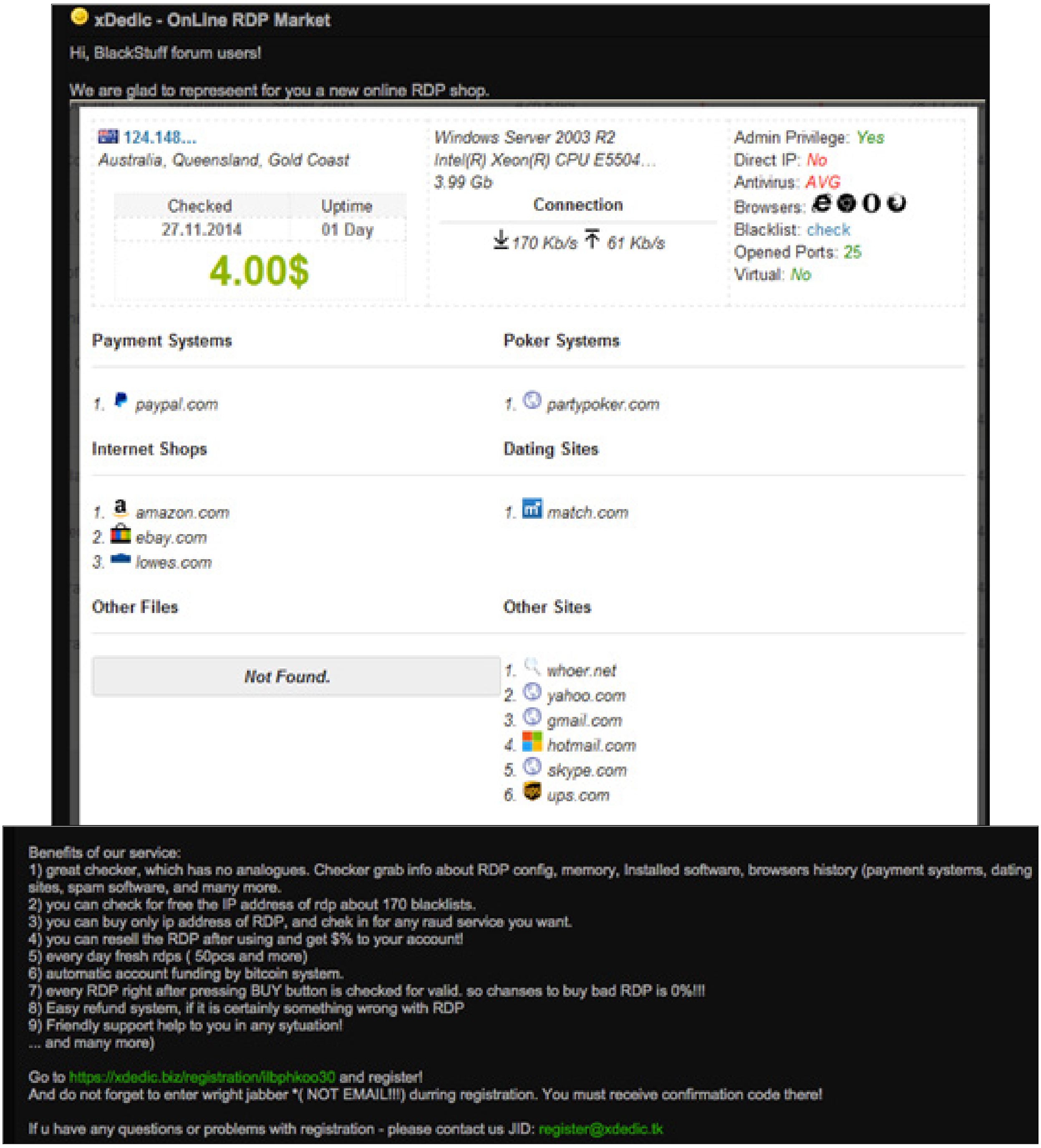


Rescator's login page

- **xdedic.biz:** Marketplace for selling stolen access credentials via RDP[3]. Compromised computers can be used for different activities though desktops (not servers) are mostly used for traffic proxying. Every computer is automatically scanned for information including:
  - Online vendor accounts (Amazon, eBay, etc.)
  - Payment systems (Paypal)
  - Gaming sites (poker.com)
  - Connection quality
  - Antimalware

  Access to compromised computers is sold on xdedic.biz, and from there, users can do as they please (use keyloggers or additional software to steal account data).

[3] *Passwords to Windows® computers are brute forced to enable RDP access so cybercriminals can remotely control them and scan for browser history activities in logs, specifically those pertaining to Amazon, for the purpose of selling in underground markets.*



xDedic - OnLine RDP Market

Hi, BlackStuff forum users!

We are glad to represeent for you a new online RDP shop.

124.148...
Australia, Queensland, Gold Coast

Checked	Uptime
27.11.2014	01 Day

4.00$

Windows Server 2003 R2
Intel(R) Xeon(R) CPU E5504...
3.99 Gb

Connection

170 Kb/s 61 Kb/s

Admin Privilege: Yes
Direct IP: No
Antivirus: AVG
Browsers:
Blacklist: check
Opened Ports: 25
Virtual: No

Payment Systems

1. paypal.com

Poker Systems

1. partypoker.com

Internet Shops

1. amazon.com
2. ebay.com
3. lowes.com

Dating Sites

1. match.com

Other Files

Not Found.

Other Sites

1. whoer.net
2. yahoo.com
3. gmail.com
4. hotmail.com
5. skype.com
6. ups.com

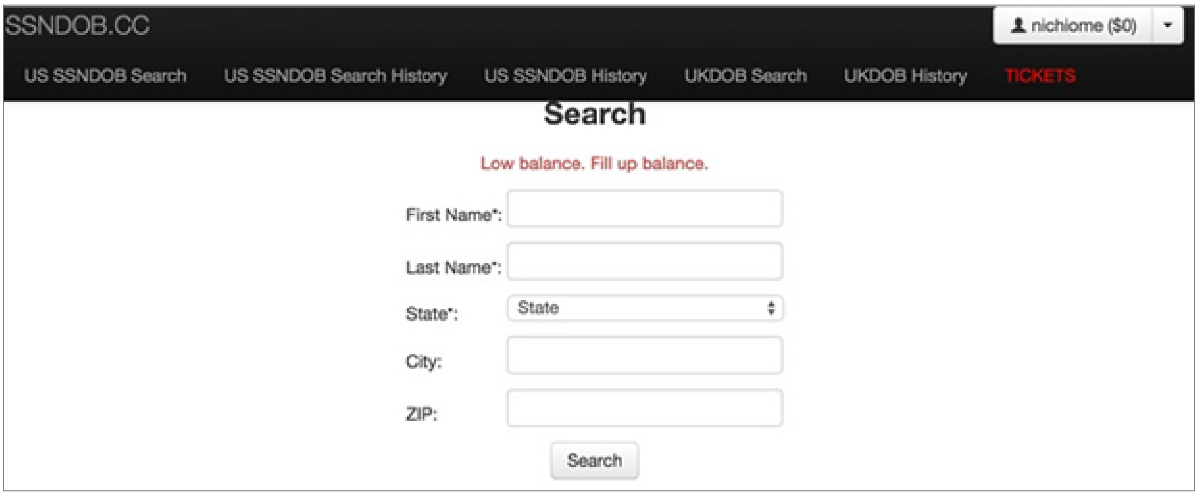
Benefits of our service:
1) great checker, which has no analogues. Checker grab info about RDP config, memory, Installed software, browsers history (payment systems, dating sites, spam software, and many more.
2) you can check for free the IP address of rdp about 170 blacklists.
3) you can buy only ip address of RDP, and chek in for any raud service you want.
4) you can resell the RDP after using and get $% to your account!
5) every day fresh rdps (50pcs and more)
6) automatic account funding by bitcoin system.
7) every RDP right after pressing BUY button is checked for valid. so chanses to buy bad RDP is 0%!!!
8) Easy refund system, if it is certainly something wrong with RDP
9) Friendly support help to you in any sytuation!
... and many more)

Go to https://xdedic.biz/registration/ilbphkoo30 and register!
And do not forget to enter wright jabber *(NOT EMAIL!!!) durring registration. You must receive confirmation code there!

If u have any questions or problems with registration - please contact us JID: register@xdedic.tk

Ad for xdedic.biz's services

- **ordaproject.com:** Marketplace to buy and sell items like:
    - Original scans of documents in different countries for fraudulent purposes:
        - Foreign passports (FRs)
        - Internal passports (for use within Russia)
        - Identification (ID) cards
        - Any foreign or internal passports or IDs (processed, including a photo that, in real life, has no connection to the address, country, or date of birth used)
            - Automated fake scanned documents (upon request, fake documents can be drawn up with special software based on information clients provide)
- **ssndob.cc:** As the name indicates, “SSN” stands for “social security number,” “DOB” for “date of birth,” and “CC” for “credit card.” Marketplace that sells social security numbers and full information about a person of interest (address, etc.). These credentials are sold for fraud. We are not entirely sure what kind of fraudulent ends these are used for but we can assume that they are used for opening bank accounts.



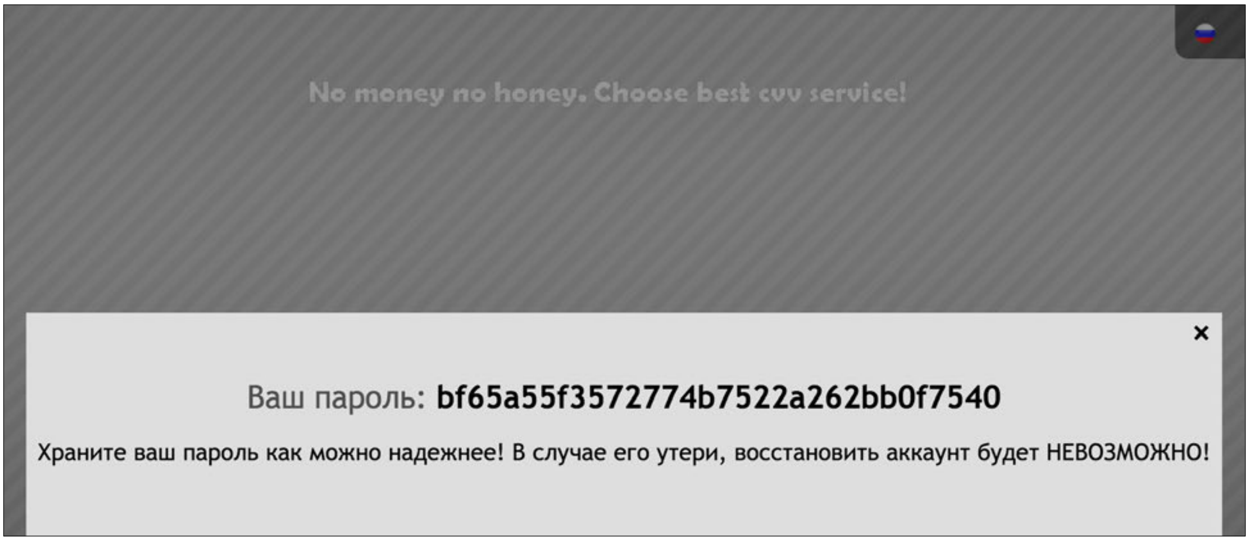
Search feature of ssndob.cc

Daily updates for credit card databases

Host:	**gocvv.cc**
IP address:	**188.xxx.xxx.203**
Provider:	**Oversun Ltd.**
Country:	**Russia**

One example for a new-generation marketplace is gocvv.cc. Its name spells out what it is about—go (go), cvv (Card Verification Value [CVV]), and cc (credit card). It is one of the biggest new-generation marketplaces that specialize in selling and purchasing stolen credit cards. Its slogan even says "No money, no honey. Choose best cvv service!" As of this paper's writing, gocvv.cc's Web server was located in Moscow, Russia at AS6870 H1ASN H1 LLC.

Registration on gocvv.cc is limited. It only allows a certain number of users. Its registration process is relatively unique; it allows users to get self-generated passwords by hitting "Register." With these passwords that aren't connected to real user names or online accounts, users can access their profiles. These are the only links connecting users to their money or goods on gocvv.cc. The site is very intent on keeping users' identities anonymous. This is an interesting feature in our opinion because it helps prevent the leakage of identities stored on the site's database, thereby protecting members from detection by undercover law enforcement agents or security researchers.

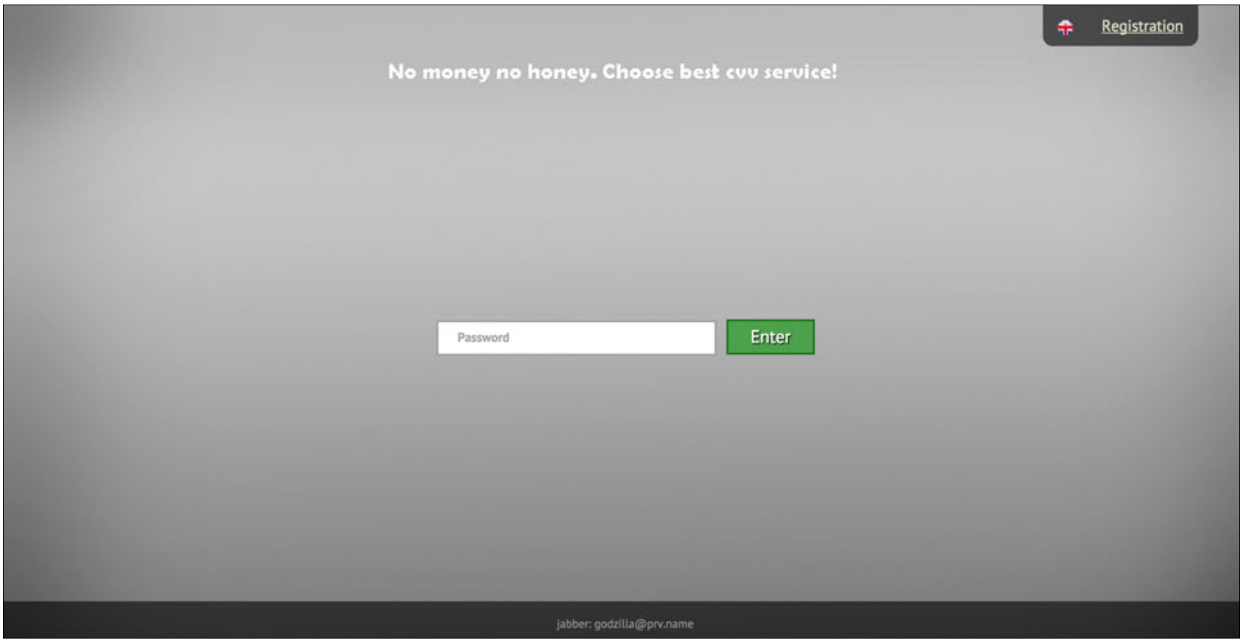


No money no honey. Choose best cvv service!

Ваш пароль: **bf65a55f3572774b7522a262bb0f7540**

Храните ваш пароль как можно надежнее! В случае его утери, восстановить аккаунт будет НЕВОЗМОЖНО!

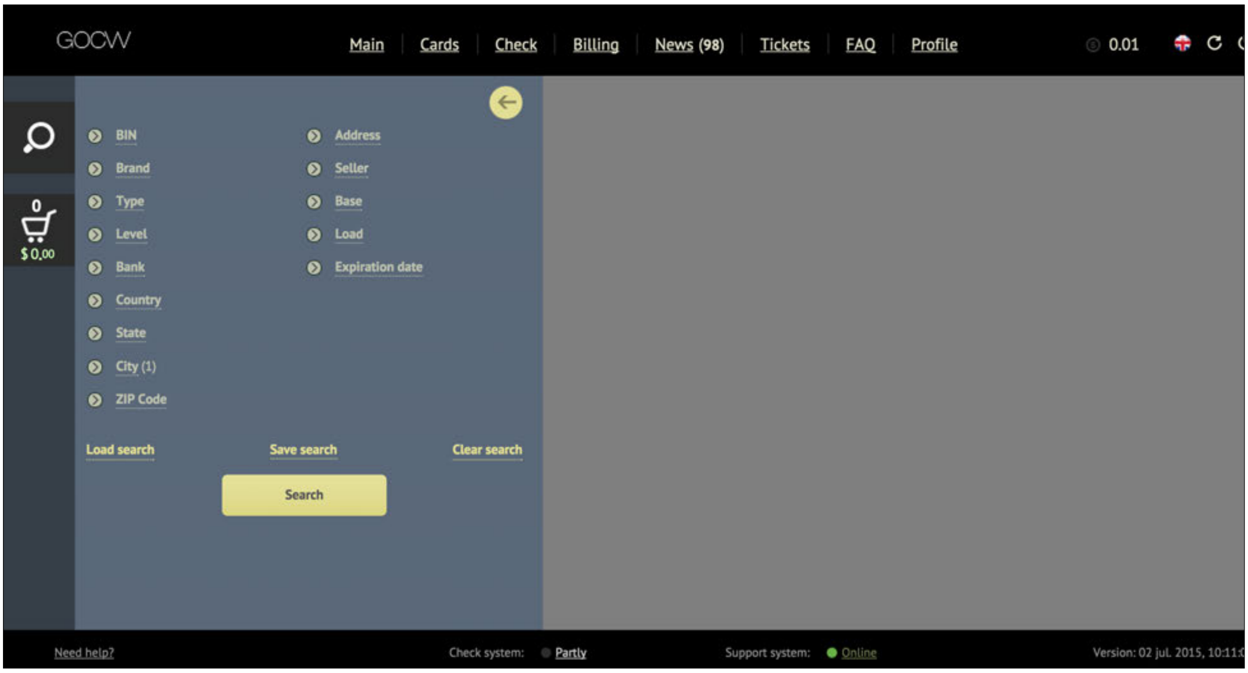
Registration message that appears on gocvv.cc, which translates to "This is your password: 43159rjiqfnejcqjndvcl1k4*. Keep your password as safe as possible. In case of password loss, there is no way to reset the password!"*


Registration
No money no honey. Choose best cvv service!
Password
Enter
jabber: godzilla@prv.name

Index page of gocvv.cc

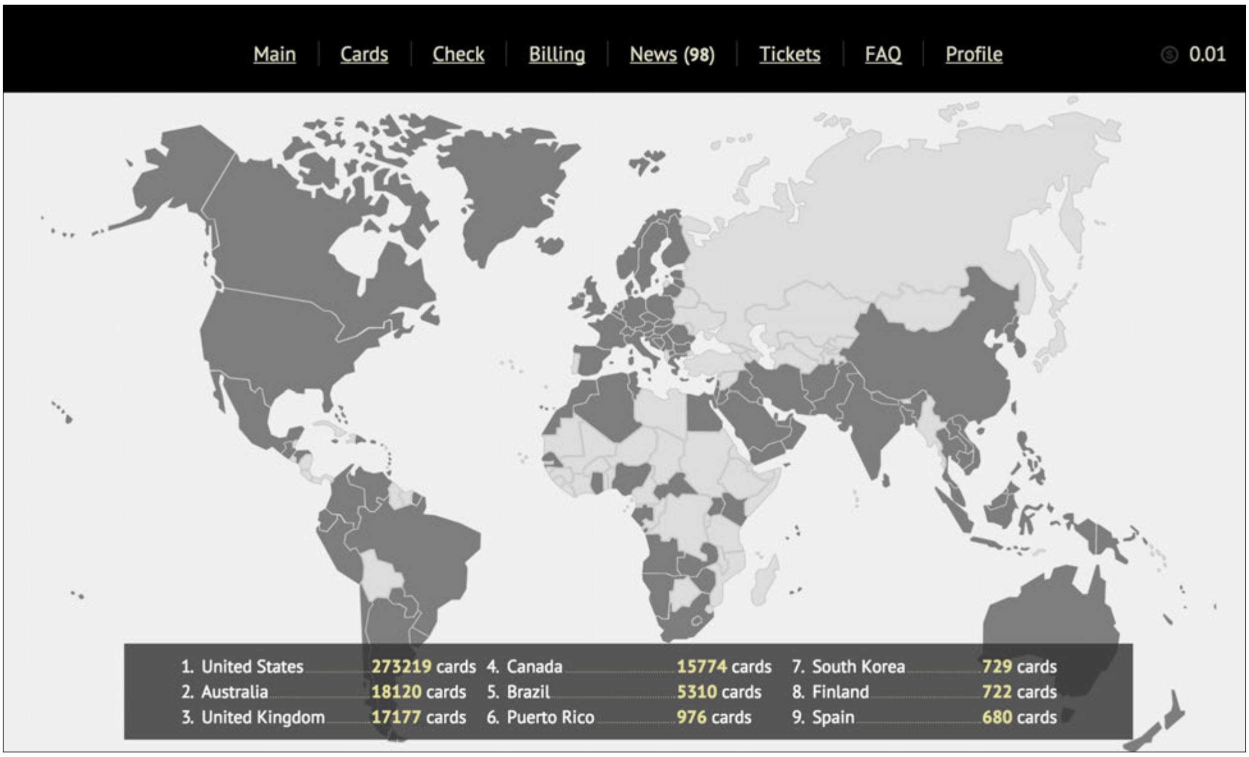
gocvv.cc has unique features, including:

- **Power search and filter:** gocvv.cc offers power search and filter features that allow users to easily sift and sort through credit cards by BIN, brand (Visa, MasterCard, etc.), card type (debit or credit), issuing country (158 countries), and US state and city ZIP code.



gocvv.cc's search and filter functionality

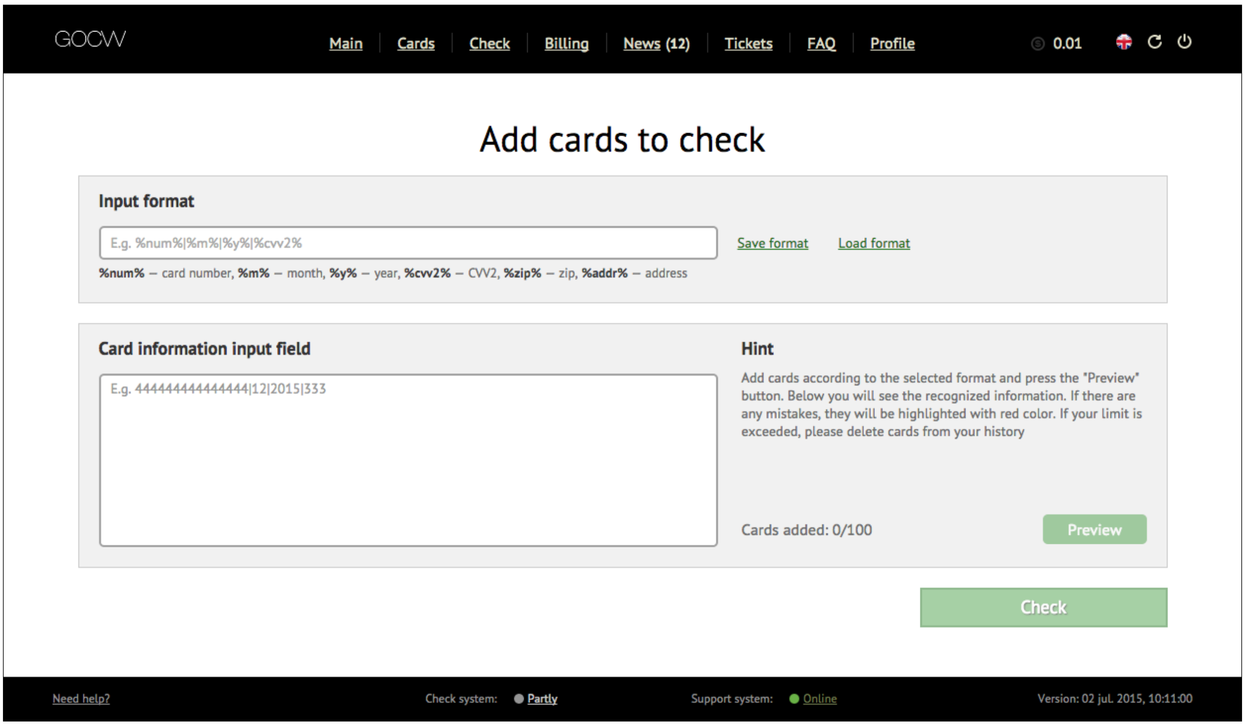
- **Global map index:** gocvv.cc's index page allows users to gauge the availability of credit cards on a world map. All users have to do is to drag their mouse to their country or region of interest to see the number of available credit cards at the moment in it.



1. United States	273219 cards	4. Canada	15774 cards	7. South Korea	729 cards
2. Australia	18120 cards	5. Brazil	5310 cards	8. Finland	722 cards
3. United Kingdom	17177 cards	6. Puerto Rico	976 cards	9. Spain	680 cards

Global map index shows the availability of credit cards to ensure a better underground shopping experience

- **Daily updates for credit card databases:** gocvv.cc updates its database every 24 hours, which consists of 121 subdatabases that are incidentally named after the political leaders of countries like "erdogan," "amato," and "chavez," among others. These subdatabases are basically files that a seller brings to the main database of gocvv.cc. This seller, who has his own dump of credit cards, zips and uploads it while the support staff of gocvv.cc will take care of the rest.
- **Card validity checks:** Cards are checked for validity by external service providers (cardok, try2check, ucheck, etc.) at US$0.30 per card. Bulk checks can be done at lower prices.



Add cards to check

Input format

E.g. %num%|%m%|%y%|%cvv2%

%num% – card number, %m% – month, %y% – year, %cvv2% – CVV2, %zip% – zip, %addr% – address

Card information input field

E.g. 4444444444444444|12|2015|333

Hint

Add cards according to the selected format and press the "Preview" button. Below you will see the recognized information. If there are any mistakes, they will be highlighted with red color. If your limit is exceeded, please delete cards from your history

Cards added: 0/100

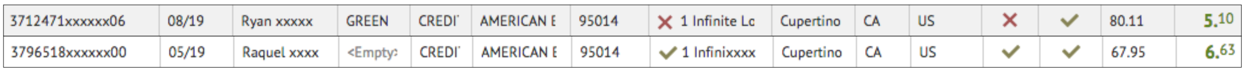
Check system: ● Partly

Support system: ● Online

Version: 02 jul. 2015, 10:11:00

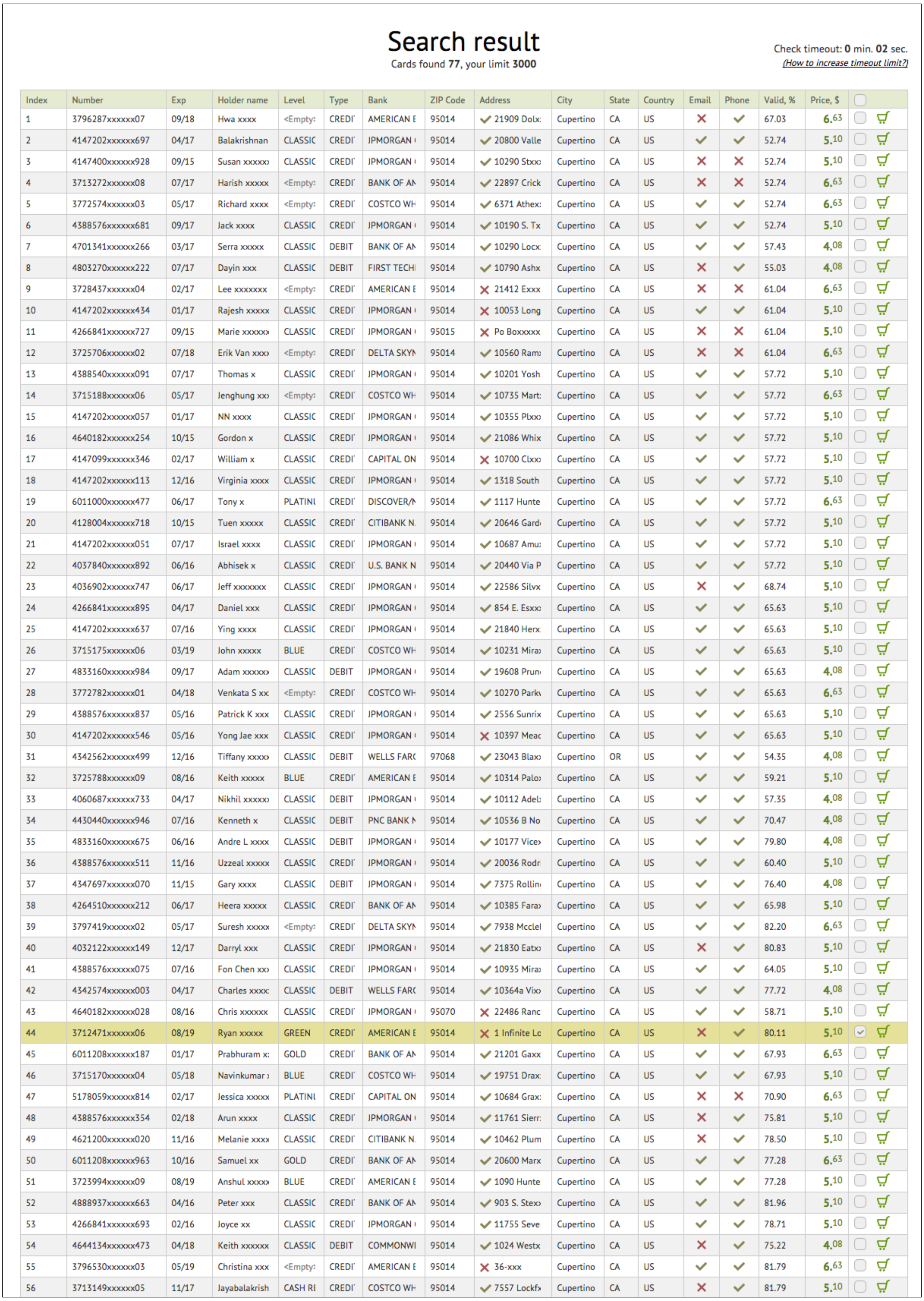
Card-validity-checking page

In a test run, we did several filter searches by ZIP code, country, and city name and successfully found the credit card details of 75 people from the Cupertino, California area. A closer look allowed us to find two credit cards linked to the address "1 Infinite Loop," which is Apple Corporation's address (see the Appendix for a sample list).



3712471xxxxxx06	08/19	Ryan xxxxx	GREEN	CREDI'	AMERICAN E	95014	✗ 1 Infinite Lc	Cupertino	CA	US	✗	✓	80.11	5.10
3796518xxxxxx00	05/19	Raquel xxxx	<Empty:	CREDI'	AMERICAN E	95014	✓ 1 Infinixxxx	Cupertino	CA	US	✓	✓	67.95	6.63

Screenshot of the two addresses appearing to belong to someone from Apple



Search result

Cards found **77**, your limit **3000**

Check timeout: **0** min. **02** sec.
(How to increase timeout limit?)

Index	Number	Exp	Holder name	Level	Type	Bank	ZIP Code	Address	City	State	Country	Email	Phone	Valid, %	Price, $	□	
1	3796287xxxxxx07	09/18	Hwa xxxx	<Empty:	CREDI	AMERICAN E	95014	✓ 21909 Dolx:	Cupertino	CA	US	✗	✓	67.03	6.63	□	🛒
2	4147202xxxxxx697	04/17	Balakrishnan	CLASSIC	CREDI	JPMORGAN (	95014	✓ 20800 Valle	Cupertino	CA	US	✓	✓	52.74	5.10	□	🛒
3	4147400xxxxxx928	09/15	Susan xxxxx)	CLASSIC	CREDI	JPMORGAN (	95014	✓ 10290 Stxx:	Cupertino	CA	US	✗	✗	52.74	5.10	□	🛒
4	3713272xxxxxx08	07/17	Harish xxxxx	<Empty:	CREDI	BANK OF AN	95014	✓ 22897 Crick	Cupertino	CA	US	✗	✗	52.74	6.63	□	🛒
5	3772574xxxxxx03	05/17	Richard xxxx	<Empty:	CREDI	COSTCO WH	95014	✓ 6371 Athex:	Cupertino	CA	US	✓	✓	52.74	6.63	□	🛒
6	4388576xxxxxx681	09/17	Jack xxxx	CLASSIC	CREDI	JPMORGAN (	95014	✓ 10190 S. Tx	Cupertino	CA	US	✓	✓	52.74	5.10	□	🛒
7	4701341xxxxxx266	03/17	Serra xxxxx	CLASSIC	DEBIT	BANK OF AN	95014	✓ 10290 Locx:	Cupertino	CA	US	✓	✓	57.43	4.08	□	🛒
8	4803270xxxxxx222	07/17	Dayin xxx	CLASSIC	DEBIT	FIRST TECHI	95014	✓ 10790 Ashx	Cupertino	CA	US	✗	✓	55.03	4.08	□	🛒
9	3728437xxxxxx04	02/17	Lee xxxxxxx	<Empty:	CREDI	AMERICAN E	95014	✗ 21412 Exxx	Cupertino	CA	US	✗	✗	61.04	6.63	□	🛒
10	4147202xxxxxx434	01/17	Rajesh xxxxx	CLASSIC	CREDI	JPMORGAN (	95014	✗ 10053 Long	Cupertino	CA	US	✓	✓	61.04	5.10	□	🛒
11	4266841xxxxxx727	09/15	Marie xxxxxx	CLASSIC	CREDI	JPMORGAN (	95015	✗ Po Boxxxxx	Cupertino	CA	US	✗	✗	61.04	5.10	□	🛒
12	3725706xxxxxx02	07/18	Erik Van xxx)	<Empty:	CREDI	DELTA SKYN	95014	✓ 10560 Ram:	Cupertino	CA	US	✗	✗	61.04	6.63	□	🛒
13	4388540xxxxxx091	07/17	Thomas x	CLASSIC	CREDI	JPMORGAN (	95014	✓ 10201 Yosh	Cupertino	CA	US	✓	✓	57.72	5.10	□	🛒
14	3715188xxxxxx06	05/17	Jenghung xx)	<Empty:	CREDI	COSTCO WH	95014	✓ 10735 Mart:	Cupertino	CA	US	✓	✓	57.72	6.63	□	🛒
15	4147202xxxxxx057	01/17	NN xxxx	CLASSIC	CREDI	JPMORGAN (	95014	✓ 10355 Plxx)	Cupertino	CA	US	✓	✓	57.72	5.10	□	🛒
16	4640182xxxxxx254	10/15	Gordon x	CLASSIC	CREDI	JPMORGAN (	95014	✓ 21086 Whix	Cupertino	CA	US	✓	✓	57.72	5.10	□	🛒
17	4147099xxxxxx346	02/17	William x	CLASSIC	CREDI	CAPITAL ON	95014	✗ 10700 Clxx)	Cupertino	CA	US	✓	✓	57.72	5.10	□	🛒
18	4147202xxxxxx113	12/16	Virginia xxxx	CLASSIC	CREDI	JPMORGAN (	95014	✓ 1318 South	Cupertino	CA	US	✓	✓	57.72	5.10	□	🛒
19	6011000xxxxxx477	06/17	Tony x	PLATINU	CREDI	DISCOVER/N	95014	✓ 1117 Hunte	Cupertino	CA	US	✓	✓	57.72	6.63	□	🛒
20	4128004xxxxxx718	10/15	Tuen xxxxx	CLASSIC	CREDI	CITIBANK N.	95014	✓ 20646 Gard	Cupertino	CA	US	✓	✓	57.72	5.10	□	🛒
21	4147202xxxxxx051	07/17	Israel xxxx	CLASSIC	CREDI	JPMORGAN (	95014	✓ 10687 Amu:	Cupertino	CA	US	✓	✓	57.72	5.10	□	🛒
22	4037840xxxxxx892	06/16	Abhisek x	CLASSIC	CREDI	U.S. BANK N	95014	✓ 20440 Via P	Cupertino	CA	US	✓	✓	57.72	5.10	□	🛒
23	4036902xxxxxx747	06/17	Jeff xxxxxxx	CLASSIC	CREDI	JPMORGAN (	95014	✓ 22586 Silvx	Cupertino	CA	US	✗	✓	68.74	5.10	□	🛒
24	4266841xxxxxx895	04/17	Daniel xxx	CLASSIC	CREDI	JPMORGAN (	95014	✓ 854 E. Esxx:	Cupertino	CA	US	✓	✓	65.63	5.10	□	🛒
25	4147202xxxxxx637	07/16	Ying xxxx	CLASSIC	CREDI	JPMORGAN (	95014	✓ 21840 Herx	Cupertino	CA	US	✓	✓	65.63	5.10	□	🛒
26	3715175xxxxxx06	03/19	John xxxxx	BLUE	CREDI	COSTCO WH	95014	✓ 10231 Mira)	Cupertino	CA	US	✓	✓	65.63	5.10	□	🛒
27	4833160xxxxxx984	09/17	Adam xxxxxx	CLASSIC	DEBIT	JPMORGAN (	95014	✓ 19608 Prun	Cupertino	CA	US	✓	✓	65.63	4.08	□	🛒
28	3772782xxxxxx01	04/18	Venkata S xx:	<Empty:	CREDI	COSTCO WH	95014	✓ 10270 Park	Cupertino	CA	US	✓	✓	65.63	6.63	□	🛒
29	4388576xxxxxx837	05/16	Patrick K xxx	CLASSIC	CREDI	JPMORGAN (	95014	✓ 2556 Sunrix	Cupertino	CA	US	✓	✓	65.63	5.10	□	🛒
30	4147202xxxxxx546	05/16	Yong Jae xxx	CLASSIC	CREDI	JPMORGAN (	95014	✗ 10397 Meac	Cupertino	CA	US	✓	✓	65.63	5.10	□	🛒
31	4342562xxxxxx499	12/16	Tiffany xxxx)	CLASSIC	DEBIT	WELLS FAR(	97068	✓ 23043 Blax)	Cupertino	OR	US	✓	✓	54.35	4.08	□	🛒
32	3725788xxxxxx09	08/16	Keith xxxxx	BLUE	CREDI	AMERICAN E	95014	✓ 10314 Palo)	Cupertino	CA	US	✓	✓	59.21	5.10	□	🛒
33	4060687xxxxxx733	04/17	Nikhil xxxxx)	CLASSIC	DEBIT	JPMORGAN (	95014	✓ 10112 Adel:	Cupertino	CA	US	✓	✓	57.35	4.08	□	🛒
34	4430440xxxxxx946	07/16	Kenneth x	CLASSIC	DEBIT	PNC BANK N	95014	✓ 10536 B No	Cupertino	CA	US	✓	✓	70.47	4.08	□	🛒
35	4833160xxxxxx675	06/16	Andre L xxxx	CLASSIC	DEBIT	JPMORGAN (	95014	✓ 10177 Vice)	Cupertino	CA	US	✓	✓	79.80	4.08	□	🛒
36	4388576xxxxxx511	11/16	Uzzeal xxxxx	CLASSIC	CREDI	JPMORGAN (	95014	✓ 20036 Rodr	Cupertino	CA	US	✓	✓	60.40	5.10	□	🛒
37	4347697xxxxxx070	11/15	Gary xxxx	CLASSIC	DEBIT	JPMORGAN (	95014	✓ 7375 Rollin	Cupertino	CA	US	✓	✓	76.40	4.08	□	🛒
38	4264510xxxxxx212	06/17	Heera xxxxx	CLASSIC	CREDI	BANK OF AN	95014	✓ 10385 Fara)	Cupertino	CA	US	✓	✓	65.98	5.10	□	🛒
39	3797419xxxxxx02	05/17	Suresh xxxxx	<Empty:	CREDI	DELTA SKYN	95014	✓ 7938 Mcclel	Cupertino	CA	US	✓	✓	82.20	6.63	□	🛒
40	4032122xxxxxx149	12/17	Darryl xxx	CLASSIC	CREDI	JPMORGAN (	95014	✓ 21830 Eatx)	Cupertino	CA	US	✗	✓	80.83	5.10	□	🛒
41	4388576xxxxxx075	07/16	Fon Chen xx)	CLASSIC	CREDI	JPMORGAN (	95014	✓ 10935 Mira)	Cupertino	CA	US	✓	✓	64.05	5.10	□	🛒
42	4342574xxxxxx003	04/17	Charles xxxx:	CLASSIC	DEBIT	WELLS FAR(	95014	✓ 10364a Vix)	Cupertino	CA	US	✓	✓	77.72	4.08	□	🛒
43	4640182xxxxxx028	08/16	Chris xxxxxx	CLASSIC	CREDI	JPMORGAN (	95070	✗ 22486 Ranc	Cupertino	CA	US	✓	✓	58.71	5.10	□	🛒
44	3712471xxxxxx06	08/19	Ryan xxxxx	GREEN	CREDI	AMERICAN E	95014	✗ 1 Infinite Lc	Cupertino	CA	US	✗	✓	80.11	5.10	☑	🛒
45	6011208xxxxxx187	01/17	Prabhuram x:	GOLD	CREDI	BANK OF AN	95014	✓ 21201 Gaxx	Cupertino	CA	US	✓	✓	67.93	6.63	□	🛒
46	3715170xxxxxx04	05/18	Navinkumar)	BLUE	CREDI	COSTCO WH	95014	✓ 19751 Drax:	Cupertino	CA	US	✓	✓	67.93	5.10	□	🛒
47	5178059xxxxxx814	02/17	Jessica xxxxx	PLATINU	CREDI	CAPITAL ON	95014	✓ 10684 Grax:	Cupertino	CA	US	✗	✗	70.90	6.63	□	🛒
48	4388576xxxxxx354	02/18	Arun xxxx	CLASSIC	CREDI	JPMORGAN (	95014	✓ 11761 Sierr:	Cupertino	CA	US	✗	✓	75.81	5.10	□	🛒
49	4621200xxxxxx020	11/16	Melanie xxxx	CLASSIC	CREDI	CITIBANK N.	95014	✓ 10462 Plum	Cupertino	CA	US	✗	✓	78.50	5.10	□	🛒
50	6011208xxxxxx963	10/16	Samuel xx	GOLD	CREDI	BANK OF AN	95014	✓ 20600 Marx	Cupertino	CA	US	✓	✓	77.28	6.63	□	🛒
51	3723994xxxxxx09	08/19	Anshul xxxxx	BLUE	CREDI	AMERICAN E	95014	✓ 1090 Hunte	Cupertino	CA	US	✓	✓	77.28	5.10	□	🛒
52	4888937xxxxxx663	04/16	Peter xxx	CLASSIC	CREDI	BANK OF AN	95014	✓ 903 S. Stex)	Cupertino	CA	US	✓	✓	81.96	5.10	□	🛒
53	4266841xxxxxx693	02/16	Joyce xx	CLASSIC	CREDI	JPMORGAN (	95014	✓ 11755 Seve	Cupertino	CA	US	✓	✓	78.71	5.10	□	🛒
54	4644134xxxxxx473	04/18	Keith xxxxxx	CLASSIC	DEBIT	COMMONWI	95014	✓ 1024 Westx	Cupertino	CA	US	✗	✓	75.22	4.08	□	🛒
55	3796530xxxxxx03	05/19	Christina xxx	<Empty:	CREDI	AMERICAN E	95014	✗ 36-xxx	Cupertino	CA	US	✓	✓	81.79	6.63	□	🛒
56	3713149xxxxxx05	11/17	Jayabalakrish	CASH RI	CREDI	COSTCO WH	95014	✓ 7557 Lockf)	Cupertino	CA	US	✗	✓	81.79	5.10	□	🛒

Screenshot of credit card details of people from Cupertino, California

SECTION VI

Political activism from the underground

Political activism from the underground

Cyberwarriors and cybermilitias

Using hacking know-how to further a political agenda is not a new phenomenon. Over the past three decades, cyberspace has turned into a digital battleground for activists with a political voice who not only want to voice their opinion, but also take direct action to make a point [7]. Their political or ideological affiliation is the basis for their activities and tactics, which usually involve blocking access to websites, website redirection, and hacking email accounts, among others. Related to this are self-proclaimed "cyberwarriors" or "cyber armies" that, via hacking tools, indirectly seek to participate in broader conflicts.

It is interesting to note that some hackers are more interested in furthering their political beliefs without monetary gain. In the Russian underground, we typically find two types politico-hackers or cyberfighters:

- Those with a political belief they deem worth fighting for and use cyber means to achieve some sort of action. Often, in their self-definition, they view themselves as self-assigned "units" and claim to act on behalf of a government or group of individuals. They make use of their cyber know-how to interrupt their target's infrastructure (via DDoS attacks, etc.).

- Those that actually do it for money or "cybermercenaries." They get paid to deliver for a third party with a political agenda. This third party can be some activist group without cyber know-how, a nonstate actor, or even state actor.

The Ukraine crisis and the hacker community

In the Ukraine crisis's case, we witnessed a considerable reaction from the underground community. The cybercommunity was divided into two groups—those supporting the revolution in the country and those supporting the Russian policy. We have to highlight here that the Russian-speaking cybercommunity does not only consist of Russian nationals, but also includes Ukrainians, Belarusians, and people from former Soviet Union nations, including the Baltic countries. We've seen intense forum discussions or fights regarding the annexation of Crimea and other military activities take place on Ukrainian territory. As a result of clashing political opinions, a large number of these forums' members were either banished or willingly left the forums. Besides debates in forums, we also saw activities that made actual impact.

CyberBerkut: Attacking in the name of the Russian cause

A pro-Russian group named “CyberBerkut” claimed responsibility for hacking German government websites early this January [8]. This group derived its name from“Berkut” (“Бе’ркут” in Ukrainian or “Golden Eagle” in English), a former special unit of the Ukrainian Police initially bestowed with high-risk interventions during riots and hostage situations that came under scrutiny for violently dispersing protesters during the Euromaidan protest movement. After its disbandment in February 2014, the Crimean Berkut unit of the police force was incorporated into the Russian Ministry of Interior under the same name. The Euromaidan protest and dissolution of the Berkut police force also marked the beginning of the group CyberBerkut, an organized group of pro-Russian cybercriminals whose proclaimed goals consist of fighting arbitrary rule and Western involvement and ensuring “freedom of speech” in the Ukraine. CyberBerkut has since been involved in a number of cyber attacks against Ukrainian and Western government entities, mostly carried out in the form of DDoS attacks, but also seem to be using more sophisticated tools to hack email accounts and steal confidential information. It claims responsibility for all of its attacks on its website (*cyber-berkut.org/en/*) and social-networking profiles.

CyberBerkut’s means of engagement include:

- “Monitoring” the computer networks of Ukrainian ministries, armed forces, prosecutor’s office, and other offices of interest

- Hacking official email accounts and servers in order to gain access to and publish confidential documents and conversations of interest (Ukraine Ministry of Information Policy, Foreign Missions (US and North Atlantic Treaty Organization [NATO] states, US European Command [EUCOM], armed forces, prosecutor’s office, presidential administration, etc.)

- Launching attacks against NATO and NATO member states’ websites (temporary disruption, for example)

Conclusion

Conclusion

When delving into the depths of cybercrime today, in the example of the Russian underground, we find a mature ecosystem that covers all aspects of cybercriminal business activities and offers an increasingly professional underground infrastructure for the sale of malicious goods and services.

We witness increasing professionalization of the crime business that allows cheaper prices to dominate sales and thereby make it easy and very affordable for anyone without significant skill to buy whatever he needs to conduct criminal dealings. The Russian marketplace is now very segmented into different service groups that aid criminals in different areas of expertise. As demand drives innovation, we see more sophisticated tools, largely automated sales processes, and optimized division of labor.

In order to tackle challenges arising from underground threats, it is important for the security industry to understand the workings and structure of such underground markets. Trend Micro is continuously working to find and analyze the most recent and significant trends from the underground. The underground is alive and thriving and won’t disappear anytime soon.

Appendix

Details on data-collection methods

Within categorizations, we can associate activities using the cross-cutting principle. In practical applications on cases, we usually associate more than one category with each cyber activity. Take, "malicious traffic," for example. We categorized it under "PPI," "traffic resale," and, in some cases, "blackhat search engine optimization (SEO)." This allows us to be more flexible and cover more aspects during categorization and create more options for data correlation.

Sometimes, cybercriminals advertise their services and/or goods on multiple forums at the same time. We use comparison techniques to correlate these information snippets to save time and resourse during further manual categorization, data normalization, and analysis of the incoming data to our underground database.

List of activity categories

1. Crypting services
2. Dedicated servers
3. SOCKS proxy
4. VPN
5. PPI
6. Programming
7. DDoS services
8. Spam
9. C&C
10. Antivirus (AV) check
11. Laundering
12. File Transfer Protocol (FTP) accounts
13. Trojans
14. Rootkits
15. Carders
16. Social engineering
17. Account hacking
18. Document scan resale
19. Abuse services
20. SMS fraud
21. Ransomware
22. Obfuscation
23. Serials
24. Exploit
25. iMoney
26. Fake
27. Traffic
28. SEO
29. Money schemas
30. Web shell
31. Database
32. Remote access tool (RAT)
33. Online gaming accounts
34. Jabber
35. Android application package (APK) development
36. Fake APK software
37. Mobile traffic
38. Mobile fraud

gocvv.cc subdatabases named after political leaders

Database	Nickname	Number of Credit Cards	Valid
grotewohl	thebest	934	87.55%
amato	krone	56	87.41%
garfield	thebest	239	86.82%
peel	usafucker	899	86.46%
kiesinger	thebest	302	85.73%
chamberlain	thebest	214	85.61%
compton	thebest	294	85.60%
luther	thebest	115	84.70%
holles	thebest	87	84.44%
caprivi	thebest	422	83.71%
harding	thebest	788	83.28%
jenkinson	thebest	1,132	82.89%
adenauer	thebest	385	82.86%
russell	thebest	55	82.73%
erhard	thebest	1,995	82.62%
taft	thebest	614	81.92%
perceval	thebest	110	81.54%
arthur	thebest	3,074	81.52%
bauer	thebest	54	81.29%
erdogan	berkut	65,565	80.97%
bruning	texasranger	4,775	80.88%
lukashenko	thebest	1,372	80.23%
goria	thebest	1,281	79.44%
bannerman	thebest	637	79.27%
north	thebest	121	79.11%
modrow	thebest	26	79.09%
michaelis	thebest	1,043	79.04%
polk	thebest	3,865	78.88%
andreotti	thebest	210	78.72%
hertling	thebest	855	78.39%
kennedy	thebest	698	78.32%
cuno	thebest	461	78.27%
grant	thebest	16,723	77.89%
law	texasranger	2,343	77.61%
letta	godzilla	106	77.38%
pierce	thebest	1,877	77.35%
cleveland	thebest	1,838	77.28%
morales	thebest	2,596	77.26%
baden	thebest	377	77.23%
dalema	wizard	2,305	77.13%
grey	thebest	1,601	76.79%
temple	thebest	775	76.49%

Database	Nickname	Number of Credit Cards	Valid
truman	thebest	676	76.36%
walpole	thebest	206	76.32%
addington	thebest	4,308	76.29%
prodi	thebest	36	76.02%
macmillan	thebest	515	75.70%
sindermann	thebest	209	75.69%
stoph	thebest	183	75.61%
fehrenbach	thebest	137	75.21%
fitzmaurice	thebest	12,821	74.81%
bentinck	thebest	554	74.58%
harrison	thebest	410	74.58%
rudd	thebest	2,301	74.31%
mitterrand	thebest	3,676	74.15%
marx	ne0	525	74.11%
buchanan	thebest	748	73.89%
lamb	wizard	1,127	72.97%
heath	thebest	2,584	72.55%
johnson	thebest	1,154	72.42%
ciampi	texasranger	574	72.32%
baldwin	texasranger	213	71.80%
andropov	thebest	598	71.67%
dini	pipedream	330	71.60%
brandt	thebest	352	71.52%
walesa	thebest	425	71.20%
douglas-home	thebest	672	71.19%
coolidge	thebest	235	70.85%
schroder	thebest	2,014	70.85%
khamenei	jsilver	138	70.66%
devonshire	thebest	625	70.38%
macdonald	thebest	1,341	70.17%
lincoln	thebest	1,017	70.14%
ford	thebest	203	70.12%
mckinley	thebest	8,789	69.94%
stresemann	thebest	468	69.54%
ebert	thebest	482	69.36%
fillmore	thebest	349	69.27%
brezhnev	thebest	682	68.85%
schwerin	thebest	1,828	68.48%
de gaulle	thebest	1,443	68.38%
khrushchev	thebest	147	68.06%
hitler	thebest	796	66.57%
goebbels	thebest	662	66.16%
disraeli	thebest	3,290	65.95%
franklin	optimus	80,931	65.54%

Database	Nickname	Number of Credit Cards	Valid
asquith	thebest	53	65.51%
blair	thebest	289	65.22%
derby	thebest	211	64.95%
balfour	thebest	472	64.71%
buren	thebest	516	64.30%
major	thebest	456	64.30%
primrose	thebest	1,579	63.99%
grafton	optimus	25	63.70%
taylor	thebest	722	62.90%
salisbury	thebest	1,262	62.41%
hollweg	krone	1,536	62.39%
callaghan	thebest	154	61.75%
aberdeen	thebest	713	60.89%
koutchma	thebest	28,297	60.71%
mussolini	thebest	111	60.41%
wilson	thebest	913	60.34%
renzi	thebest	1,474	59.69%
chavez	long	209	59.55%
grenville	thebest	567	59.22%
churchill	thebest	361	58.68%
chlodwig	thebest	483	58.45%
brown	thebest	1,028	58.24%
silva	thebest	1,024	58.16%
pitt	thebest	604	57.69%
hayes	optimus	3,735	56.60%
papen	thebest	433	56.43%
eden	thebest	841	56.12%
clinton	thebest	6,762	55.53%
haase	thebest	4,123	55.03%
cameron	thebest	265	53.86%
bolivar	thebest	3,493	52.37%
chernenko	thebest	348	52.05%
bulow	thebest	1,757	51.89%
carter	optimus	4,955	50.19%
merkel	thebest	230	49.14%
wirth	qwer	90	48.95%
jinping	optimus	8,079	35.18%

References

1. Max Goncharov. (2012). *Trend Micro Security Intelligence.* “Russian Underground 101.” Last accessed on 21 July 2015, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf.

2. Max Goncharov. (2014). *Trend Micro Security Intelligence.* “Russian Underground Revisited.” Last accessed on 21 July 2015, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf.

3. TrendLabs. (2013). *Trend Micro Security Intelligence.* “Blurring Boundaries: Trend Micro Security Predictions for 2014 and Beyond.” Last accessed on 24 July 2015, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-trend-micro-security-predictions-for-2014-and-beyond.pdf.

4. Max Goncharov. (2015). *Trend Micro Security Intelligence.* “Criminal Hideouts for Lease: Bulletproof Hosting Services.” Last accessed on 23 July 2015, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-criminal-hideouts-for-lease.pdf.

5. Bill Hardekopf. (14 January 2015). *Forbes.* “The Big Data Breaches of 2014.” Last accessed on 24 July 2015, http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/.

6. Trend Micro Incorporated. (7 October 2014). *TrendLabs Security Intelligence Blog.* “No Honor Among Thieves: Beware the Lampeduza Scam.” Last accessed on 23 July 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/no-honor-among-thieves-beware-the-lampeduza-scam/.

7. Steven Levy. (1984). “Hackers: Heroes of the Computer Revolution.”

8. Trend Micro Incorporated. (20 January 2015). *TrendLabs Security Intelligence Blog.* “Hacktivist Group CyberBerkut Behind Attacks on German Official Websites.” Last accessed on 23 July 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/hacktivist-group-cyberberkut-behind-attacks-on-german-official-websites/.

Created by:

TrendLabs

The Global Techincal Support and R&D Center of TREND MICRO

TREND MICRO™

Trend Micro Incorporated, 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 Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com.

TREND MICRO™

Securing Your Journey
to the Cloud