



THE UNDERGROUND ECONOMY



THE UNDERGROUND ECONOMY

The seeds of cybercrime grow in the anonymized depths of the dark web – underground websites where the criminally minded meet to traffic in illegal products and services, develop contacts for jobs and commerce, and even socialize with friends.

To better understand how cybercriminals operate today and what they might do in the future, Trustwave SpiderLabs researchers maintain a presence in some of the more prominent recesses of the online criminal underground. There, the team takes advantage of the very anonymity that makes the dark web unique, which allows them to discretely observe the habits of cyber swindlers.

Some of the information the team has gathered revolves around the dark web's **intricate code of honor**, reputation systems, **job market**, and techniques used by cybercriminals to **hide their tracks from law enforcement**.

We've previously highlighted these findings in an extensive three-part series featured on the Trustwave SpiderLabs blog. But we've decided to consolidate and package this information in an informative e-book that gleans the most important information from that series, illustrating how the online criminal underground works. Knowledge is power in cybersecurity, and this serves as a weapon in the fight against cybercrime.



Where Criminals Congregate

Much like your everyday social individual, cyber swindlers convene on online forums and discussion platforms tailored to their interests. Most of the criminal activity conducted occurs on the dark web, a network of anonymized websites that uses services such as Tor to disguise the locations of servers and mask the identities of site operators and visitors.

The most popular destination is the now-defunct Silk Road, which operated from 2011 until the arrest of its founder, Ross Ulbricht, in 2013. Many platforms still exist and offer a variety of illegal products and services, including drugs, weapons, child pornography, and even murder for hire.

Access to these forums is mostly free. However, the most lucrative ones charge fees for access. Users can communicate in nearly every major language, but a majority of these destinations cater to Russian speakers.

Monetary transactions involve the use of cryptocurrencies, such as bitcoin, which allow visitors to anonymously transfer money, avoiding bank accounts that are traceable and linked to specific individuals.



Similar to legitimate discussion platforms, underground forums enforce codes of conduct to protect members and ensure a minimum level of order and legitimacy. Below is an example of a set of rules from one underground site we investigated:

- 1.** Members are not allowed to engage in threatening behavior toward other members in posts, PMs or profiles. This includes flaming, threats to steal accounts, dox or swat.
- 2.** No short, low-quality posts like "bump," "lol," "roflmao," "thanks" or any repeated characters to defeat the minimum character count.
- 3.** Don't attempt to infect members with trojans, viruses or backdoors.
- 4.** No direct links to infected downloads in posts or profiles.
- 5.** No posting of personal information that isn't yours. This includes any passwords, logins or dumps. Privacy is to be respected here.
- 6.** Signature images can be no larger than 650x200 pixels and 500k size. Animated gifs should not be annoying.
- 7.** You cannot ask for or offer reputation in posts, signatures or PM. This includes encouragement like "rep is appreciated."
- 8.** No adult images, adult links or adult account trading.
- 9.** Multiple accounts will not be allowed unless you are reporting your original account as hacked. Ban evading will result in the permanent closing of your old account and new accounts. No exceptions.
- 10.** Advertising of competing sites is not allowed. This refers to any website with a hacker forum that's similar to HF or has a relatively similar forum structure. Advertising includes signatures, PMs, profiles and posts.
- 11.** No posting of fake programs.
- 12.** No threads or posts begging for donations or requesting loans.
- 13.** All black-hat hacking activity listed on that linked page is forbidden.
- 14.** Read the violations for profile policies and rules in that Help doc.
- 15.** Any rules posted in the forums header must also be reviewed. Some forums have special policies that must be adhered to. Don't post in any forum without reading them.
- 16.** Any marketplace-type threads must be in the Marketplace area. A three-day posting ban and a warning is the penalty for wrong forum posting marketplace threads.
- 17.** No advertising of Discord channels or usernames.



Given the criminal activity occurring on these forums, rules like these are ironic, but needed for site operations to run smoothly.

Some rules, such as “don’t con other members of the forum” are obvious enough. Others, such as disallowing multiple accounts or identities may seem odd in the context of an anonymous forum but are necessary for the reputation system to function effectively. Some members game the reputation system by creating multiple accounts, resulting in fake conversations or reviews.

Though the primary purpose of the underground is commerce, it’s also a community, or a network of communities. Most discussion forums include spaces for off-topic conversations where members banter, form friendships, and discuss current events and hobbies. Arrests of cybercriminals typically lead to a burst of discussion, which can range from expressions of sympathy for the arrested party to conversations about what went wrong and how the arrest could have been prevented.

| | |
|--|---|
| <p>9.04.2017, 19:29</p> | <p>Отправлено #48</p> |
| <p>Цитата(1up @ 9.04.2017, 19:18)</p> <p>Очень странно, что ему приписывают там причастность к выборам и т.д.</p> | <p><i>It's really strange, they're trying to tie him to elections involvement.</i></p> |
| <p>есно! щас еще сделают так что он это подтвердит! что бы потом в новостях писать! вот видите!!! мы же гвоорили что, это из за хацкеров из РФ выборы сфабриковали! это все продуманно было до начала зоворушек и санкций! ведь многие люди не понимают что в монике просиходит совершенно, и видуться на алерты в браузере типо "ваш комп заблокирован"! а на подобное, тем более... глупо, очень глупо, жаль Северу.</p> | <p><i>Sure! They will make him confirm this (intrusion of US elections) so they can write it in the news....</i></p> <p><i>[snip]</i></p> <p><i>.. Feel bad for Severa.</i></p> |



Around major holidays, some underground communities even host charity drives, with beneficiaries including hospitals, orphanages and other people in need. Some charity drives have netted more than USD \$7,000.

Благотворительность под НГ

Каскадный - [Стандартный] - Линейный

Подписка на тему | Сообщить другу | Версия для печати

hackcore 28.12.2016, 19:56 Отправлено #1

exploit

недосягаемый

Группа: Доверенный

Сообщений: 2 786

Регистрация: 20.10.2014

Из: Krung Thep

Пользователь №: 58 100

Деятельность: хакинг

Репутация: 313

(34% - хорошо) +

Я вижу что на форуме все таки остались добродушные люди, люди которые могут и хотят помочь детишкам.

Сейчас у нас рождественские праздники и каждый из нас может сделать одинокого ребенка счастливым. Возможно кто-то посчитает тему мрачной или унылой или скажет что уже такое было, есть найдутся такие люди просьба идты лесом. Кто захочет тот поможем, от себя обещаю организовать пруфы: фото, возможно видео. Предположительно деньги пойдут на одежду, еду, новогодние подарки. Я пока не говорил еще ни с кем, на днях постараюсь объехать несколько детдомов и распросить администрацию в чем они нуждаются.

Нашу новогоднюю акцию уже начали такие юзеры как:

Kokain+up0 - 215\$

Dancho - 100\$

allah - 50\$

12309 - 0.31337 бтс

Lebron - 0.1 бтс

oculus - 400\$

Аноним - 100\$

severa - 100\$

Go101 - 10\$

finistro - 97\$

.....

crbr - 3 btc

Я уже не успеваю вести историю.. смотрите по кошельку движению средств

Так же был получен бтс код на 400\$

Кошелек: 1BN3611pJkqKTtKzTNLNWtZkTXBE1DTWU4

Jabber: arbitr@exploit.im

There are good people on this forum who are able and willing to help children in need. Christmas holidays are coming up and every one of us can help make a lonely child happy.... [snip]...Whoever wants to help can help. I promise all kinds of proof: photos, possibly videos. The money will go towards clothes, food and New Years gifts... [snip] ... This New Year's promotion has already been supported by the following users: [names and donations of members]



Honor Among Thieves: Trust, Reputation and Cooperation

All underground forums and markets struggle with the basic problem of ensuring trust between parties.

Though anonymity is an essential factor for conducting business away from the prying eyes of the law, it also introduces a large degree of risk: Markets break down if participants believe there is a large likelihood that they will be swindled. To solve this problem, underground forums use a complex and interconnected web of mechanisms for tracking participants' reputations and punishing dishonorable behavior.

STARTING AT THE BOTTOM

Most forums offer different levels of access; however, even the lowest levels typically begin with a vetting process like one might experience when trying to land a new job, enroll in college, or join an exclusive club. Candidates must provide profiles from other forums for inspection before they receive access. Administrators can also ask for recommendations from existing forum members. Additionally, some forums use a system in which an existing member can provide a code so a prospective member can acquire limited forum access. In some cases, prospective members can purchase this code.

Restricted access helps maintain anonymity and build a reputation within the underground community.

The site is invite-only! Try to find an invite from the forum: [d\[REDACTED\].onion](#)

Brenda, Nicholas, Joshua, Jerry and Wayne. Who of them is a woman?

[Browse products](#)



ESTABLISHING (AND LOSING) TRUST

In a community of anonymous criminals, a person's word is only as good as other people say it is. Each member accumulates a reputation score based on reactions to their contributions. Members often appreciate useful contributions, such as new exploit tutorials or novel infrastructure setups, which can raise one's reputation. On the other hand, forums do not tolerate attempts to cheat or con other forum members and often ban and/or blacklist violators.

Other ways to tarnish one's reputation in the underground include disrespecting other cybercriminals' content by publishing the details of proprietary or in-use solutions, such as the source code of a tool not intended for publishing.

Administrators and "trusted" members are the dependable inner circle of a forum. Highly trusted members can become section administrators with privileged access to particular areas, and are often called upon to be guarantors. A guarantor acts as an escrow service and facilitates trades between members.

The guarantor receives the goods from the seller and the payment from the buyer. Upon verifying the goods fulfill the terms of the deal, they complete the transaction by forwarding the goods to the buyer and the money to the seller. Members usually expect newly registered users to employ a guarantor for transactions. Well-trusted members, on the other hand, often agree to close deals without using escrow, as they presume the threat of losing a hard-earned reputation is enough to deter bad behavior from either party.

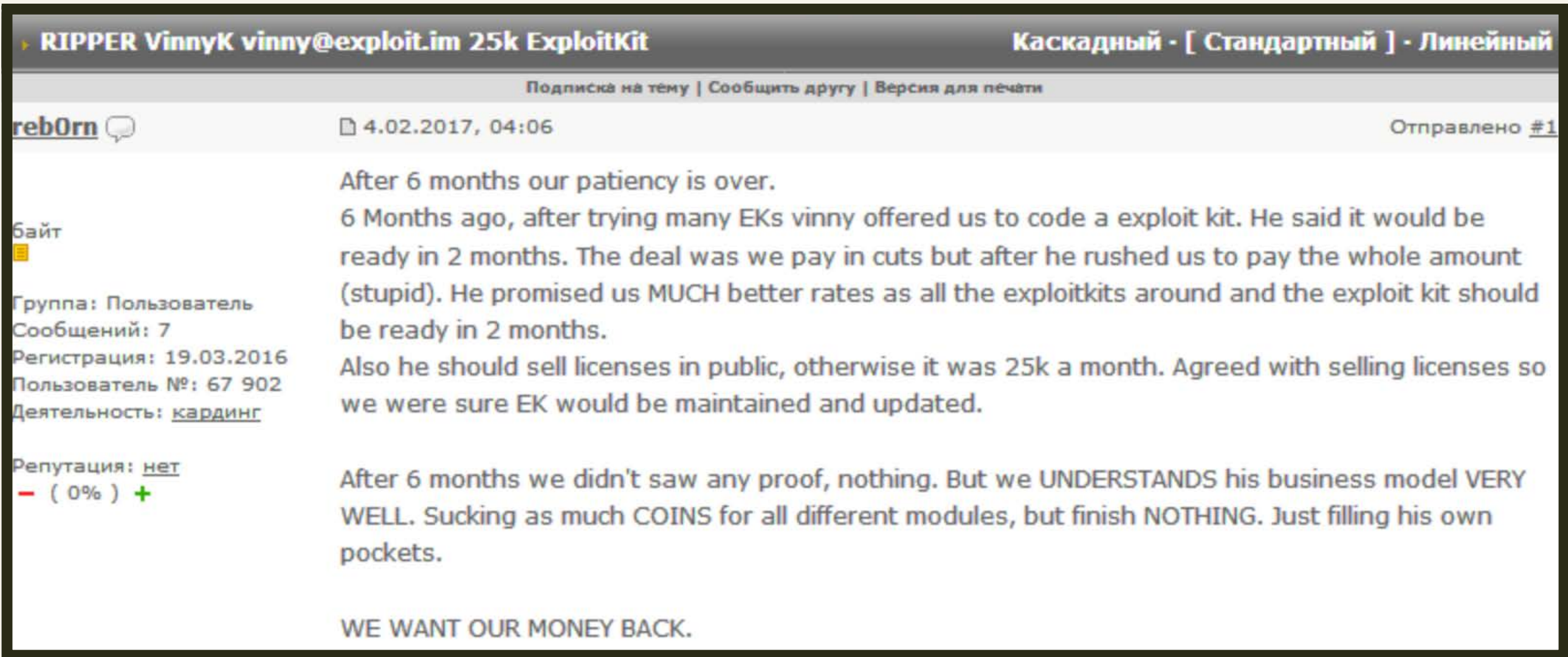
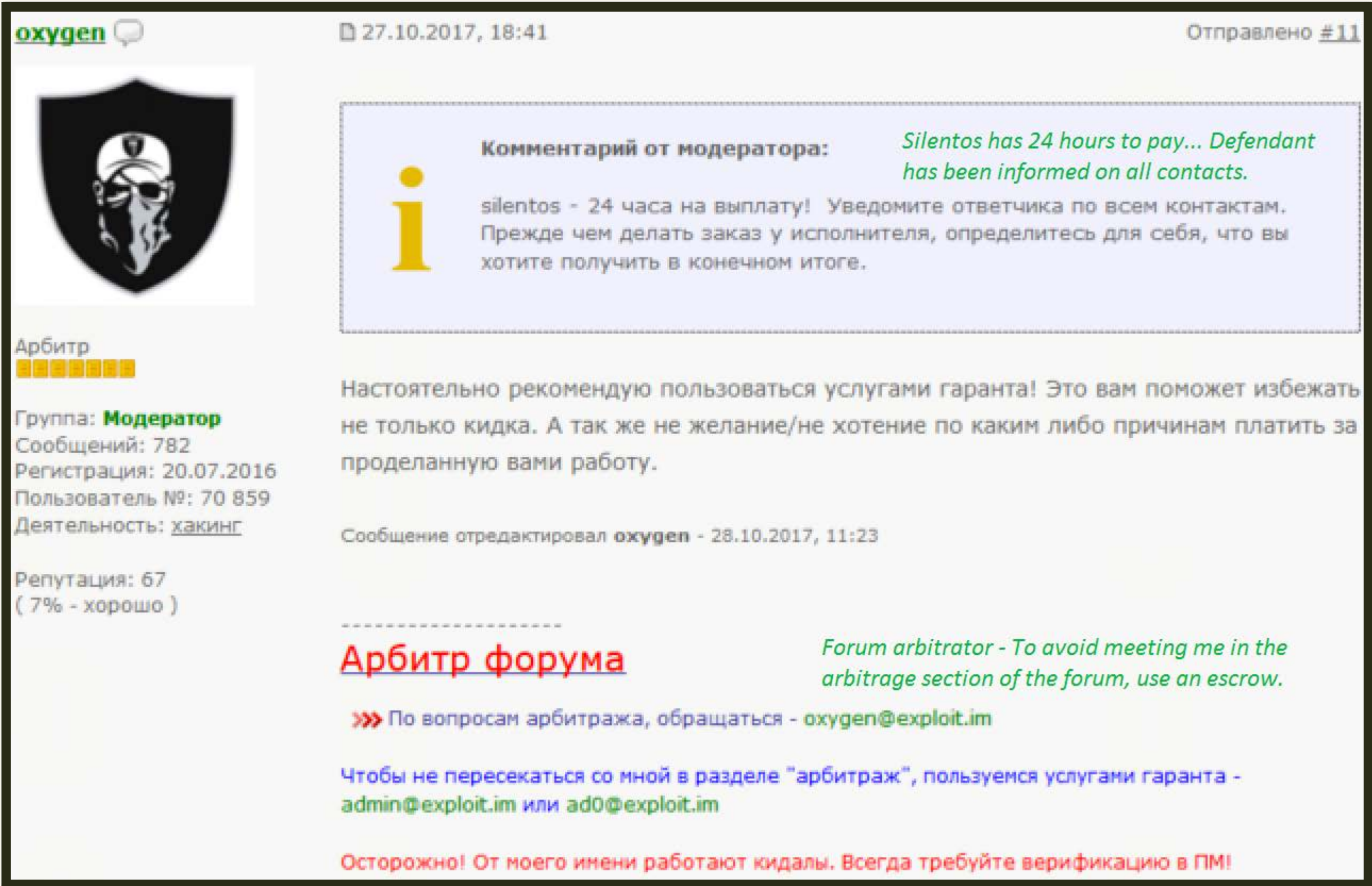
Despite these safeguards, disputes still arise, and, occasionally, two or more members find themselves in a conflict.



To settle disputes, trusted forum members nominate an arbitrator to hear the claims made and facts presented and make a binding decision based on the evidence, similar to a judge in a court trial. In a typical arbitration case, the “plaintiff” creates a new thread in the arbitration section of the forum and provides evidence supporting their claim. The arbitrator then informs the “defendant” of the claim and gives them some time to respond with their own side of the story and any evidence they can provide. If the arbitrator determines the claim is legitimate, they order the parties to take steps to honor their obligations or cancel the agreement. Forums blacklist and/or ban a party that refuses to abide by the arbitrator’s agreement, branding the violator as a “ripper” (scammer) and making the details known to other forum members.

Being blacklisted is the underground equivalent of the death penalty. Underground communities share blacklists, and those blacklisted will find it nearly impossible to transact with anyone anywhere without starting over with a new identity.

In some extreme cases, communities will dox violators, publishing details of their personal identities and invariably attracting the attention of law enforcement.





Criminals for Hire: The Underground Job Market

Many of the schemes cybercriminals run require using paid accomplices, which they can't exactly advertise for on conventional employment websites.

Luckily, the dark web offers many ways for criminal employers and job seekers to find each other and come to terms that satisfy everyone except their victims and the law.

SO, YOU'VE DECIDED TO BECOME A CRIMINAL

Underground job offers typically target college students and other young people by promising “easy money” from the very beginning for positions that require little to no experience.

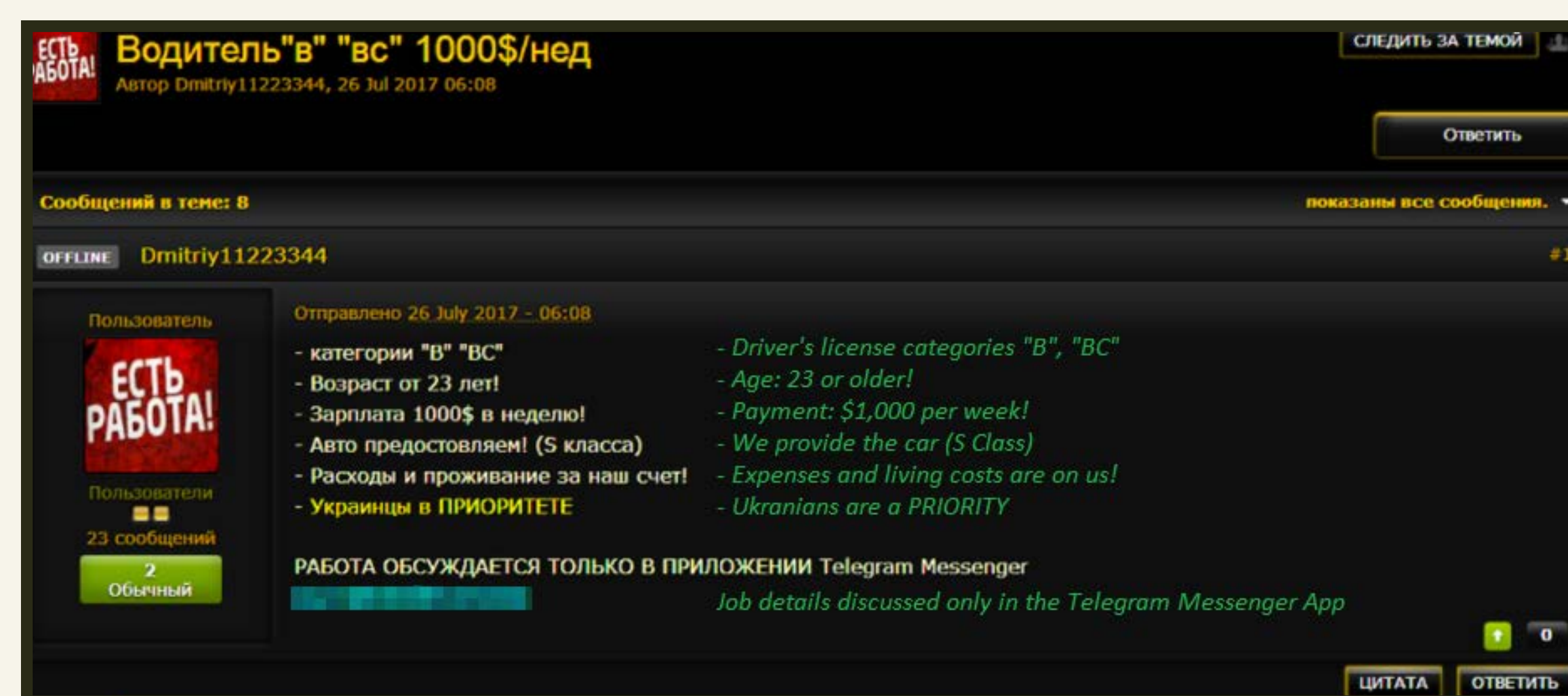
For example, one advertisement we found in 2018 promised potential respondents 400 Ukrainian hryvnia (about USD \$15) per day to spray paint advertisements around major cities. Compare this offer to the local minimum wage of 3,723 UAH (about USD \$140) per month or the highest available student scholarship of 1,660 UAH (about USD \$63) per month. Within one work week, a student could earn more than a scholarship and within two weeks more than a full month's salary at minimum wage. That's an appealing offer for a part-time job with only a minor risk of being punished for vandalism.

Other offers target tech-savvy job seekers for cybercrime positions, promising to provide training for a range of illegal activities.



Even on the dark web, employers and job seekers often avoid explicitly advertising for illegal work, resorting instead to well-understood euphemisms or leaving the details unstated but obvious to those in the know.

For example, this ad appears to be a common everyday job offer for a car driver:



The immediate tip-off is the offered salary of USD \$1,000 per week. Jobs for drivers advertised on legitimate sites rarely offer more than 85,000 Russian rubles (about USD \$1,350) for a month's work.

For the position advertised here, the employer offers the driver more money for just over a week's worth of work, not including the prestigious luxury car and living-expense compensation the underground employee would receive. The next step is to discuss further details via Telegram, a cloud-based instant-messaging and voice-over IP service that allows secure chatting between clients. Further conversation in the thread hinted this position was related to drug delivery.

The main reason underground jobs pay so well is to compensate for the risk of arrest or harm employees may face. The employers themselves also face risk not only from prosecution but also from their own employee. For example, an employee might disappear with a large amount of the employer's cash or valuable property, never to be seen again. To mitigate this risk, underground jobs that involve entrusting employees with valuable assets often require the employee put down a deposit of their own money when collecting the goods. The employee receives a refund on the deposit along with their salary upon completing the job. This helps incentivize employees to do the work and get their pay, rather than take the goods and run.

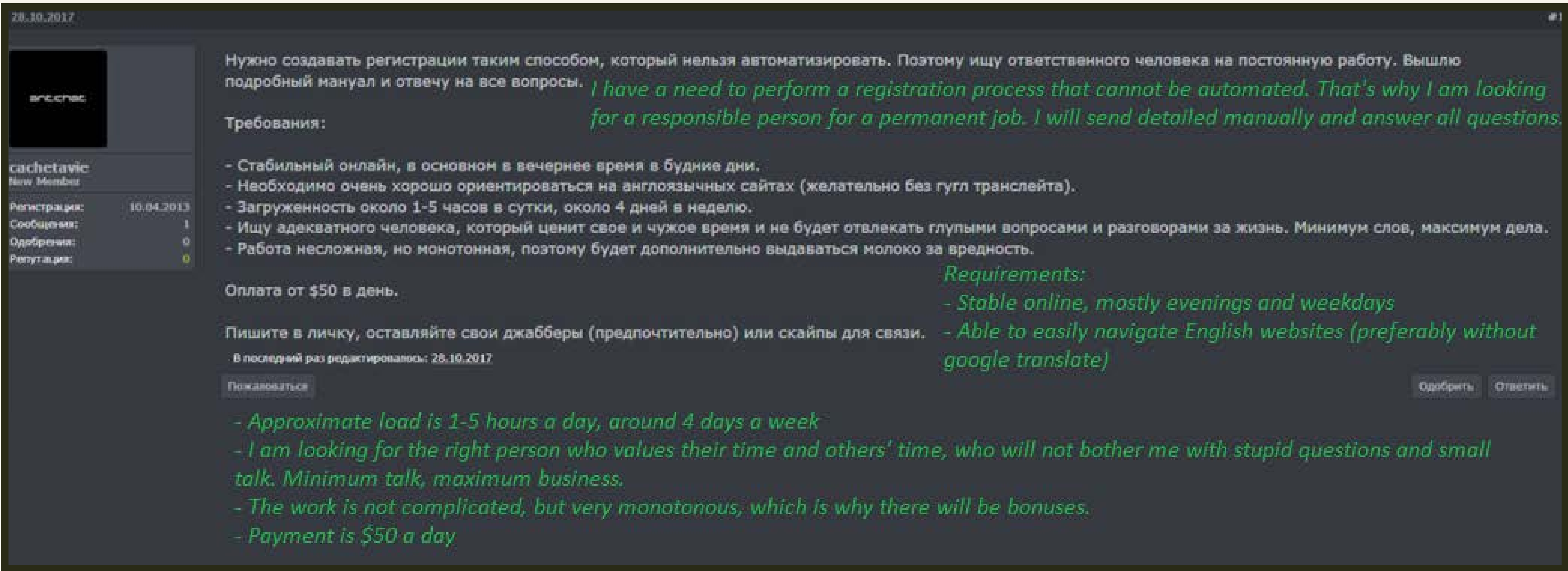
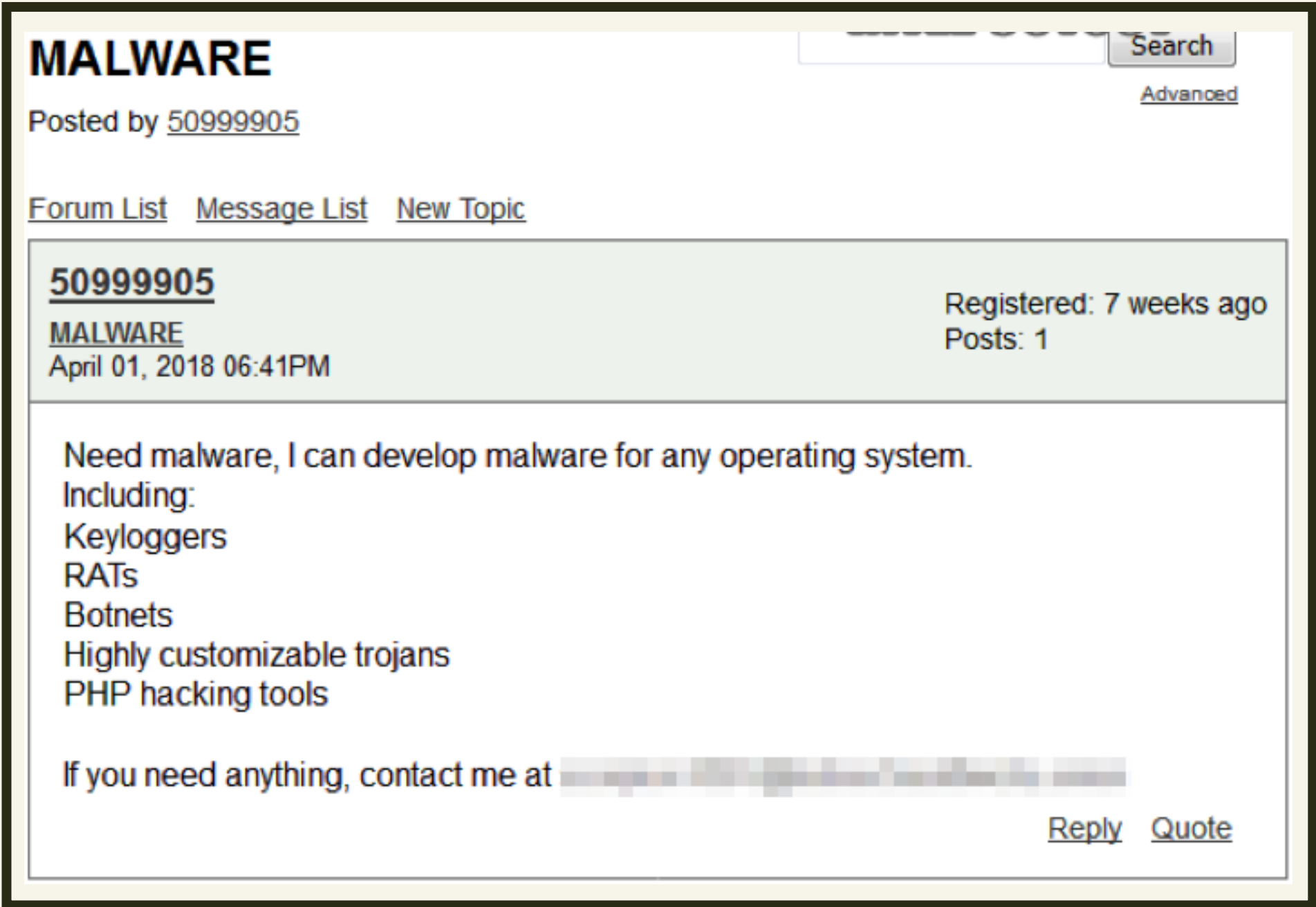


TYPES OF WORK

Whereas finding illegal work in the past often meant cultivating contacts who could point seekers in the right direction, the rise of the dark web has led to spaces where employers and job seekers can openly advertise about a variety of positions, ranging from unskilled manual labor to sophisticated black hat activity. Some of the more common categories we’ve seen being advertised include:

Cybercrime: Unsurprisingly, forums where members buy and sell exploits, credit card numbers, and passwords also feature cybercriminals advertising their skills and availability. Rarely are malware developers and hackers-on-demand represented, but one can find them if you know where to look. The advertisements mostly list the person’s general technical skills and specializations.

More common are advertisements for low-level online work, usually amounting to data entry for CAPTCHA solvers, form fillers, Facebook spammers, bulk account creators and more. These positions require little skill beyond the ability and patience to perform repetitive tasks for lengthy periods.





Moonlighters: As the saying goes, it’s easier to find a job when you already have one. One interesting category of job advertisements targets employees of certain companies or in certain fields that would trade their knowledge or access for extra money.

UNITY → Резюме → Работа для сотрудников Всех Операторов РФ

Страницы 1

Сообщений 1

Farmaцевt

05.01.2018

1

Начинающий

Зарегистрирован: 11.12.2017

Сообщений: 15

Карма: 3

Отправить ЛС

Набираем сотрудников Всех операторов РФ для работы в сфере поиска информации.Мы настроены на долгую и добросовестную работу.Своевременные выплаты

Особенно требуются:
МТС
Мегафон
Йота
Теле2

Оплата услуг достойная!!!

Контакты:
Jabber :
Wickr : (все буквы через английскую раскладку,никаких цифр)

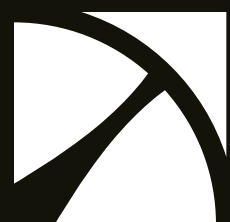
Прием на работу,только через подтверждение на сайте.Не нарвитесь на фейков

We are looking for employees of any cellular operators in the Russian Federation to find information for us. We are looking for long-term quality employees. Payment on time.

Highly needed:
MTS
MegaFon
Yota
Tele2

Fair payment.

Offers like the above require the employee to provide inside information. Offers targeting employees of cellular operators often seek mobile phone usage or location data, typically to track specific people or monitor the progress of an unrelated criminal operation. Criminals frequently pursue employees of banks and postal systems to assist with bank drops or intercept packages with offers of compensation that dwarf what the employees earn from their legitimate jobs.



Compensation starts at 200,000 Russian rubles (about USD \$3,200) per month, more than five times the amount an entry-level bank clerk can expect to make in the targeted geographic area. This is a tempting proposition for an unethical bank employee that includes a serious risk of imprisonment.

Advertisements also target security professionals and government employees for unspecified long-term “collaboration” and offer different rates of compensation for “white” (legal) information and “black” (illegal) information:

ddfeder

Пользователь

Регистрация: 10 дек 2017

Сообщений: 15

Симпатий: 0

Пол: Мужской

Приветствую!

Bank employees of any bank needed. Sberbank, VTB, Alfa are a priority. Remote job, any city. 1 hour per day. Daily payments, 200k RUB per month. Our best employee earned 370k last month.

All your questions write in telegram.

Требуются сотрудники любых банков. Сбер, ВТБ, Альфа в приоритете. Подработка удалённо. Любой город. Всего 1 час в день.

--

Выплаты ежедневно. В месяц от 200т.р.

Наш лучший работник в прошлом месяце заработал 370 тысяч.

--

По всем вопросам писать в Telegram:

--

Актуально! Пишем, не стесняемся. Тут бываю редко, пишите в Telegram.

UNITY → [Вакансии](#) → Требуется сотрудники ВСЕХ банков (СБ), ФССП и налоговой.

Страницы 1

Сообщений 4

MaxPayne

14.09.2017 (11.11.2017 отредактировано Dredd)

1

Гость

Зарегистрирован: 31.05.2017

Сообщений: 2

Карма: 0+

Отправить ЛС

Приветствую!

Если ты работаешь в службе безопасности банка, в ФССП или налоговой, либо же имеешь таковых среди своих знакомых, то предлагаю сотрудничество. Перспективное. Долгосрочное.

Работа подразумевает передачу нам запрашиваемой информации (есть как белая тема, так и черная).

Выхлоп для Вас- от 400к руб за 2 недели (по белой теме) и от 50к в день- по черной.

[Удалено. Заведите себе джаббер и рдр-ключ. Dredd]

Сообщить модератору

Цитировать

Greetings!

If you or your friends work at bank security, Federal Services of Court Bailiffs, or a tax agency I am offering collaboration.

Long term.

The job entails providing us with requested information (black or white).

From 400k RUB for two weeks (white info), and from 50k RUB per day (black info)



Manual labor: Cybercrime operations often extend into the physical world, and a large subset of underground jobs fall into the general category of moving something from one place to another. The most popular job, both in offers and for those looking for employment, involve “drops.”

A dropper receives property (cash, physical goods or anything else they can convey) and then redirects it to a target point or to another dropper. (See the “Money Laundering” section for more on droppers.)

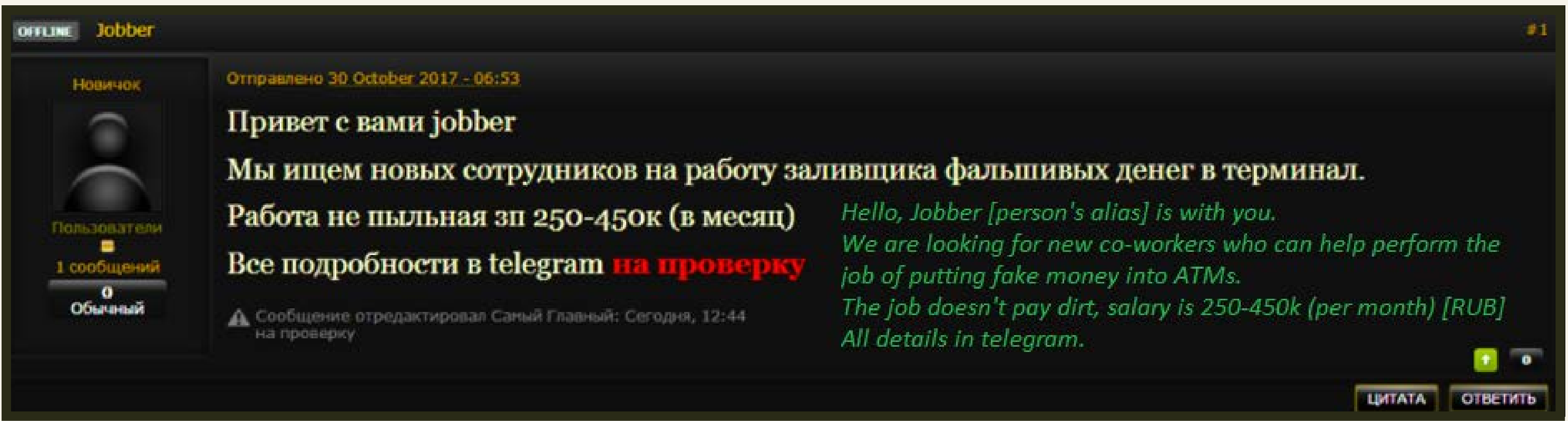
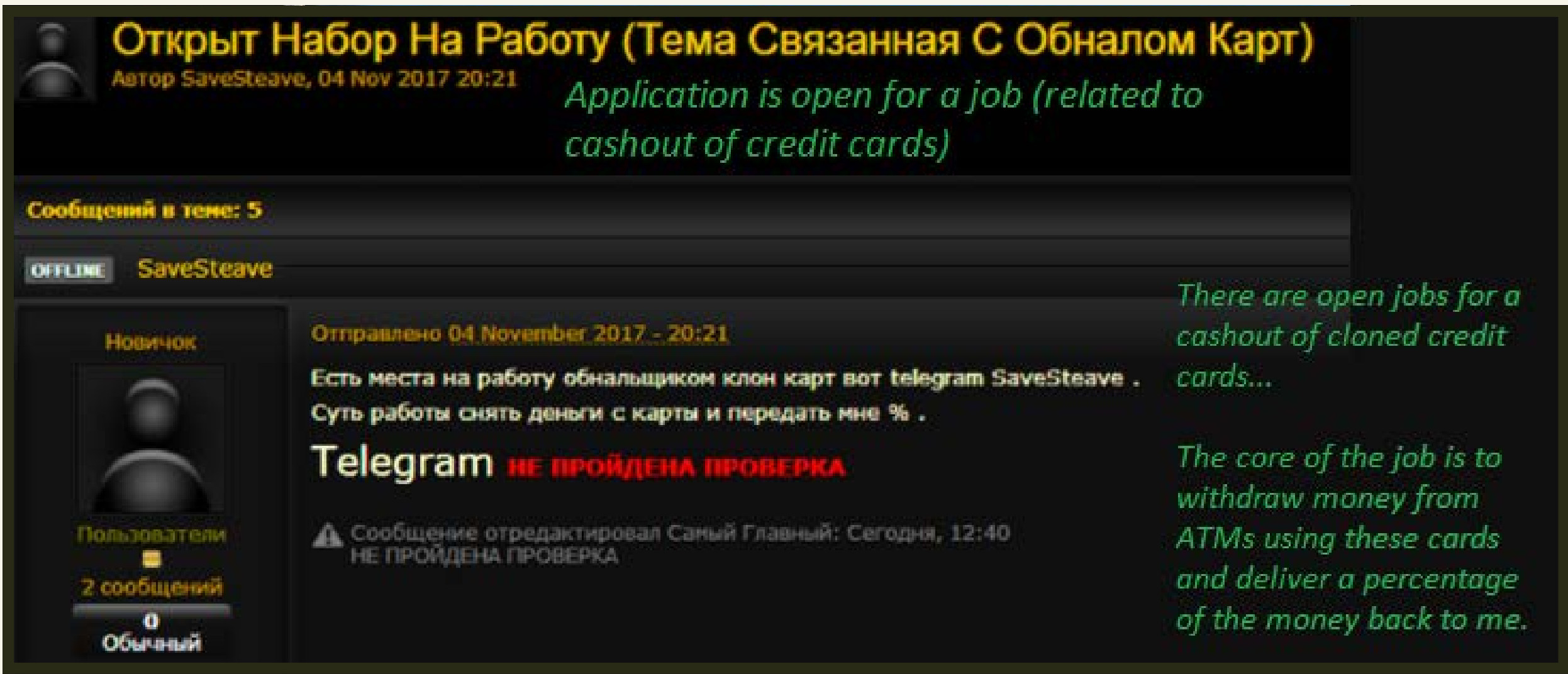
Droppers, who make it more difficult to trace the flow of a criminal operation by separating the source of goods from their destination, often transport goods across international borders to complicate law enforcement efforts.

Dropper positions are available worldwide and range from largely unskilled “mule” jobs to specialized positions that require specific skills or access, such as a legitimate job filling ATMs with cash.

Among the more commonly seen advertisements are those for “cashouts,” who take delivery of stolen or forged credit and debit cards and use them to withdraw money from ATMs and then return a portion of the proceeds to the employer.

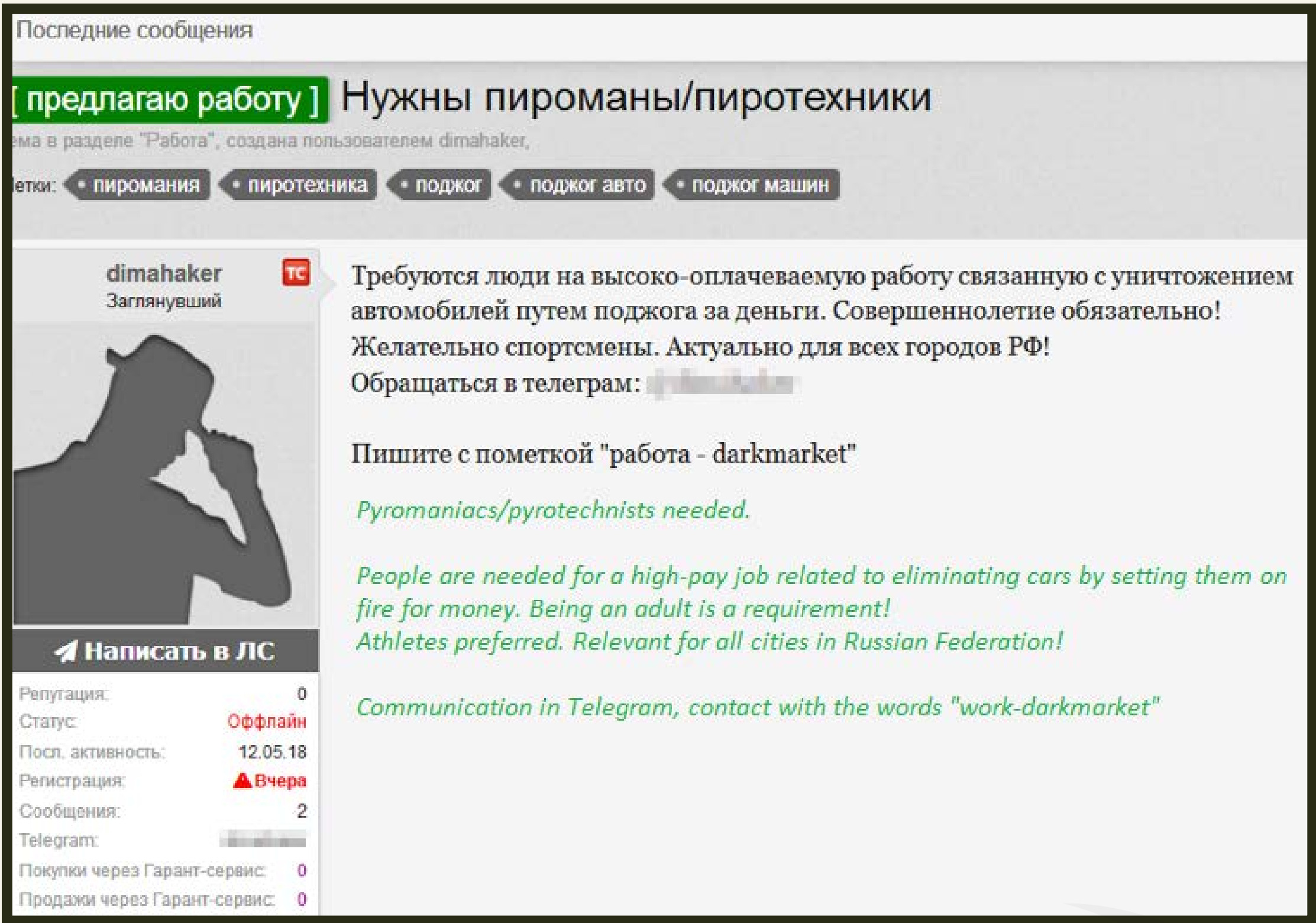
Dropper jobs, which are particularly risky in the underground due to the possibility of discovery and capture, commensurately usually pay well. This advertisement seeking ATM fillers offers between USD \$4,000 and \$7,200 per month, which would be a generous salary nearly anywhere

and represents a lucrative opportunity for working-class job seekers in Russia:

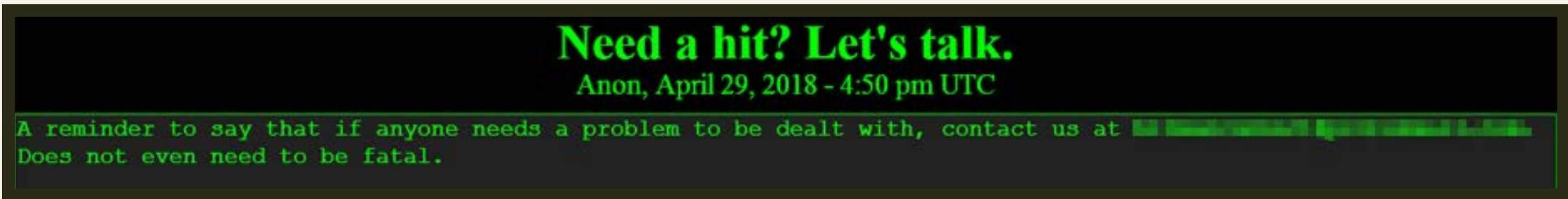




Traditional crime: Many of the jobs discussed here have only come into existence since the rise of the internet, but the underground job market also offers plenty of opportunities for advertising and procuring the services of more traditional criminal professions. If you specialize in setting other people’s cars on fire for money, for example, there’s a position for you:



Plenty of less-conspicuous opportunities are available as well. Advertisements for drug mules, smugglers, insurance scam artists and similar criminal services abound on dark markets. Alongside these relatively nonviolent ads, however, one can also find solicitations for more serious crimes such as assault, kidnapping and even murder.

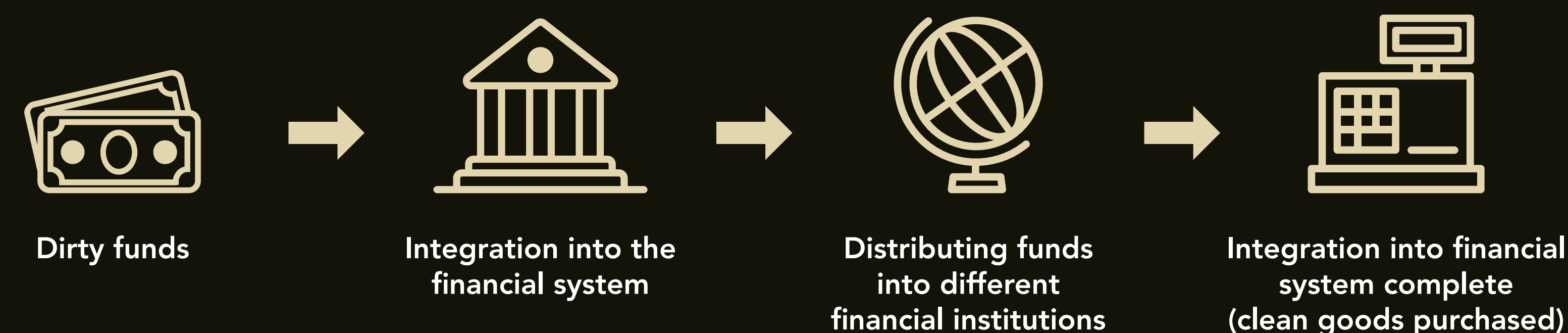




Money Laundering: Getting Rid of the Evidence

Any cash earned through carding, fraud or other illegal schemes where the origin of the money cannot be explained without revealing the criminality behind it is referred to in the underground as “dirty money.” Essentially, dirty money is useless to the criminal who does not want to attract the attention of the authorities by spending large sums with no apparent source.

To make use of stolen funds, the miscreant must find ways to obfuscate the source of the treasure. They usually accomplish this through money laundering – in the popular vernacular—which can make the funds appear to come from legitimate activity.



Money laundering is a significant international problem. The United Nations Office on Drugs and Crime (UNODC) estimates the amount of money laundered globally in one year is two-to-five percent of global gross domestic product (GDP), or USD \$800 billion to \$2 trillion. It’s an age-old concept that is familiar to consumers of crime-themed novels, films and television shows. Many of the money laundering schemes cybercriminals use derive from techniques long used to conceal the source of profits from the sale of illegal drugs and other contraband.

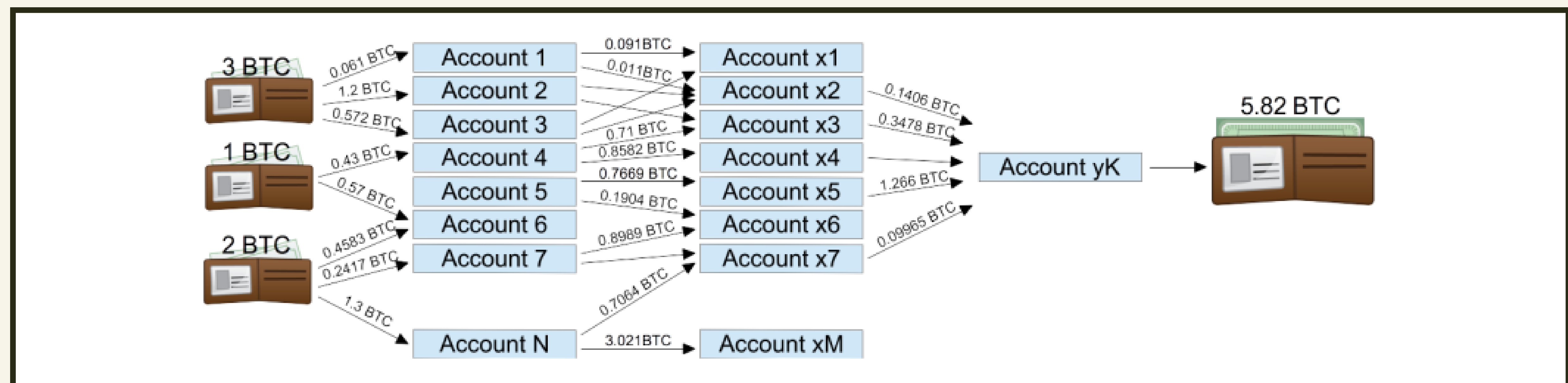
True to form, however, cybercriminals put their own spin on the practice by developing new high-tech tricks that depend on cryptocurrencies and services such as Uber and Airbnb. Money laundering on the dark web has evolved into its own cottage industry, often led by criminals with extensive banking and financial backgrounds who know the ins and outs of staying ahead in the game.



COIN LAUNDRY

As internet-based monetary systems designed around anonymous transactions, cryptocurrencies naturally form the backbone of money-laundering schemes on the dark web. But even using anonymous cryptocurrency doesn't fully protect a criminal from the law. Many cryptocurrencies, including bitcoin, allow anyone to inspect the contents of a wallet with a known ID. Moreover, the nature of the blockchain, a distributed record of transactions, means law enforcement can monitor transactions even of newer cryptocurrencies that have additional privacy and security features.

The simple mistake of using a wallet ID, a unique identifier, filled with stolen cryptocurrency to shop online with delivery to a home address can result in a different kind of knock on the door. These inherent problems led enterprising cybercriminals to develop a new kind of underground service – the cryptocurrency tumbler, or mixer.



Mixers are a popular way of anonymizing and cleaning dirty bitcoins. The principle idea is to divide the currency among multiple accounts, transfer the funds among several more accounts and eventually collect the total amount (minus a fee) to one external, newly-created clean account. To hamper outside investigators, criminals transfer the funds between wallets in unequal amounts, as shown above. Because of the sheer volume of small transactions made daily within the blockchain, the mixer transactions become lost in the noise of all the other simultaneous transactions, which effectively breaks the connection between the crime and the reward.



DIRTY DROPS AND CLEAN PICKUPS

This approach bears some resemblance to the use of droppers, described earlier, who earn money delivering goods from one party or location to another and make it more difficult for authorities to tie a crime directly to its perpetrator. Droppers operate in the virtual and physical worlds to obfuscate the source of ill-gotten gains so criminals can use them undetected.

For example, a cybercriminal might wish to use stolen credit-card credentials to buy goods at an e-commerce site. If the owner reported the card as stolen, investigators likely will check the delivery address, which could expose the criminal to prosecution. To avoid this, the criminal is likely to pass the credentials to a dropper who will act as a straw buyer who purchases the goods and forwards them to the criminal. More advanced cybercriminals or services in this field will use a chain of droppers to further encumber the process of tracing the goods back to the dirty money.

Underground money-laundering specialists advance this scheme further by having the dropper send the purchased goods not back to the criminal, but to an uninvolved third party who may not be aware they are taking part in a crime. This is an individual who was lured to an online storefront, typically through an advertisement on a dark web search engine, that offers huge discounts on popular consumer products.



Y10 Apple iPhone X

| Quantity | Capacity | price from USA \$ | price from EU € |
|----------|----------|--------------------|-----------------|
| 100pc | 256GB | \$42000(\$4200/pc) | 42000€(420€/pc) |
| 100pc | 64GB | \$35000(\$3500/pc) | 35000€(350€/pc) |
| 10pc | 256GB | \$5400 (\$540/pc) | 5400€ (540€/pc) |
| 10pc | 64GB | \$4500 (\$450/pc) | 4500€ (450€/pc) |
| 5pc | 256GB | \$2850 (\$570/pc) | 2850€ (570€/pc) |
| 5pc | 64GB | \$2375 (\$475/pc) | 2375€ (475€/pc) |
| 1pc | 256GB | \$600 | 600€ |
| 1pc | 64GB | \$500 | 500€ |

Detailed item information



Y13 Apple iPhone 8

| Quantity | Capacity | price from USA \$ | price from EU € |
|----------|----------|-------------------|-----------------|
| 100pc | 256GB | \$31500(\$315/pc) | 31500€(315€/pc) |
| 100pc | 64GB | \$29400(\$294/pc) | 29400€(294€/pc) |
| 10pc | 256GB | \$4000 (\$400/pc) | 4000€ (400€/pc) |
| 10pc | 64GB | \$3800 (\$380/pc) | 3800€ (380€/pc) |
| 5pc | 256GB | \$2135 (\$427/pc) | 2135€ (427€/pc) |
| 5pc | 64GB | \$2000 (\$400/pc) | 2000€ (400€/pc) |
| 1pc | 256GB | \$450 | 460€ |
| 1pc | 64GB | \$420 | 430€ |

Detailed item information



Y12 Apple iPhone 8 Plus

| Quantity | Capacity | price from USA \$ | price from EU € |
|----------|----------|-------------------|-----------------|
| 100pc | 256GB | \$35000(\$350/pc) | 35000€(350€/pc) |
| 100pc | 64GB | \$31500(\$315/pc) | 31500€(315€/pc) |
| 10pc | 256GB | \$5400 (\$540/pc) | 5400€ (540€/pc) |
| 10pc | 64GB | \$4500 (\$450/pc) | 4500€ (450€/pc) |
| 5pc | 256GB | \$2425 (\$485/pc) | 2425€ (485€/pc) |
| 5pc | 64GB | \$2175 (\$435/pc) | 2175€ (435€/pc) |
| 1pc | 256GB | \$490 | 500€ |
| 1pc | 64GB | \$450 | 460€ |

Detailed item information

The iPhone X have a high demand and will not be available until 3/Nov/17. It will be sent by order of payment, the bulk orders have priority.



Apple Pack

CardedStore@icloud.com
CardedStore@icloud.com
CardedStore@icloud.com

LXXX TEAM

| | |
|---|----------------|
| B75 iPhone 8 plus 128 Gb + Watch 3 + iPad Pro 12.9 (w+c) + Macbook pro 15" 2.5GHz | \$1990 1980€ |
| B74 iPhone 8 plus 128 Gb + Watch 3 + iPad Pro 9.7 (w+c) + Macbook pro 15" 2.5GHz | \$1890 1880€ |
| B73 iPhone 8 plus 128 Gb + iPad Pro 12.9 (w+c) + Macbook pro 15" 2.5GHz | \$1740 1730€ |
| B72 iPhone 8 plus 128 Gb + Watch 3 + Macbook pro 15" 2.5GHz | \$1590 1580€ |
| B71 iPhone 8 128 Gb + iPad Pro 9.7 (128 GB w+c) + Macbook pro 15" 2.5GHz | \$1590 1580€ |

Available only for a limited time at this price. Offer ends: 31/12/2017

A criminal actually runs this storefront that cleans money from legitimate buyers and fulfills their orders using goods purchased with dirty money, again breaking the chain between the crime and its beneficiary.

The criminal nets less profit than they would otherwise due to the steep discount the legitimate buyer receives, but the lowered risk is often worth the discrepancy. Of course, sometimes the criminal simply takes the legitimate buyer's money and doesn't deliver anything.



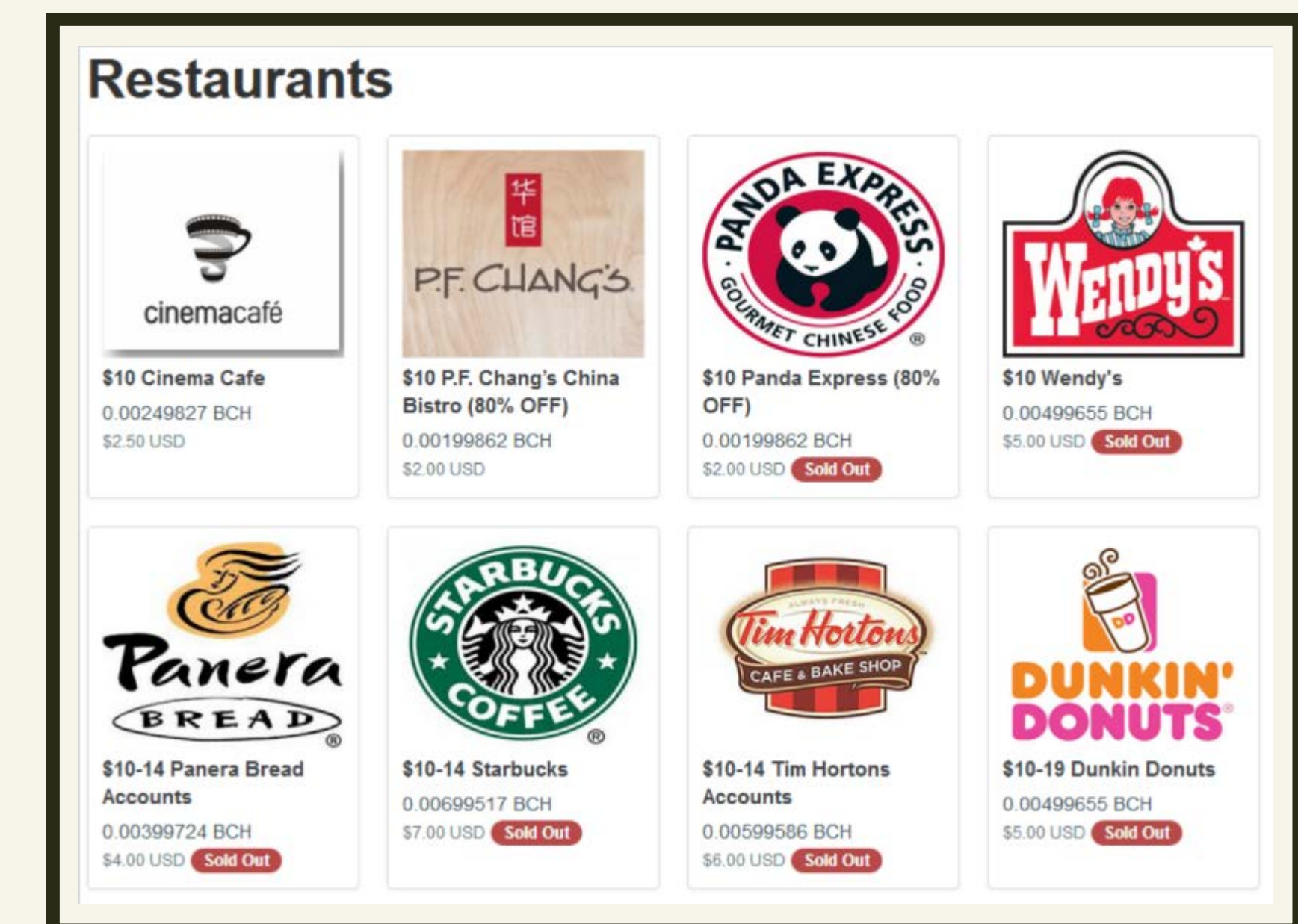
OTHER TECHNIQUES

The money laundering schemes cybercriminals use run the gamut from low tech to high tech and often piggyback on trends in business and popular culture. Other techniques include:

Gift cards: Gift cards and codes for stores and restaurants have become big business.

Customers like them because they make it easier to buy gifts for friends and acquaintances, and businesses like them because they drive customers through their doors. Why do cyber crooks like them? Because they provide yet another way to clean dirty money clean – often with the assistance of unwitting accomplices.

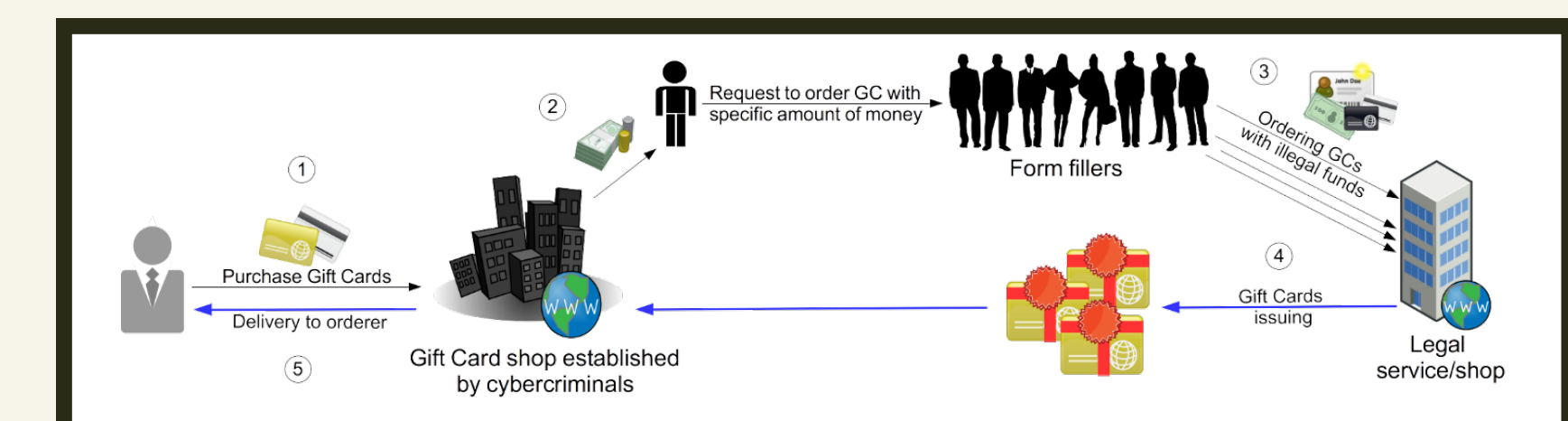
The idea is to use stolen credit-card data to buy gift cards and then immediately push the cards to the underground market or purchase goods with them for reselling. Selling gift cards directly carries risk for the cybercriminal and the purchaser, as merchants are likely to invalidate cards immediately if they discover someone fraudulently purchased cards.



To compensate for the risk, the criminal typically offers the cards at a steep value, often 75 percent or more off the face value, depending on the seller's confidence in the card's validity. Gift cards judged less likely to be invalidated go for a higher price.

Shops on the dark web sell gift cards for an impressive variety of merchants. Cards for online merchants are easiest to transact because they can be exchanged in the form of codes one can use at e-commerce sites; but ads for physical cards from walk-in establishments, such as restaurants, are also common. Cybercriminals also use legitimate websites, such as r/giftcardexchange on Reddit, and services where people trade gift cards they don't want for ones they do.

There are also "on-demand" gift-card storefronts on the dark web, where a customer can order cards specifying the store and amount desired. The criminal then deploys form fillers to order the cards or codes using stolen funds and delivers them to the purchaser after a delay of a few hours or days.






Shell corporations: One technique we’ve seen more frequently on the dark web involves using “legitimate” registered companies as links in the money-laundering chain. Typically, these companies exist only on paper and are created and staffed with corporate directors only as needed. Although, occasionally, a purchaser will surface looking to buy a company with a clean record and a history of real operations, as with this urgent request:

Partners in the field: The rise of peer-to-peer services, such as Uber and Airbnb, has created an opening for criminals to launder money with the help of complicit partners who sign up to make money through the ridesharing and vacation rental services.


In a typical example, a criminal would book a stay with an Airbnb host recruited through the underground market and pay with a stolen credit card. The criminal would never actually show up at the rented property, of course, and the host would pay the criminal a percentage of the payment they receive from Airbnb.

This technique was used heavily with “drivers” of the Uber ridesharing service – who never need to get behind the wheel – using GPS spoofing software to take criminals on nonexistent rides paid for with stolen money. Uber used improved anti-spoofing and fraud-detection techniques to crack down on such schemes, but criminals adapted by relying more heavily on actual drivers with established records working for Uber.



Daspo
 Интересующийся

30 Окт 2017#1

Срочно куплю компанию с оборотом не меньше 200 млн, прибылью не меньше 3 млн год, со всеми отчетностями, без смены, регион любой!!!
Телеграмм 
P.s.покупку и передачу мне ООО рассматриваю только в МСК!!!

I will urgently buy a company with a turnover of at least 200 million , with a profit of at least 3 million a year, with all reports, without changes, any region !!!

...

I consider buying and transferring LLC in Moscow only!!!

Posted at: 2 days ago
 Views: 67

ищу хостоводов airbnb [45755](#)
0.10 BTC / Per project

Other

Ищу людей имеющих реалхосты данной конторы

I’m looking for Airbnb hostdrivers (managers of Airbnb hosts)
 I’m looking for a people who have real hosts from this company



Why You Should Care

The cybercriminal underground borrows institutions, structures and customs from both traditional organized crime and the world of legitimate e-commerce. This maintains a functioning underground economy that uses the power of networked communities and the cover of anonymity to find opportunities for illicit profits that never could have existed even a decade or two ago.

Although clever, a majority of these tactics are not undetectable and have led to arrests and prosecutions of many notable cybercrime figures, most of whom placed too much faith in their ability to thwart law enforcement agencies and the white hat security community.

While your organization may have the proper controls in place to limit employees from accessing the dark web, it's still very important to understand what's out there and how it works. Understanding your enemy will only help you understand your own threat posture, which ultimately helps you determine your **cyber risk tolerance**. Familiarizing yourself with the threat landscape is just one of the foundational tenets that leads to locking down your own environment. It helps assess your approach to cybersecurity and decide if implementing the basic best practices is enough, or if **it's time to get adaptive** and partner with a **trusted security advisor**.

Trustwave SpiderLabs researchers continue to keep tabs on the underground as a vital part of its **mission to protect its customers** and make the online world safer. **Stay tuned for new posts on our blog** that feature the latest details on this topic.



trustwave.com