Nethone

Fraudster Dictionary

Learn the slang and operational techniques of online payment fraudsters

Table of Contents

English Language Sphere

Russian Language Sphere

Intro

Going up against online fraudsters is a tough battle. There isn't one rule that can help you win it all, but there are certainly some crucial steps each fraud specialist should undertake.

Anti-fraud tools are a "must-have", but a more sophisticated approach is to **understand the behaviour and language of your opponent**. However, 75% of fraud analysts admit that they do not research and collect evidence from the darkweb.

We totally understand that. Digging through the darknet is a time-consuming job, and it's hard to keep up with evolving criminal threats and technological advances. It's also a risky activity. If you're not experienced, you may find yourself in cyber trouble.

We prepared a gift for you. Our team of Profilers infiltrated the darknet, followed and understood every detail about the fraudsters' community, so you don't have to do it. We gathered it all into one piece, and now we are handing it to you.

The Fraudster Dictionary ebook will give you **deep insight into the darknet reality** and will teach you fraudsters' slang, both from English and Russian language sectors. Those are the two most powerful language groups in the darknet, and each one of them uses different slang and techniques.

In the second part of the publication, we focus on **deep profiling of a fraudster. You can find examples of fraudsters' characteristics and techniques** discovered by our researchers, that help fraud prevention systems detect unwanted users.

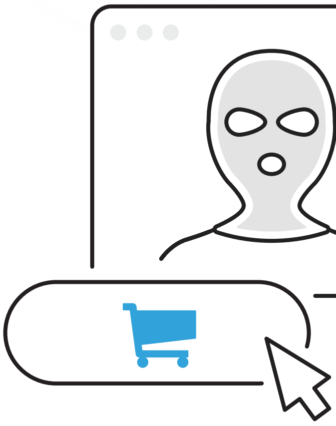
We hope this publication will become an everyday resource for your fraud prevention work.

Let's begin!

Step 1: Learn the language. Dictionary.

Scammers use specific slang to communicate and commit online payment crimes which already gives a broad understanding of their operational techniques. Learn the most common phrases.

English Language Sphere



A

Altcoins

/ɑlt kɔɪnz/

Alternative coins. Slang name for all cryptocurrency other than BTC.

Anonymity Checker

/ænəˈnɪmɪti ˈʧɛkər/

When any user enters an eCommerce website, the merchant can see many details about the visitor. Before the attack, the fraudster needs to ensure that his browser and connection configuration will not seem suspicious to the system. For this purpose carders use **anonymity checkers**. On such websites, anybody can check his browser version, user agent, type of operating system, plugins in a browser, IP address, IP presence on blacklists and many more. Popular checkers are whoer.net and browserleaks.com.

If the fraudster does not like certain information (e.g. that the website shows his real IP), he may try to change it. Imagine he knows that the owner of the stolen account/card is using a Macbook and the anonymous checker shows that the fraudster is using Windows. In that case, the cybercriminal may see the inaccuracy and react to it.

Automatic Vending Cart (AVC)

/ɔtəˈmætɪk ˈvɛndɪŋ kɑrt/

Automatic Vending Cart (AVC) is an automated "click and buy" website selling compromised data, which operates in the darknet as well as in the Clearnet. Most AVCs sell stolen credit cards (fullz, dumps), but there are also AVCs that offer stolen accounts, travel points and anonymity tools.

To make the process of purchasing credit cards more comfortable for the fraudster, AVC websites have filter features that help carders find "the right credit card" they need. A fraudster can filter by price, BIN, card type, bank, country, state (only for the USA), city, zip code, reseller and base (credit cards are placed on AVCs in big batches consisting of thousands of cards, every set has its name). There is also an option to find cards with wanted personal data like phone, email, SSN, date of birth, mother maiden name, cardholder IP, address.

After receiving a payment buyer immediately and automatically receives bought data.

AVS

/eɪ-vi-ɛs/

Address verification system. Another phrase from the financial industry used by fraudsters. It is an operating mode used by the processor to confirm that the legitimate owner, in fact, carries out a card transaction. It uses the billing address entered in the registration process and compares it to the one registered with the credit/debit card company. If they are not similar, then the transaction will be declined. For this reason, crooks buy fullz and registered accounts with the details. Also, many shops won't ship to addresses other than given in the bank as billing address.

B

BIN

/bɪn/

A term is well known among the bank and credit card industry.Knowledge of what a BIN is and how to use it is also the basis for carders. Bank Identification Number is the first six digits of the credit card number. BIN determines card issuer, card type, level of security (for example the presence of 3D Security), country of origin, and sometimes even bank regional branches. Knowing the cardholder state of origin, even without the address, carder knows from which country he should connect to e-shop to be successful.

Sometimes fraudsters buy a card from Germany and try to connect to a shop from India, but that's where the antifraud system enters. It will detect that mismatch and decline the transaction.

Bulletproof hosting

/ˈbʊlətˌpruf ˈhoʊstɪŋ/

Fraudsters who run their services in the darkweb also need hosting services. Sure, they could make everything by themselves, but most of them are not skilled enough. So they need professional hosting servers that are called **bulletproof**. That means hosting providers won't cooperate with law enforcement authorities (lea). Even illicit or strongly unethical content will find their place there. Usually, such servers are located in countries that reluctantly cooperate with lea from other countries, especially from the West.

Real darknet stories

Hosting servers inside a military bunker

In September 2019 German authorities arrested seven people in connection with the raid of a bulletproof hosting provider "CyberBunker" located in Traben-Trarbach, Germany. The provider supported multiple child porn, cybercrime and drug markets with hundreds of servers buried inside a heavily fortified military bunker.

Investigators believed the 13-acre former military facility served a number of darknet sites, including: the Wall Street Market; the drug portal "Cannabis Road;" and the synthetic drug market "Orange Chemicals." German police seized $41 million worth of funds tied to these markets, and more than 200 servers.

For at least two of the men accused in the scheme, Herman Johan Xennt, and Sven Kamphuis, this was their second bunker-based hosting business. CyberBunker 1.0 facility was a lab used to produce the drug ecstasy/XTC. In 2003 Xennt and others were denied a business license to continue operating in the bunker, and they were forced to resell servers from a different location — even though they bragged to clients for years to come about hosting their operations from an ultra-secure underground bunker.

Between 2012 and 2013, Xennt purchased a new bunker in Traben-Trarbach, and the CyberBunker was reborn.

Kamphuis was later arrested in Spain on the DDoS attack charges. He was convicted in The Netherlands and sentenced to time served, which was approximately 55 days of detention prior to his extradition to the United States.

Herman Johan Xennt was believed to have links to organized crime. He has been seen frequently associating with another man: an Irish mobster named George "the Penguin" Mitchell, listed by Europol as one of the top-20 drug traffickers in Europe and thought to be involved in smuggling heroin, cocaine and ecstasy.

Source: krebsonsecurity.com

Carding

/ˈkɑrdɪŋ/

It's a process of using stolen credit cards to make a purchase. Fraudsters who use this technique are called carders. There are two different types of carding: real and virtual. In the first one, the carder uses a forged credit card – a plastic card with loaded data from a stolen credit card. This fraud is also called in-store carding.

The second type of carding is a virtual one and doesn't require a physical item but just its data: number, validation date and security code. Virtual carding is easier than in-store for many reasons:

- everything is done online
- carder can card shops from all around the world
- no special equipment is needed to load data on physical credit cards
- it's just safer. When something goes wrong with the transaction, it is only cancelled, and the card is burned.

Fraudsters increasingly choose virtual carding than in-store.

Cashout

/kæʃ aʊt/

The point in all fraud attacks is to earn money that will be usable. It is child's play to buy a stolen credit card, but it is much more difficult to withdraw money from it. To cashout, stolen credit cards is to transfer money and make them easy and safe to use. Carders often prefer to cashout by buying merchandise similar to real money, e.g., cryptocurrencies, gift cards, loyalty points.

When a fraudster buys stolen bank accounts, he also needs to cashout these accounts to get money.

Cardable websites

/ˈkɑrdəbl ˈwɛbˌsaɪts/

Fraudsters are aware of anti-fraud systems, 3-D Secure and other security measures undertaken by online merchants. But they also know that not the whole eCommerce sector has implemented those solutions. Carders (scammers) describe such websites as "easy cardable", and they exchange information about them.

Forum administrators show examples of such sites to make their forum more attractive for carders. Regular users also share such information to gain a reputation in crooks society.

Credit card checkers

/ˈkrɛdət kɑrd ˈʧɛkərz/

When a carder buys a stolen credit card, he's never sure if the card hasn't been blocked already. Cybercriminals have to be 100% sure that their crime tool is usable and will not cause them trouble. To check that they use "credit card checkers".

In the past, it was a software application that used credit card data to perform 1 cent transactions. However, finance security departments noticed that when a large one follows 1 cent transactions, it is probably a fraud. They started to red-flag those payments, and such checkers are mostly useless now.

Currently, card checkers use, for example, paid accounts with free trials where users have to add a valid credit card. Another method is to send small donations to charity organisations. Such entities can play an important, mostly unaware, role in carding and money laundering.

Criminal forums

/ˈkrɪmənəl ˈfɔrəmz/

There are various criminal forums on the Internet. Some of them are available only in the darknet, but many are also available in the clearnet. There are three main illegal subjects on cybercriminal forums: frauds, hacking/cracking and drugs.

There are places specialised in one topic or general forum where all three are welcome. 1 or 2 of these subjects can be forbidden, for example, because the forum doesn't want to be involved in criminal activity (e.g. they claim that drugs are harmless) or on the contrary, they say that drugs are harmful to people and should be not allowed.

Some sections can be found on all types of forums: anonymity and operational security, discussions about vendors, and marketplaces where users can trade. Administrators often get paid for sales brokerage (e.g. for escrow service) and for advertisements. Many underground forums are hubs for hackers or fraudster environments.

Most cybercriminals don't want to have anything in common with terrorism and child pornography. There is no permission for such topics, and all users who try to talk about it are banned. On many forums, other prohibited topics include guns, explosive devices, poisons, etc.

Cryptocurrency mixer

/ˈkrɪptoʊ ˈkɜrənsi ˈmɪksər/

A cryptocurrency mixer is a service associated with cryptocurrency to increase the anonymity of transactions and to make bitcoin harder to trace.

Many cryptocurrency transactions are transparent, and it is possible to see from which wallet to which the currency has travelled. The cryptocurrency mixer serves as a place where crypto owners can tumble money to obfuscate transaction flow.

Crooks often use those platforms in laundering money from cybercrimes.

D

Darknet

/dark nɛt/

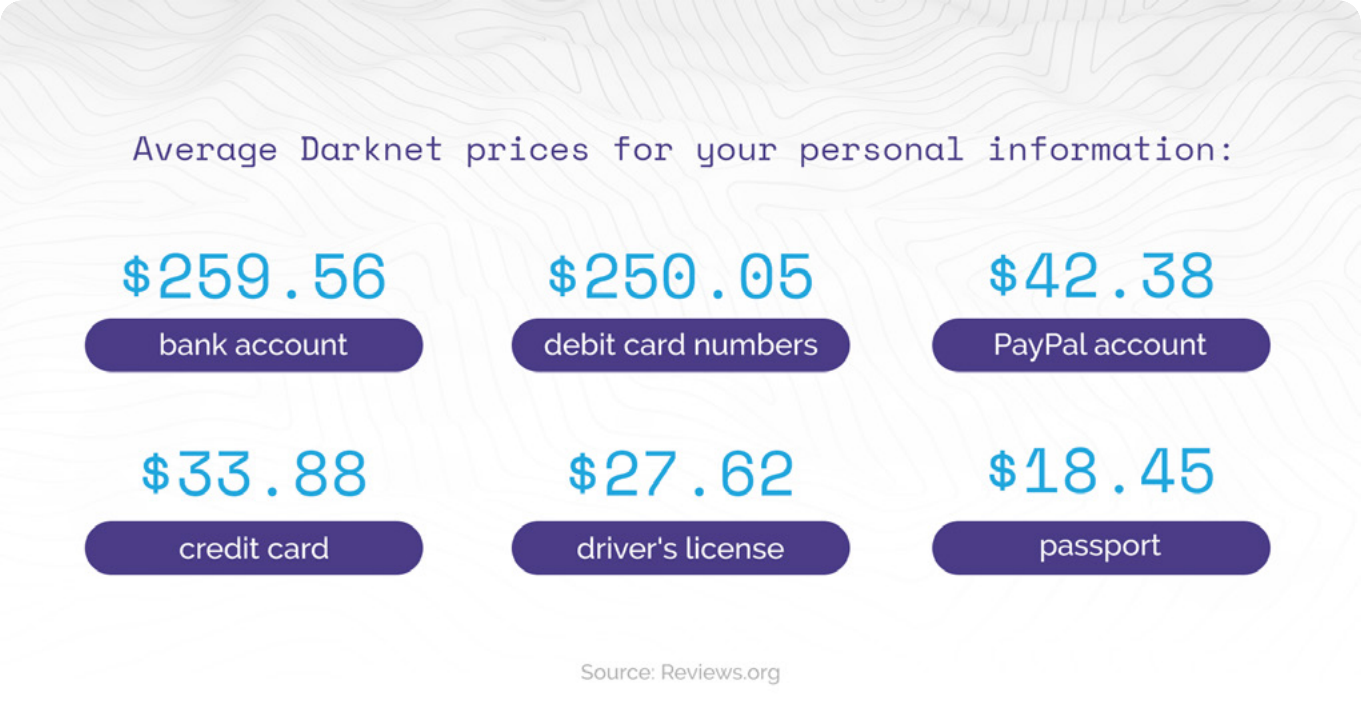
It's a part of the unindexed Internet and a subset of the deepweb consisting of several encrypted networks. To get access to it, users have to use specific software, such as the TOR browser, which is often wrongly identified with the darknet. Apart from TOR, the darknet includes networks like I2P, Freenet, GNUnet and others. They were created to ensure anonymous and uncensored access to the Internet and communication. Because of a high level of anonymity, the darknet is often used for unethical or illicit activities like trading of stolen or illegal merchandise, money laundering and others. Sometimes cybercriminals consider criminal forums in clearnet as part of the darknet, but it is incorrect.

Despite the above, the darknet can still be used for positive purposes. Citizens from countries where the Internet is censored can use it to access websites from other parts of the world. Companies like Facebook and BBC have websites on TOR.

Darknet market (DNM)

/dark nɛt ˈmarkət/

Darknet market (DNM) is a trading platform that operates in the darknets for various vendors who want to anonymously sell their illicit, stolen or somehow crime-related goods. Its appearance and features resemble e-shops like eBay. DNM can be general or focused on, e.g., fraud, drugs, tutorials, counterfeit items, digital products, carded items, services, malware, security, personal data. If your company suffered from online fraud, the big chances are that products stolen from you are now available on some DNM. The first and best known DNM - Silk Road was established in 2011, but it was shot down in 2013 by the FBI. You can find practically anything you want in the Darknet Markets. The example below shows for how much you can purchase personal data.



Average Darknet prices for your personal information:

$259.56	bank account
$250.05	debit card numbers
$42.38	PayPal account
$33.88	credit card
$27.62	driver's license
$18.45	passport

Source: Reviews.org

Darkweb

/dark wɛb/

This word is used in various meanings, which often lead to misunderstanding. It seems that among both threat intelligence researchers and the fraudsters community, there is no consensus on the word's meaning. Many people incorrectly treat the darkweb as a darknet synonym. Apart from this, the two most popular darkweb definitions are:

- All websites in the darknet
- All websites connected to criminal activity on the Internet, both in clearnet and darknet. A big part of the fraudsters community operates its forums and shops in clearnet. Also, there are many criminal "brands" that have both darknet and clearnet websites.

Dead fullz

/dɛd fʊlz/

Check first the definition of Fullz. Why should you care about dead fullz? While a credit card can be declined by a bank and useless afterwards, personal data of a cardholder remains the same and can be used in different types of fraud, including ordering credit cards on behalf of the victim, without their knowledge, leading to payment fraud. That's why those data, called dead fullz, are a lucrative subject of trade for fraudsters. Nothing goes to waste in the darknet!

DOB

/di-əʊ-bi/

Date Of Birth. One of the fundamental pieces of personally identifiable information used both by financial institutions and fraudsters. It is often needed for more complicated fraud.

Drop

/drɑp/

It's a physical or online space where a carder sends illicit consignments. Fraudsters can create a drop address, an e-mail address or a bank account; each used for a different purpose:

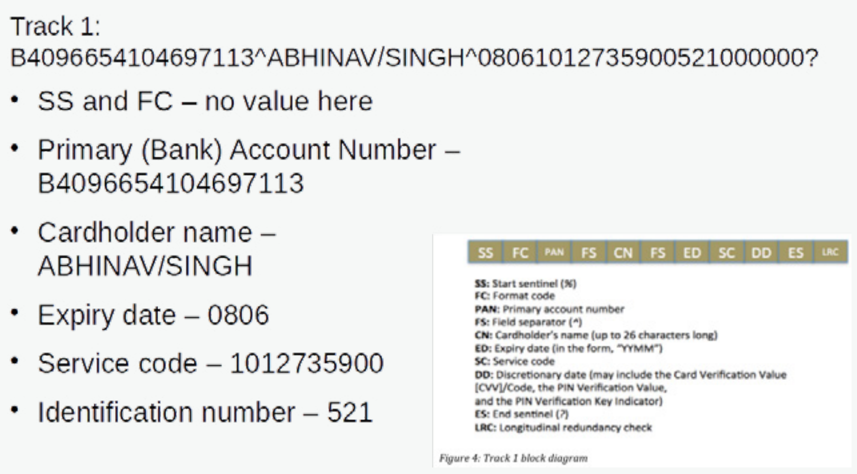
- Drop address is used to receive stolen physical merchandise.
- To obtain carded digital goods like gift cards, tickets or game keys, a fraudster will use a drop e-mail.
- A drop bank account can be used to receive money transfers (a step in money laundering).

Organising a physical drop address is more laborious than creating a simple drop e-mail. This is one of the reasons why carding gift cards and game keys is so popular. For lazy or uncreative fraudsters other fellows set up criminal groups in the darknet specialised in drops.

Dump

/dʌmp/

That's how fraudsters call data loaded on physical plastic: it includes bank account number, cardholder name, expiration date, service code, Identification number. Dumps can be bought in the same darknet markets where CC (credit card data) and fullz (CC and cardholder personal data) are offered. In that way, carders obtain forged credit cards that can be used for in-store carding.



Track 1:
B4096654104697113^ABHINAV/SINGH^08061012735900521000000?

- SS and FC – no value here
- Primary (Bank) Account Number – B4096654104697113
- Cardholder name – ABHINAV/SINGH
- Expiry date – 0806
- Service code – 1012735900
- Identification number – 521

SS: Start sentinel (%)
FC: Format code
PAN: Primary account number
FS: Field separator (^)
CN: Cardholder's name (up to 26 characters long)
ED: Expiry date (in the form, "YYMM")
SC: Service code
DD: Discretionary date (may include the Card Verification Value [CVV]/Code, the PIN Verification Value, and the PIN Verification Key Indicator)
ES: End sentinel (?)
LRC: Longitudinal redundancy check

Figure 4: Track 1 block diagram

Example of track 1 - part of data in dump.

In most cases, dumps come from credit cards without an EMV chip. Copying and loading data on cards with only magnetic stripes is much simpler. The US is the last G7 country that has not fully introduced EMV cards; that's why in-store carding is much more popular in the US than in Europe. But in the last few years, they have accelerated the introduction of EMV cards.

Escrow service

/ɛˈskroʊ ˈsɜrvəs/

Escrow service is the most common payment method on the Darknet Market (DNM). It's a security measure in a world where nobody can be trusted. It helps make transactions more secure between a buyer and vendor by keeping the payment in a secure account which is only released when all of the terms of an agreement are met, as determined by the escrow representative (DNM staff or carding forum administration).

When a buyer receives his order and s/he is satisfied, the escrow representative releases the money to the vendor. If the buyer is not satisfied, sometimes a dispute can occur—the buyer might claim that s/he didn't receive anything and the vendor might claim that s/he sent the order. The role of escrow is to settle the dispute. Its resolution is usually based upon proof provided by both sides as well as a consideration of their reputation from their previous activity.

Exit scam

/ˈɛgzɪt skæm/

As described above, escrow holds money during a Darknet Market (DNM) transaction. Sometimes it can keep the money for several days or weeks because the physical package must be sent from one state to another. The more popular a DNM/forum/escrow service is, the more escrows are created and a large amount of money can be stored by one entity — mostly in Bitcoin.

What stands in the way of stealing the money and never coming back? Such a getaway is called an "exit scam." Among the darknet society, it is a well-known fact that no DNM lives forever (at least not in the English language sphere of the darknet) and every DNM will eventually go "exit scam" or will be seized by law enforcement.

In 2019 there were at least a few known exit scams:

- Wall Street Market
- Nightmare Market
- Grey Market

There were also a few unexplained DNM shutdowns. Not only are the DNMs doing exit scams, but the cryptocurrency exchange is also known for this.

Real darknet stories

Wall Street Exit Scam

In the middle of April 2019 fraudsters experienced strong turbulence in their darknet reality. Wall Street Market (WSM), one of the biggest dark markets in TOR. The market was available in six languages and was used by approximately 5 400 vendors and 1,15 million customers. Moreover, it offered encrypted communications between buyers and sellers. On April 16th vendors started claiming that their cryptocurrency stored in WSM was gone and administrators stopped responding to messages. Ten days later, the information about maintenance and closing the registration appeared on the market's page. Moreover, all Bitcoins (BTC) from WSM wallet were transferred to one specific BTC wallet, and from there, it was distributed to others wallets. After several days the whole community was certain – WSM had employed an exit scam and stolen **11-30 million USD in BTC** belonging to WSM vendors. On May 2nd, everything was crystal clear; the information about maintenance on the WSM website was switched by a seizure page made by German law enforcement(LE). According to the German Federal Police (BKA), WSM administrators were in fact, attempting an exit scam with stolen BTC. But the bad guys weren't aware that they were already under LE surveillance. When LE understood that WSM owners would try to disappear, they arrested them. Apart from administrators, three other prominent vendors were arrested.

Source: nethone.com/blog

F

Fullz

/fʊlz/

Fullz it's a slang name for a batch of credit card data (CC) and cardholder personal data used to commit credit card fraud, tax refund fraud, medical identity theft, and other types of fraud. CC data includes the credit card number, validation date and security code. Still, for advanced carding operation, these data can be insufficient, and the carder may need cardholder personal data: name and surname, date of birthday, home address, mother's maiden name, social security number, phone number, e-mail. Criminals obtain the information in fullz through hacking or data leaks. So, if you have been the victim of a company's data breach, there could be fullz with your data available for sale in the darknet.

M

MMN

/ɛm-ɛm-ɛn/

Mother's Maiden Name. One of the basic personally identifiable information used both by financial institutions and fraudsters. It is often needed for more complicated fraud.

MSCS

/ ɛm-ɛs-siː-ɛs/

Short for MasterCard Secure, another term from the credit card industry. Fraudsters never use the phrase "3D security" for that type of payment protection. They always use the acronym "mscs" for Mastercards or "vbv" for Visa cards. One of the basic characteristics of stolen credit cards sold in the darkweb is information if the given card is vbv/mscs or is no-vbv/mscs. Presence or absence of such protection change carder tactics in card usage. Carding with mscs or vbv requires much more knowledge and effort, while no-vbv/no mscs are much easier in carding.

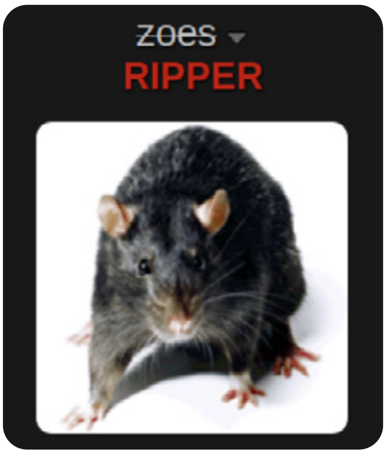
R

Ripper

/ˈrɪpər/

Fraudsters are not the most honest people. But often they have to cooperate with each other: stolen credit cards suppliers have to sell cards, carders have to buy cards and operation security tools; in many occasions, fraudsters need many bank accounts etc. It's hard to specialise in stealing/counterfeiting everything, that's why fraudsters have to work with other fraudsters.

A fraudster who deceives other fraudsters is called a ripper or a scammer. As the black market is entirely beyond any regulations and control, the fraudsters community tries to deal with rippers on their own. Every identified ripper on a forum or Darknet Market (DNM) is banned and marked as a scammer. On one forum nicks (nicknames) of identified scammers are crossed, a ripper mark is added, and the avatar is replaced with a rat picture.



S

Spoofing

/ˈspufɪŋ/

A spoofing attack is a situation in which a person or program successfully identifies as another by falsifying data, to gain an illegitimate advantage. There are a lot of spoof attacks using various ways of communication tools. The most common among fraudsters, and the easiest to use, are phone number spoofing, email spoofing and website spoofing. They are used during carding, account takeovers, phishing, business email compromise and other fraud attacks. It is also possible to spoof things like IP address, GPS location, communicators messages and so on.

T

TOR

/tɔr/

The Onion Router (TOR) is a secure, encrypted protocol to ensure the privacy of data and communications on the web. It uses a series of layered nodes to hide IP address, online data, and browsing history. The U.S. government initially developed it. Since 2006, it has been developed by the NGO Tor Project and financed by various entities: US government, universities, NGOs and companies. Because of the high level of anonymity, it is often used for illegal or unethical purposes. TOR is the biggest and the most famous Darknet network, but not the only one. There are other encrypted nets similar to TOR, and they all together form the Darknet.

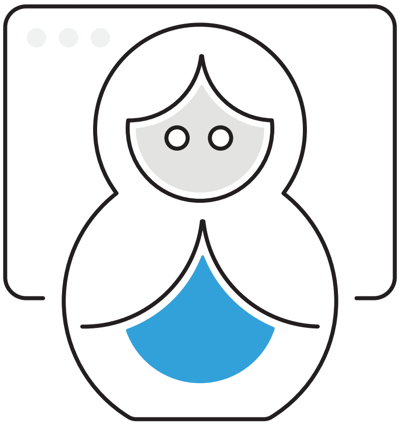
V

VBV

/vi-bi-vi/

Short for Verified by Visa, another word from the credit card industry. See MSCS.

Russian Language Sphere



В

Вбив

/Vbiv/

This is the way Russian speaking carders describe part of the carding process, where crooks enter stolen credit card data into payment form during payment. English speaking carders don't have a slang phrase for this word.

Вещевой/Вещевуха

/Veshchevoy/Veshchevukha/

Slang phrases for stuff carding – clothes, electronics, jewellery, car parts, etc.

Д

Дроп

/Drop/

Russians often divide drops into two categories: **Неразводные** (Nerazvodnie) and **Разводные** (Razvodnie):

Неразводные

/Nerazvodnyye/

These are people that fully understand what they are up to. Such drops receive a good salary, and the life of the drops is on average 2-3 months. However, they often have a few other requirements for their rules of work. The cost of admission is 70-100$ or some % of the value of the pack.

Разводные

/Razvodnyye/

The ones that were lied to about their role. They think they are doing legal work and are not aware of their role in illicit activity. They could be recruited, for example, on job sites. Using such drops takes the risk of losing packs, so they are not recommended for expensive stuff. Estimated drop life: 10-15 days. The main advantage of that drop type is the low price; they could be used for 50$ per pack shipment.

Дропowод

/Dropowod/

A drop supervisor. Apart from supervising drops, he often acts as a proxy between a drop and drop service clients.

Э

Энрол

/Enroll/

Credit card registration process on an online account management service on a bank website. Having access to such an account, a fraudster can for example view balance, transactions, statements, and most importantly, change account data like phone, address and email. Thanks to this, fraudsters will be able to bypass security systems like AVS and 3Ds. Not all banks allow credit cards.

З

Закладка

/Zakladka/

Zaklada is a tagged hiding spot from where online buyers pick up drugs. The most appropriate English word for it is stash or cache, but they are not precisely the same. "Zakladka" is strongly connected with Russian DNMs environment because they use that shipment method by default. "Zakladka" is not used by DNMs from other then CIS-state regions.

К

Кладсмен

/Kladsmen/

The courier who left the pack in zakladka. Like in zakladka case it is used by Russian speaking DNMs in CIS region.

Р

Разогревать Шопа

/Razogrevat' Shopa/

Fraudster acting like a typical customer on an eCommerce website for gaining credibility. In other words, it's a warm-up shop. After registering a new account, or login first time on a bought stolen account, the fraudster tries to create his history as an average user. He searches for different things, adds merchandise to the basket, and he won't make an order 1 hour after registration. Activity on the account should be repeated. Tutorials recommend various times for warming up. Sometimes it is 24h, sometimes a week.

Some tutorials as warm-up understand contacting shops before (in small shops cases) or after (big shops) making orders. It could be by email or by phone. This technique can be used as an occasion to inform shops about different shipping addresses or billing addresses. However, it requires social engineering skills from a fraudster.

Реролл

/Reroll/

It's a credit card account takeover of an already enrolled account. It is riskier than to simply enroll.

Ф

Фулка

/Fulka/

The Russian word for fullz. See fullz.

Ч

чернухи

/Chernukha/

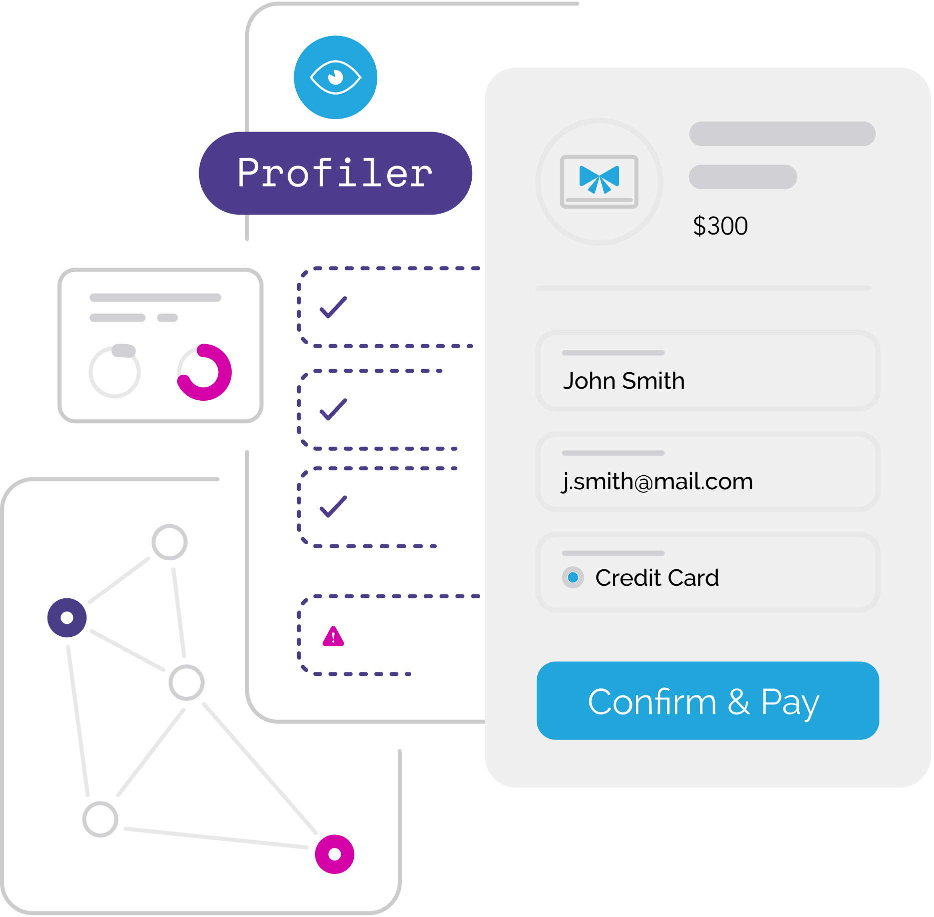
Russian slang phrase for dirty money.

Step 2: Learn techniques. Profiler.

You know the language; now it's time for more advanced stuff - behaviour and techniques. Learn about Profiler Technology that significantly impacts fraud detection efficiency.

Just like the police use profilers to solve the most advanced cases, the same can and should be done with cybercriminals. Only by knowing specific behaviour and techniques of this criminal group can you prevent the attack.

At Nethone, we invented a unique **Profiler Technology**. Based on our darknet knowledge, we listed all essential characteristics about the online user that can tell apart fraudsters and real customers. We extract **5,000 attributes about each user** who lands on a page to see if they are attempting to anonymise their actions, conceal their actual location, or use automation tools to deceive your business. Profiler also observes raw behaviour associated with keystrokes, mouse or accelerometer.



We basically create a full profile of a user from declared **and undeclared data the second he/she enters the website**. It's an in-depth screening of a user, who will no longer trick you with system emulations or spoofing.

There are three main groups of attributes that Profiler distinguished:

Hardware software and browser intelligence

This variable shows the truth about the crime tool.

- GPU characteristics
- GPU detection
- Virtual machine detection
- Number of processor cores
- Mobile device detection
- Mobile emulation detection
- Battery
- Server OS detection
- DOM rendering engine anomalies
- HTML quirks
- Special cookies (based on HTML technologies, self regenerating)
- Popular fraudster's tools detection
- Spoofing detection
- Incognito mode detection
- Browser quirks
- Various fingerprints

Behavioral data

This attribute shows the way the user interacts with the website and his behaviour.

- Mouse/Touchpad movements
- Swipes/Touches or scrolls
- Keystroke dynamics
- Gyro readings
- Accelerometer
- Clipboard usage

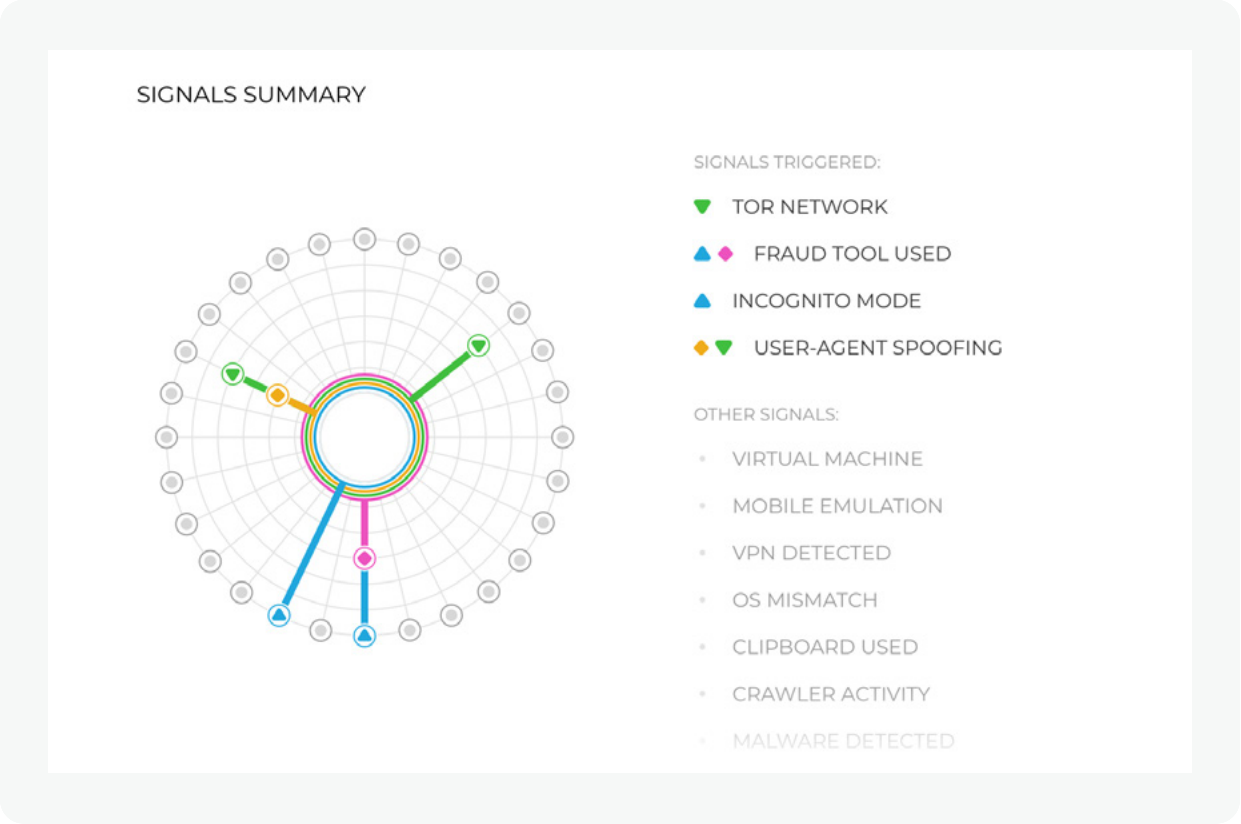
Network data

It describes the network environment where the crime is committed.

- IP geolocation
- TCP/IP stack analysis and anomalies detection
- Connection type detection (Wi-Fi, cellular) based on low level network analysis and/or browser features checks
- OS Fingerprinting
- VPN/Proxy/Tunneling detection
- Tor detection
- Public IP leak /Local IP leak
- Server-based connection detection

The list is never final. The constant challenge is to come up with new ways to screen users' interactions with the website or application to understand them better and to always be one step ahead of fraudsters.

Out of those 5K attributes, we created the list of **Signals**. A signal is an information based on a certain group of attributes, occurring at the same session which may be an indicator of a higher probability of fraud. (i.e. 'Virtual Machine', 'User-Agent spoofing', 'Tor Network'). Profiler is currently able to identify **more than 60 signals** and the list is growing.



SIGNALS SUMMARY

SIGNALS TRIGGERED:

- ▼ TOR NETWORK
- ▲◆ FRAUD TOOL USED
- ▲ INCOGNITO MODE
- ◆▼ USER-AGENT SPOOFING

OTHER SIGNALS:

- VIRTUAL MACHINE
- MOBILE EMULATION
- VPN DETECTED
- OS MISMATCH
- CLIPBOARD USED
- CRAWLER ACTIVITY
- MALWARE DETECTED

Again, not all transactions with signals triggered means that it's a scam. The problem with fraud is that the schemes are changing rapidly and that there are barely any hard rules about what is and what is not fraudulent behaviour.

If we can see multiple transactions coming out of a common IP address, it can mean a fraud attack, but it can also mean employees using their corporate, proxied network to make purchases.

Mainly it's about the context, taking as many factors in as possible and finding patterns. Data gathered by Profiler is the first stage in the process of user recognition. To complete the picture, you need to boost it with merchants data and proper technology to analyse it - Machine Learning. Only ML models can connect those thousands of dots, find correlations and tell you "this is actually a fraudster".

However, without the first step - in-depth knowledge of fraudsters techniques, no model can be trained, and fraud specialists can't do their job properly. That's why it is so important to be fluent in fraudster language and their behaviour.

If you would like to know more about the Nethone hybrid approach to fraud prevention, visit **our page** or contact us via **contact@nethone.com**.

If you would like to just follow current darknet news, we regularly publish deep research and studies from the fraudster community on **our Blog**.