Inside Russian Carding:

Threat Report

NETACEA

Contents

Abstract

Carding – the unauthorised trading and use of stolen payment card data – is a significant problem for cardholders, financial institutions, and businesses. According to Juniper, online payment fraud will cost merchants over $343 billion globally between 2023 and 2027.[1] This white paper delves into the dark and secretive world of Russian carding, offering a unique perspective on the evolving landscape and intricate web of activities associated with these criminal practices. The Russian speaking carding underworld is infamous for being highly organised and capable, and operating on a global scale.

As the cat-and-mouse game between the law enforcement and carders escalates, this paper provides vital insights into increasingly elusive carding operations. We explore their typical victim profile, their tool kits, their tactics for acquiring, validating, and using payment card data, their diverse strategies for cashing out and laundering their illicit gains and their techniques for evading detection. We finish by suggesting practical measures organisations can take to protect themselves from this growing threat.

[1] https://www.juniperresearch.com/pressreleases/online-payment-fraud-losses-to-exceed-343bn [last accessed August 2023]

Executive Summary

The key points from the white paper are:

- The scale of Russian carding operations is staggering. Russian speaking organised crime groups are the foundation for the global carding underworld and play a major role at all stages of the criminal value chain from initial card compromise to laundering the illicit proceeds.
- Russian carders strategically target individuals and organisations outside of Russia to maximise their profits while minimising their risk of prosecution. Organisations in the United States are at highest risk.
- Operational security is critical to Russian carders. All their internet traffic is routed through virtual private networks and proxy networks to obscure its origin. Carders also employ “drops” to stand in for them whenever personal data or a physical address is needed.
- Success for carders is highly dependent on the quality of compromised data they can acquire. Businesses and individuals must not only protect their payment card details, but supporting personal data which may be used for identity verification.
- Cryptocurrency exchanges, money transfers, gift cards, consumer electronics, hotel accommodation and flight tickets are amongst the most popular cash out targets for Russian carders. Businesses offering these goods and services must be extra vigilant against purchases made with compromised card details.
- Implementing bot management solutions and anti-fraud tools empowers organisations to effectively protect themselves from falling victim to both human powered and automated carding attacks.

Introduction to Carding

What is Carding?

Carding is a type of fraud where unauthorised persons (known as "carders") use stolen payment card information for personal gain. This can include acquiring and validating stolen card information, making unauthorized purchases and withdrawals, and selling card information to other criminals for profit. It ultimately results in a theft of money from a payment cardholder; however, the impact of carding can be significant for all the parties involved in the payment process:

- The direct victim, the cardholder, may suffer financial losses, damage to their credit score, and have to expend time and effort to resolve the issue;
- The merchant may lose revenue for the goods and services they provided and may acquire chargeback fees or other penalties if they are found to have accepted a fraudulent transaction. Moreover, they may suffer reputational damage which can make customers hesitant to do business with them in the future; and
- The issuing bank may face financial loses in the form of reimbursement of funds to the defrauded cardholder in addition to the operational costs associated with detecting and investigating fraud.

For some, carding is associated with easy money, for others, with illegal activity followed by prosecution, and for the rest, it is an abstract concept of a mysterious hacker who carries out sophisticated financial cybercrimes. Carding is partially all the above, however, the key in carding is not only gaining access to card data, but also successfully cashing out without getting caught.

There are several ways carders look to profit from carding:

- **Online purchases**

  The stolen card details are used to purchase goods online, which can then be resold for a profit or kept for personal use. This is the most popular carding method.

- **Money transfers**

  Money from the stolen cards is transferred to the carder's account. This is a complex method due to a number of technical aspects; it is impossible to transfer money directly and as a result, carders look for workarounds to launder the funds.

- **Offline purchases and withdrawals**

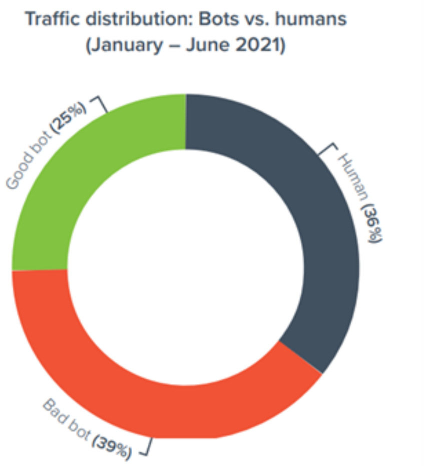
  The stolen card details are used to create a duplicate card, which can be used for two types of Card Present transactions: cash withdrawals through ATMs and purchases via Point of Sale (POS) terminals. This is the most complicated method to implement since it requires specialised equipment and highly technical knowledge.

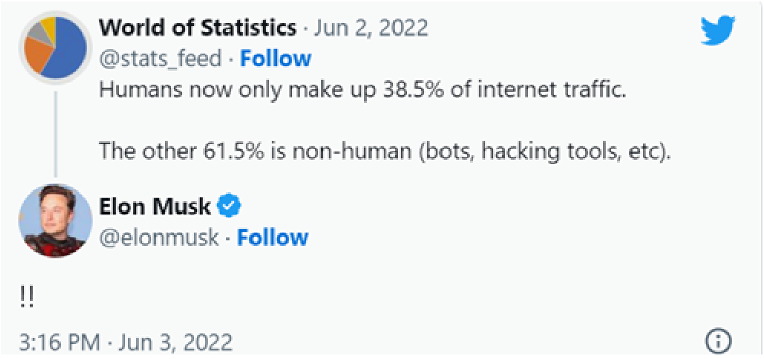
- **Resale of data**

  The stolen card details are sold on carding forums or underground marketplaces specialised in carding. The purchasers would then use one of the above methods to monetise the card details.

How are Bots Involved in Carding?

According to a report published by Barracuda in 2021, bots[2] make up nearly two-thirds of internet traffic. Bad bots accounted for 39% of all internet traffic over the first six months of 2021 while humans accounted for only 36%.[3] Other studies have come out with similar findings. In June 2022, the World of Statistics tweeted that "humans now only make up 38.5% of internet traffic – The other 61.5% is non-human (bots, hacking tools, etc.)":




World of Statistics · Jun 2, 2022
@stats_feed · Follow
Humans now only make up 38.5% of internet traffic.

The other 61.5% is non-human (bots, hacking tools, etc).

Elon Musk
@elonmusk · Follow

!!

3:16 PM · Jun 3, 2022

Source: https://assets.barracuda.com/assets/docs/dms/Bot_Attacks_report_vol1_EN.pdf

[2] Bots are automated processes that run over the internet. Malicious bots exploit business logic weaknesses in websites, mobile apps and APIs.

[3] https://assets.barracuda.com/assets/docs/dms/Bot_Attacks_report_vol1_EN.pdf

Automation through bots is integral to carding operations. Carders can use bots to increase the speed and scale of their operations in the following ways:

1 **Automated validation of credit cards** – Carders can use bots to rapidly test large amounts of credit card numbers, to identify cards that are valid and have not been cancelled by the card issuer. The carder can then use the validated cards to make fraudulent purchases or sell the list of validated cards to other cybercriminals.

2 **Card cracking** – In cases where carders only have access to partial card details, for example, where they are missing CVV codes or expiry dates, they use automated bots to enumerate the missing values in a brute force attack against a website's payment gateway until a valid combination is found.

3 **Credential stuffing** – Adversaries can use credential stuffing bots to automate the process of testing stolen usernames and passwords combinations across multiple websites or platforms and gain unauthorized access to user accounts. Once they have gained access to user accounts, they can exfiltrate sensitive data including credit card information, which can then be used in carding attacks.

4 **Mass account registration** – Carders can also use bots to automate the process of registering large amounts of accounts on online retailers, marketplaces, and carding forums. This allows them to quickly and easily establish many "shopping" accounts that can be used for carding attacks.

5 **Automated purchases** – Carders can also use bots to automatically make purchases on websites using stolen credit card information. This allows them to carry out large scale carding operations quickly and efficiently.

6 **Botnets** – Carders also use botnets, which are networks of infected computers or devices that can be controlled remotely, to carry out large-scale attacks on retailers or payment processors.

Bots play significant role in carding fraud globally by automating many of the steps involved and increasing the scale and efficiency of carders' operations, making it more challenging for law enforcement, financial institutions, and individuals to prevent, detect and respond to their activities.

The Carder's Dictionary

Russian carding communities use a combination of slang, codewords and jargon which may be unfamiliar to those outside the communities or the payment industry. Below, we have defined some of the more commonly used carding terms and phrases which may come up throughout this paper, including Russian language terms:

AVS (Address Verification System) – A security measure that enables merchants to detect suspicious credit card transactions and prevent credit card fraud. For card-not-present transactions, it verifies that the billing address entered by the customer matches the one associated with the cardholder's credit card account. AVS typically looks at the numeric portion of the address, the ZIP code, or both. The system will then return a response code indicating the degree of address matching and determining whether to accept or reject a transaction.

BIN (Bank Identification Number) – A unique sequence of digits at the start of the payment card number that identifies the issuing bank. The BIN can provide information such as the name, address, and phone number of the issuing bank, the card brand (Visa, Mastercard, American Express, etc), the card type (debit, credit, prepaid), the card level (black, platinum, business, etc), level of security (for example the presence of 3D secure), and whether the issuer is in the same country as the device used in the transaction. Knowing some of this information is crucial for carders and helps them to avoid detection by fraud prevention systems.

Buyer / [Russian: Scup] – A person who buys goods acquired by the means of carding for further resale.

Cash out / [Russian: Obnal] – The process of converting the stolen credit card information into actual money, cryptocurrency, goods or services, gift cards, loyalty points, etc.

Chargeback – A credit or debit card charge that is forcibly reversed by an issuing bank. This typically happens after a cardholder claims a transaction was the result of fraud or abuse.

Dedicated server / [Russian: Dedik] – A remote desktop or server with a powerful network and hardware configuration used for processing information and data storage. The server location is chosen based on the country where payment cards will be used.

Dump – Sets of payment card or cardholder data exfiltrated by physical skimming of the card, infecting point-of-sale devices with malware, or compromising computer systems and company servers. There are two types of dumps bought and sold on darknet marketplaces:

- **CC Dump** – The raw data loaded on a credit card's magnetic strip, usually consisting of track data and PIN. It includes data such as credit card number, first and last name, expiry date, CVV code.
- **Fullz dump** – The CC dump plus personally identifiable information (PII) relating to the cardholder such as social security number, date of birth, mother's maiden name, physical and email addresses, phone number, employment status and bank account details.

Drop – A person who performs intermediate operations for carders, bearing most of the risk for a small cut of the money. The use of drops allows carders to avoid direct involvement in the fraudulent transactions and makes it more difficult for law enforcement to track them down. Drops are commonly used to take delivery of the fraudulent purchases made with stolen credit card information. Once the goods are sent to the drop's shipping address, the drop forwards them to either the carder, another designated location or the final buyer. A drop may also be used to launder illicitly obtained money, for example, by transferring money to or from a drop's account in order to conceal the origin of money. Carders may also use a drop's personal information to complete verification processes such as know-your-customer (KYC). Drops are typically recruited through carding forums or social media and promised a percentage of the proceeds in exchange for their service; however, some drops may be unknowingly facilitating in fraudulent activity.

Enrol / [Russian: Rollka] –The process of gaining access to personal online banking services. Online banking typically allows customers to view balances, account activity and statements; perform account transfers, payments, and deposits; set up security alerts and notifications; and more. Most importantly for carders, online banking allows them to change personal account data, such as phone number, address and email.

Input / [Russian: Vbiv] – An attempt to make a fraudulent online purchase using stolen payment card data. Russian carders use the term "vbiv" to describe the process of entering stolen payment card data into payment forms.

Liquid goods – High-value goods that can be easily and quickly sold on the black market or online marketplaces for a fraction of their retail value. These items are usually electronic devices such as cameras, smartphones and laptops, or high-end fashion items like trainers, bags and jewellery. Liquid goods are an attractive target for carders, offering a high return on investment and quick conversion of stolen credit card information into cash.

Logs – An archive of compromised user data, such as usernames and passwords to websites visited, cookies, browsing history, IP addresses, device fingerprints and keystrokes, gathered from a hacked computer. Carders use logs to obtain sensitive information such as credit card numbers, bank login credentials, and personal identifiable information (PII) and use it to make fraudulent transactions. Additionally, logs can also be used to identify vulnerabilities in a system, which can be exploited in further attacks. Carders often sell or trade logs on underground marketplaces, making them a valuable commodity in the cybercrime world.

Magecart – A form of malware that infects online stores and eCommerce platforms to facilitate digital card skimming. In a Magecart-style attack, hackers steal credit card information from customers by embedding malicious code into the source code of pages with payment sections, for example, Checkout or Order Confirmation pages.

Material – A combined term for tools and resources that carders can use to carry out credit card fraud. This may include lists of stolen credit card numbers, physical payment cards, bank accounts, cardholder's information or fullz, card verification codes (CVC) and proxies.

- **MCSC (Mastercard SecureCode)** – Mastercard Identity Check, formerly SecureCode, is a 3-D secure service that provides an extra layer of security when paying with Mastercard debit or credit card. This may be a single-use code sent to mobile phone, or another form of two-factor authentication decided by the issuing bank.

- **Merchant account** – A commercial bank account that help process online transactions for businesses.

- **POS (point of sale)** - Payment card reading devices used to process transactions and accept payments.

- **Reroute** – A service that arranges for a package to be redirected to a new address. In carding, orders are typically rerouted to the drop's shipping address.

- **Self-registered bank account / [Russian: Samoreg]** – This term is used to describe manually registered online bank account using other people's data from purchased fullz. Carders use stolen personal identifiable information (PII) and credit card data without the knowledge or consent of legitimate cardholder.

- **SOCKS (proxy)** – An intermediary used to hide IP address from online servers. SOCKS is an Internet protocol that exchanges network packets between a client and server through a proxy server. SOCKS5 optionally provides authentication so only authorized users may access a server.

- **Stealer** – A type of malware that gathers data and extracts logs from infected devices. The most common form of stealers is used to gather login information, such as usernames and passwords, and then send that information to another system either via email or over a network.

- **VBV (Verified by Visa)** – Visa Secure is an advanced security feature from Visa that helps authenticate purchasers as authorized cardholders. Visa Secure is the card network-branded deployment of 3-D Secure technology and was formerly known as Verified by Visa.

Russian Carding Landscape

The Scale of Russian Carding

Carding is a global issue. However, it has become a significant problem in Russia over the past few years, where organised crime groups have exploited the widespread availability of stolen credit card information and the global growing e-commerce market. These groups are highly capable, well-resourced and well-connected. They have a significant presence within underground carding forums, marketplaces and messaging channels. These serve as platforms for carders to communicate, exchange information and buy and sell compromised payment card data, carding tools or supporting services. They operate across geographical borders, making it difficult for law enforcement agencies to effectively target them.

Russian speaking cybercriminals are widely regarded to be among the most active and sophisticated actors in the cyber underground. For example, Recorded Future, a cyber threat intelligence provider, stated that "Russian-language actors dominate the majority of fraud-focused dark web forums and top-tier carding marketplaces... Recorded Future analysts expect that an increase in Russian cybercrime would correspond to an expansion of Russian carding targeting vulnerable entities, financial organizations, merchants, and individuals that store valuable repositories of card data."[4]

However, it is difficult to quantify the exact size of the Russian carding presence as it is a constantly evolving and largely hidden environment. Due to the illegal nature of their activities, carders are secretive about their operations and hide behind anonymity services, encrypted communications, middlemen, puppet accounts and pseudonyms. This makes it challenging for security researchers and law enforcement to track and identify prominent carders and assess the scale and success of their operations.

[4] https://www.recordedfuture.com/magecart-attacks-the-dark-art-fraudsters-use-to-steal-payment-data [Last accessed 22 February 2023]

Russian Carding Target Profile

Research on the nature and activity patterns of Russian carders indicates that they tend to focus on targets outside of Russia. In January 2023, researchers from Recorded Future's Insikt reported that of the 60 million compromised payment card records for sale on dark web platforms in 2022, 70% were issued by financial institutions in the USA.[5] As one of the largest economies and e-commerce markets in the world, the USA is certainly a lucrative target for financial crime and many Russian carders look to take advantage of American retailers with weak security measures in place. However, Russian carding attacks are not limited to the USA; Russian carders can also attack retailers in other countries, depending on their focus and opportunities.

Targeting foreign markets and payment systems may also be seen as the safer option for Russian carders, since attacks against targets in the Commonwealth of Independent States (CIS)[6] can carry significant legal risks in Russia. Local law enforcement agencies such as the Federal Security Service (FSB) have become increasingly active in cracking down on cybercrime in recent years. For example, in 2022, Russian law enforcement seized the domains of several prominent carding marketplaces, arresting ten men purportedly behind the sites. The takedown notices on the seized marketplaces, which included Trump's Dumps, UniCC and Ferum Shop, the then leading stolen payment card shop, were designed to spread fear within the carding community with the message "Which one of you is next?".[7]

Information sharing agreements and joint investigation capabilities have been established between different departments and agencies within the Russian Federation and CIS countries. Conversely, the lack of extradition treaties between Russia and NATO or other Western countries makes it less likely that Russian carders will be prosecuted internationally for their activities. It is also costlier to investigate and prosecute crimes instigated from abroad, and in many cases, it is not financially viable for foreign entities to look for carders internationally, extradition issues aside. For example, foreign law enforcement is unlikely to expend time and resources to find and prosecute the actors behind the theft of $2,000, when the investigation will cost significantly more than the amount to be recovered. This has led to an unspoken rule among Russian carders to never target organisations in Russia, CIS countries and the entire post-soviet space. By doing so, carders can avoid the attention of local law enforcement and operate with relative impunity. However, it is worth noting that some Russian carders do still target victims in Russia.

Overall, a Russian carder's targets can vary depending on a range of factors, including legal risks, profitability, and market conditions. Generally, any individual or organisation which does not adequately protect cardholder information can fall victim to an attack. At an industry level, common targets include retail, hospitality, and financial services organisations.

[5] https://therecord.media/59-4-million-compromised-payment-card-records-posted-for-sale-on-dark-web-in-2022-report

[6] The Commonwealth of Independent States (CIS) is an intergovernmental organisation established following the dissolution of the Soviet Union in 1991. It consists of some of the states that formerly comprised the Soviet Union. Its objective is to coordinate cooperation between members states' law enforcement actions, economies, foreign relations, defense, and other areas of national policy.

[7] https://krebsonsecurity.com/2022/02/russian-govt-continues-carding-shop-crackdown/ [Last accessed 27 February 2023]

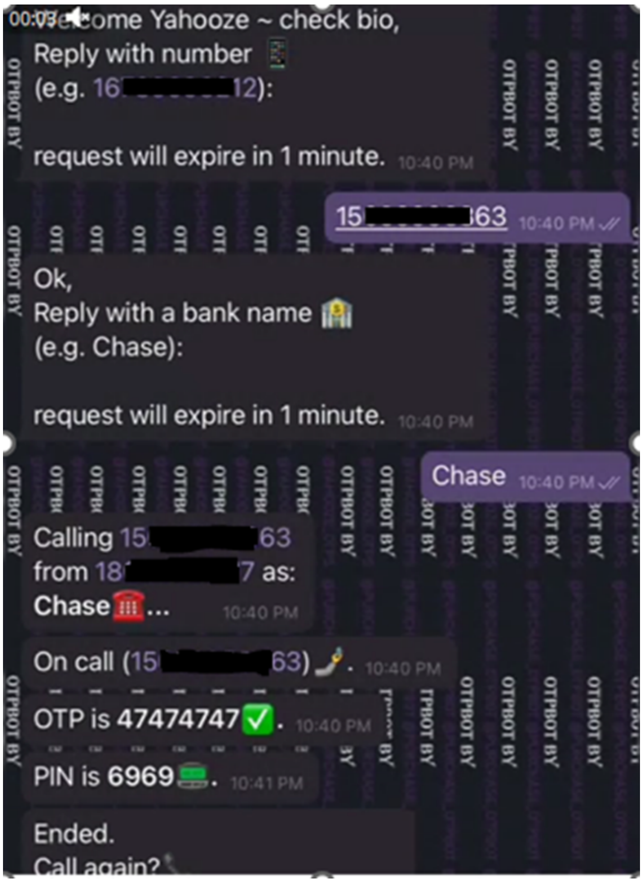
Russian Carder Toolbox

Russian carding groups have developed a reputation for being particularly adept, with many skilled programmers and hackers. They are known for developing sophisticated malware and hacking tools which are used to breach payment systems, steal card data, and compromise online accounts. In addition to carding bots discussed earlier, these include:

1 **Digital skimmers:** Digital skimmers are malicious JavaScript programs used to steal payment card details from websites. The code is injected into the website's payment page and captures any payment card details entered by the customers at the checkout. Magecart is a collective term used to refer to disparate hacking groups notorious for their use of digital skimmers. They have been responsible for several high-profile data breaches, including attacks on British Airways[8] and Ticketmaster.[9] It is not clear who is behind the groups, but several cybersecurity firms have identified links between Magecart, and other Russian-speaking hacking groups based on a majority of Magecart hacking tools being advertised in the Russian language and a significant number of underground forums where JS-sniffers are put up for sale or rent being Russian-speaking.[10]

2 **Banking Trojans:** Banking Trojans, such as TrickBot, can be used to steal financial information, banking credentials and PII. TrickBot's operators, a cybercrime-as-a-service group based in Russia, were recently sanctioned by authorities in the US and UK for its involvement in numerous ransomware attacks and bank account takeovers. According to the Group-IB Crime Trends 2022/2023 report, many other banking Trojans including Q-bot, Emotet, IcedID, Godfather and InTheBox have also been connected to Russian speaking developers, hackers, or ransomware groups. However, it should be noted that these groups operate globally and typically have members from various countries.

3 **OTP Bots:** One Time Password/Passcode (OTP) bots allow carders to bypass OTP, two-factor authentication, and SMS verification. The OTP bot captures verification codes by spoofing a bank or company's caller ID, calling the victim, and then tricking them into providing the code.



Welcome Yahooze ~ check bio,
Reply with number 📱
(e.g. 16[redacted]12):

request will expire in 1 minute. 10:40 PM

15[redacted]63 10:40 PM

Ok,
Reply with a bank name 🏦
(e.g. Chase):

request will expire in 1 minute. 10:40 PM

Chase 10:40 PM

Calling 15[redacted]63
from 18[redacted]7 as:
Chase☎... 10:40 PM

On call (15[redacted]63). 10:40 PM

OTP is 47474747✅. 10:40 PM

PIN is 6969. 10:41 PM

Ended.
Call again?

OTP bot retrieving one time password and PIN

[8] https://www.theregister.com/2018/09/11/british_airways_web site_scripts/ [Last accessed 10 August 2023]

[9] https://www.theregister.com/2018/07/12/ticketmaster_breach_ magecart/ [Last accessed 10 August 2023]

[10] https://www.group-ib.com/resources/research-hub/js-sniffers/

Carding Deep Dive

Material Acquisition

At the foundation of every carding attack are stolen payment card details. However, supporting resources are often required for carders to monetize the card details. Russian-speaking carders refer to these resources as “material”. This can include information such as payment cards, bank accounts, personal data, device fingerprints and user data. There are various methods carders can use to acquire material.

Initial Acquisition

1 **Data Breaches:** Large scale data breaches are one of the biggest contributing factors to the amount of compromised payment card data being circulated. Cyber criminals break into company servers, payment systems or online stores in attempts to steal databases of sensitive financial and personal data. Alternatively, the breach is perpetrated by insiders within the victim organisation itself. The stolen databases, which contain credit card details and personal data are then leaked or sold on carding forums and marketplaces.

2 **Physical Skimmers:** Historically, payment cards stored all their data on magnetic strips; ATMs and point-of-sale devices would read the data from the strip to process a transaction. However, this resulted in the advent of card skimmers, physical devices that adversaries could install onto ATMs or point-of-sale devices to clone data from a card’s magnetic strip. The cloned data would either be transmitted wirelessly to the adversary, for example, via Bluetooth, or stored on the skimmer for the adversary to retrieve later. Whilst newer chip-based cards are more resistant to skimming, many chip cards still have magnetic strips for backwards compatibility.

3 **Digital Skimmers:** As online transactions and e-commerce have grown in popularity, the concept of card skimming has spawned a digital equivalent. Adversaries developed card skimming malware that can be embedded into a victim website and steal payment card data entered into payment forms or checkout pages during online transactions. The stolen data is transmitted to command-and-control servers under the attacker’s control.

4 **Infostealers:** Adversaries use infostealer malware to covertly steal sensitive information such as login credentials, banking and payment card details, cryptocurrency wallet information, and other personal data. Once the malware is installed on a victim’s device, it harvests the desired information and transmits it back to the attacker’s command and control server. The stolen data can then be used for various criminal activities, including identity theft and financial fraud.

5 **Phishing/Vishing:** Phishing is a social engineering technique where attackers use fraudulent emails, messages or websites to trick individuals into divulging their personal or financial information. When performed over the phone, such attacks are known as vishing. In both cases, the attacker typically masquerades as a legitimate party, such as a bank or online retailer. These attacks can be highly effective, especially if the attacker has already obtained some personal information about the victim, which they can use to make the lure seem more convincing.

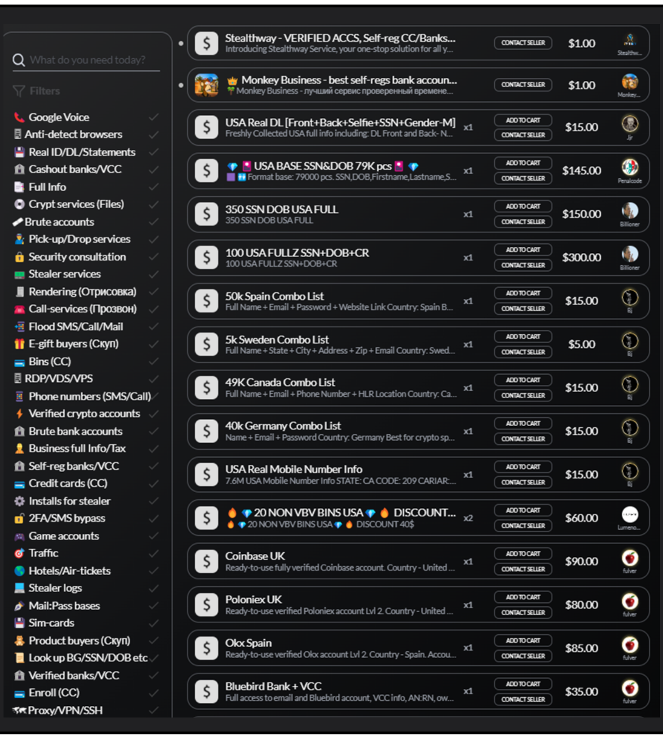
6 **Account Takeover:** Payment card data can also be stolen directly from the cardholder through account takeover attacks.
These happen when cybercriminals gain unauthorized access to user’s e-commerce or online banking account, for example, through a credential stuffing attack, phishing or with data gathered by an infostealer.

Carding Marketplaces

Trading compromised payment cards is commonplace in the cyber underground. Card data obtained from data breaches, skimmers, phishing, or any of the other initial acquisition methods quickly finds its way onto carding stores and forums. These marketplaces exist both on the clear and dark web and offer a range of carding material and services. Carders can purchase credit cards, bank account information, personal information leaks, money laundering or document forgery services, carding tutorials and guides, and other illicit content related to credit card fraud.

It is not uncommon for new or inexperienced carders to be scammed or ripped off by fake carding vendors. Hidden amongst the underground's many marketplaces are scammers, who take advantage of the anonymous nature of carding operations. They open a carding store with competitive prices, demand payment upfront and disappear with the payment without delivering any material. To protect themselves and their money from unscrupulous vendors, carders favour purchasing material from sources where an escrow arrangement is available. Many reputable carding marketplaces now offer escrow or guarantor services, as well as transaction dispute resolution procedures.

The price of payment card information on carding marketplaces can range from a few dollars to several hundred dollars per card, depending on the quality of the information. For example, payment card leaks complete with expiration dates and CVV codes are more valuable than card numbers alone. Similarly, cards with high credit limits, such as gold, platinum or corporate cards are more valuable than basic cards. The country of origin, issuing bank and security features of the card are also factors in the price. The cost can also be influenced by supply and demand, as well as the risk involved in obtaining the information. For example, payment card information that was obtained through a high-profile data breach may be more valuable than information obtained through phishing scams or other lower-risk acquisition methods.



Google Voice
Anti-detect browsers
Real ID/DL/Statements
Cashout banks/VCC
Full Info
Crypt services (Files)
Brute accounts
Pick-up/Drop services
Security consultation
Stealer services
Rendering (Отрисовка)
Call-services (Прозвон)
Flood SMS/Call/Mail
E-gift buyers (Скуп)
Bins (CC)
RDP/VDS/VPS
Phone numbers (SMS/Call)
Verified crypto accounts
Brute bank accounts
Business full Info/Tax
Self-reg banks/VCC
Credit cards (CC)
Installs for stealer
2FA/SMS bypass
Game accounts
Traffic
Hotels/Air-tickets
Stealer logs
Mail:Pass bases
Sim-cards
Product buyers (Скуп)
Look up BG/SSN/DOB etc
Verified banks/VCC
Enroll (CC)
Proxy/VPN/SSH

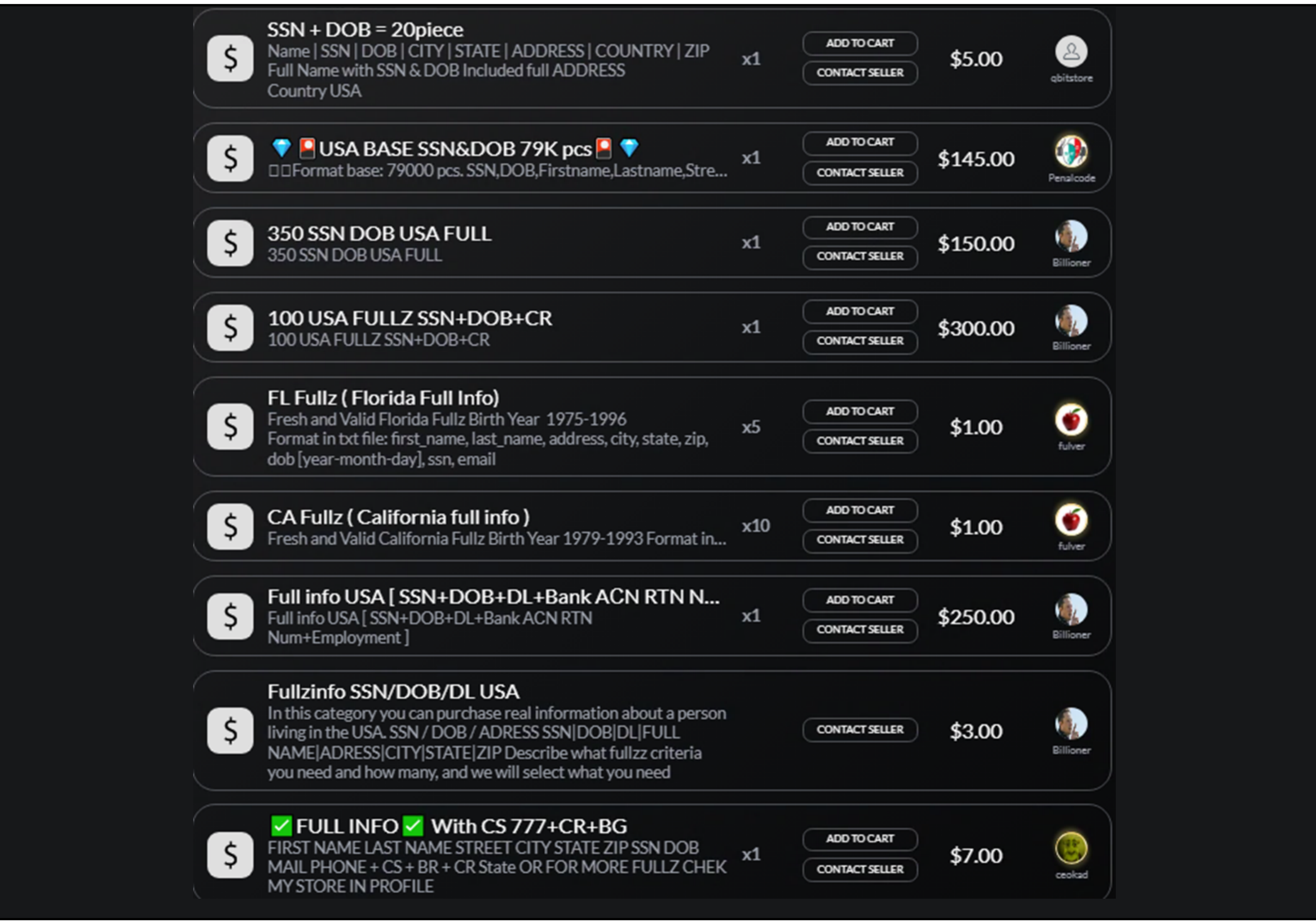
Stealthway - VERIFIED ACCS, Self-reg CC/Banks... Introducing Stealthway Service, your one-stop solution for all y...		CONTACT SELLER	$1.00	Stealthw...
👑 Monkey Business - best self-regs bank accoun... Monkey Business - лучший сервис проверенный времене...		CONTACT SELLER	$1.00	Monkey...
USA Real DL [Front+Back+Selfie+SSN+Gender-M] Freshly Collected USA full info including: DL Front and Back- N...	x1	ADD TO CART CONTACT SELLER	$15.00	Jjr
💎 USA BASE SSN&DOB 79K pcs 💎 Format base: 79000 pcs. SSN,DOB,Firstname,Lastname,S...	x1	ADD TO CART CONTACT SELLER	$145.00	Penalcode
350 SSN DOB USA FULL 350 SSN DOB USA FULL	x1	ADD TO CART CONTACT SELLER	$150.00	Billioner
100 USA FULLZ SSN+DOB+CR 100 USA FULLZ SSN+DOB+CR	x1	ADD TO CART CONTACT SELLER	$300.00	Billioner
50k Spain Combo List Full Name + Email + Password + Website Link Country: Spain B...	x1	ADD TO CART CONTACT SELLER	$15.00	Bj
5k Sweden Combo List Full Name + State + City + Address + Zip + Email Country: Swed...	x1	ADD TO CART CONTACT SELLER	$5.00	Bj
49K Canada Combo List Full Name + Email + Phone Number + HLR Location Country: Ca...	x1	ADD TO CART CONTACT SELLER	$15.00	Bj
40k Germany Combo List Name + Email + Password Country: Germany Best for crypto sp...	x1	ADD TO CART CONTACT SELLER	$15.00	Bj
USA Real Mobile Number Info 7.6M USA Mobile Number Info STATE: CA CODE: 209 CARIAR:...	x1	ADD TO CART CONTACT SELLER	$15.00	Bj
🔥 💎 20 NON VBV BINS USA 💎 🔥 DISCOUNT... 🔥 💎 20 NON VBV BINS USA 💎 🔥 DISCOUNT 40$	x2	ADD TO CART CONTACT SELLER	$60.00	Lumeno...
Coinbase UK Ready-to-use fully verified Coinbase account. Country - United ...	x1	ADD TO CART CONTACT SELLER	$90.00	fulver
Poloniex UK Ready-to-use verified Poloniex account Lvl 2. Country - United ...	x1	ADD TO CART CONTACT SELLER	$80.00	fulver
Okx Spain Ready-to-use verified Okx account Lvl 2. Country - Spain. Accou...	x1	ADD TO CART CONTACT SELLER	$85.00	fulver
Bluebird Bank + VCC Full access to email and Bluebird account, VCC info, AN:RN, ow...	x1	ADD TO CART CONTACT SELLER	$35.00	fulver

Popular Carding Marketplace

Fullz

The most valuable material for carders are packages of cardholders' personal data known as fullz, which is slang for full information. Fullz can include the cardholder's name, date of birth, Social Security number, mother's maiden name, postal address including zip code, email address, phone number, driving licence number, bank account details and online account credentials, providing carders with a complete profile of the victim. This makes it easier to bypass security checks and fraud detection measures, impersonate the cardholder, and commit various types of fraud, including identity theft, opening new lines of credit and making fraudulent purchases.

Fullz packages are sold on carding forums and marketplaces. Their price varies depending on the quality, completeness and accuracy of the information, the age and type of the credit card and the cardholder's credit score. For example, a fullz package that contains high-limit credit cards with good credit scores and long credit histories can be sold for a higher price than one with lower-limit cards or poor credit scores. Similarly, a fullz package which contains background information about the victim, such as their previous addresses, employment history or educational background commands a higher price, as this information is difficult to gather.

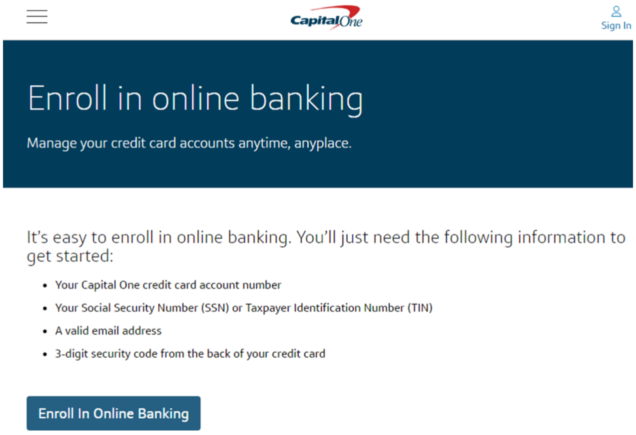


$	**SSN + DOB = 20piece** Name | SSN | DOB | CITY | STATE | ADDRESS | COUNTRY | ZIP Full Name with SSN & DOB Included full ADDRESS Country USA	x1	ADD TO CART CONTACT SELLER	$5.00	qbitstore
$	**💎 📛USA BASE SSN&DOB 79K pcs📛 💎** □□Format base: 79000 pcs. SSN,DOB,Firstname,Lastname,Stre...	x1	ADD TO CART CONTACT SELLER	$145.00	Penalcode
$	**350 SSN DOB USA FULL** 350 SSN DOB USA FULL	x1	ADD TO CART CONTACT SELLER	$150.00	Billioner
$	**100 USA FULLZ SSN+DOB+CR** 100 USA FULLZ SSN+DOB+CR	x1	ADD TO CART CONTACT SELLER	$300.00	Billioner
$	**FL Fullz (Florida Full Info)** Fresh and Valid Florida Fullz Birth Year 1975-1996 Format in txt file: first_name, last_name, address, city, state, zip, dob [year-month-day], ssn, email	x5	ADD TO CART CONTACT SELLER	$1.00	fulver
$	**CA Fullz (California full info)** Fresh and Valid California Fullz Birth Year 1979-1993 Format in...	x10	ADD TO CART CONTACT SELLER	$1.00	fulver
$	**Full info USA [SSN+DOB+DL+Bank ACN RTN N...** Full info USA [SSN+DOB+DL+Bank ACN RTN Num+Employment]	x1	ADD TO CART CONTACT SELLER	$250.00	Billioner
$	**Fullzinfo SSN/DOB/DL USA** In this category you can purchase real information about a person living in the USA. SSN / DOB / ADRESS SSN|DOB|DL|FULL NAME|ADRESS|CITY|STATE|ZIP Describe what fullzz criteria you need and how many, and we will select what you need		CONTACT SELLER	$3.00	Billioner
$	**✅ FULL INFO ✅ With CS 777+CR+BG** FIRST NAME LAST NAME STREET CITY STATE ZIP SSN DOB MAIL PHONE + CS + BR + CR State OR FOR MORE FULLZ CHEK MY STORE IN PROFILE	x1	ADD TO CART CONTACT SELLER	$7.00	ceokad

Variety of fullz advertised for purchase

Enrolment

Fullz are primarily purchased to enable carders to enrol stolen cards into online banking. Enrolment requires an individual to provide personal details such as their full name, date of birth, Social Security number, and contact information; carders can use a fullz package to obtain the necessary details. Once enrolled, the carder can view the victim's account information, including their account balance, transaction history, and account number.



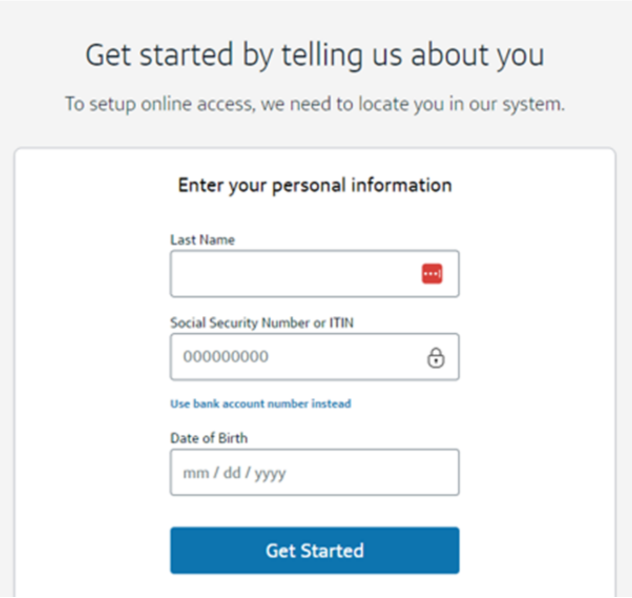
Enroll in online banking

Manage your credit card accounts anytime, anyplace.

It's easy to enroll in online banking. You'll just need the following information to get started:

- Your Capital One credit card account number
- Your Social Security Number (SSN) or Taxpayer Identification Number (TIN)
- A valid email address
- 3-digit security code from the back of your credit card

Example of enroll on Capital One bank



Get started by telling us about you

To setup online access, we need to locate you in our system.

Enter your personal information

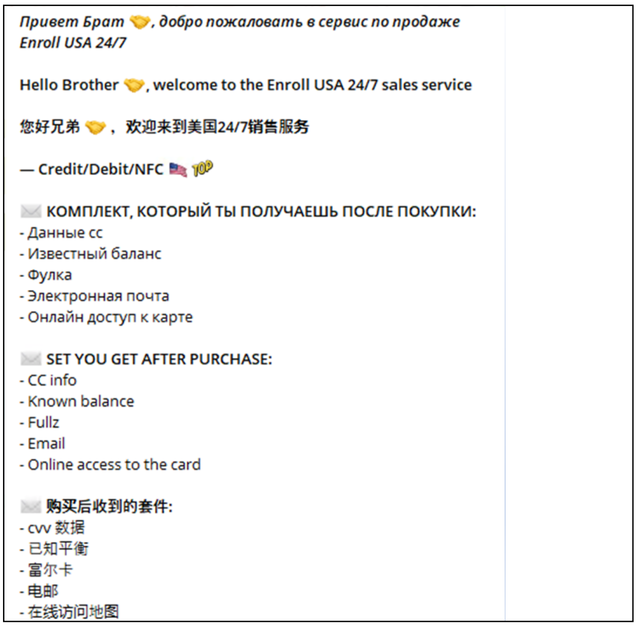
Last Name:

Social Security Number or ITIN: 000000000

Date of Birth: mm / dd / yyyy

In this example, the data required for enrol includes last name, social security number and date of birth

One of the primary benefits of having access to online banking is that it allows the carder to change the account holder's information. Most merchants use an AVS (Address Verification System) check which compares the shipping address with the cardholder's billing address, as a part of their fraud prevention measures. If the AVS check fails, they can decline the transaction or perform further antifraud checks. However, carders can get around AVS if they have access to online banking, by changing the cardholder's billing address to their drop's address, so it matches the shipping address. Similarly, carders can intercept messages from the bank intended for the cardholder by replacing the contact details on the account with their own. This prevents the cardholder from getting notified of suspicious transactions.



Привет Брат 🤝, добро пожаловать в сервис по продаже Enroll USA 24/7

Hello Brother 🤝, welcome to the Enroll USA 24/7 sales service

您好兄弟 🤝， 欢迎来到美国24/7销售服务

— Credit/Debit/NFC 🇺🇸 🔝

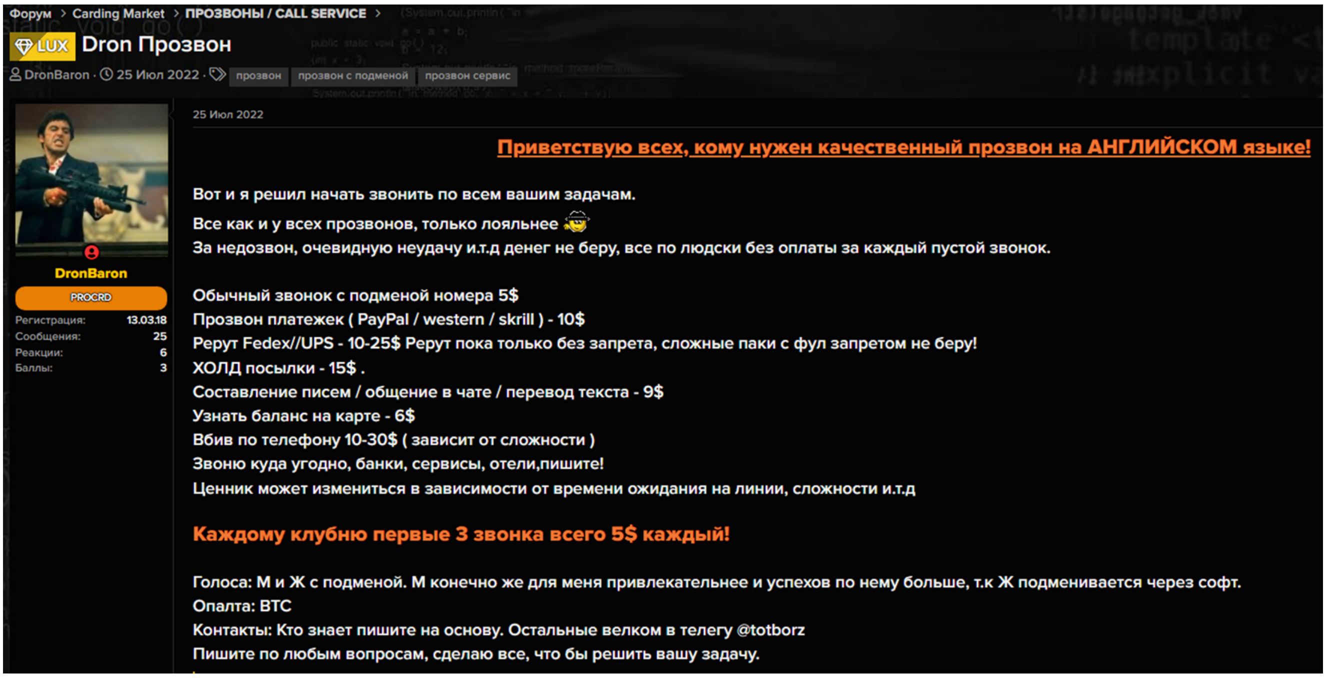
✉️ **КОМПЛЕКТ, КОТОРЫЙ ТЫ ПОЛУЧАЕШЬ ПОСЛЕ ПОКУПКИ:**
- Данные cc
- Известный баланс
- Фулка
- Электронная почта
- Онлайн доступ к карте

✉️ **SET YOU GET AFTER PURCHASE:**
- CC info
- Known balance
- Fullz
- Email
- Online access to the card

✉️ **购买后收到的套件:**
- cvv 数据
- 已知平衡
- 富尔卡
- 电邮
- 在线访问地图

Threat actor selling enrol services

Changing the phone number also allows the carder to call the bank's customer support team or the merchant pretending to be a card holder. This helps the carder to build trust relationships, decreasing the risk of transactions being blocked or flagged as suspicious. Carders often employ third party specialist call services to handle communication with the bank, especially when they do not have the language skills to communicate in the cardholder's first language. These services provide a live operator who can impersonate the cardholder and provide the necessary information to complete the transaction or help bypass phone-based multi-factor authentication.



Dron Прозвон

DronBaron · 25 Июл 2022

DronBaron

Регистрация: 13.03.18
Сообщения: 25
Реакции: 6
Баллы: 3

25 Июл 2022

Приветствую всех, кому нужен качественный прозвон на АНГЛИЙСКОМ языке!

Вот и я решил начать звонить по всем вашим задачам.
Все как и у всех прозвонов, только лояльнее
За недозвон, очевидную неудачу и.т.д денег не беру, все по людски без оплаты за каждый пустой звонок.

Обычный звонок с подменой номера 5$
Прозвон платежек (PayPal / western / skrill) - 10$
Рерут Fedex//UPS - 10-25$ Рерут пока только без запрета, сложные паки с фул запретом не беру!
ХОЛД посылки - 15$.
Составление писем / общение в чате / перевод текста - 9$
Узнать баланс на карте - 6$
Вбив по телефону 10-30$ (зависит от сложности)
Звоню куда угодно, банки, сервисы, отели,пишите!
Ценник может измениться в зависимости от времени ожидания на линии, сложности и.т.д

Каждому клубню первые 3 звонка всего 5$ каждый!

Голоса: М и Ж с подменой. М конечно же для меня привлекательнее и успехов по нему больше, т.к Ж подменивается через софт.
Опалта: BTC
Контакты: Кто знает пишите на основу. Остальные велком в телегу @totborz
Пишите по любым вопросам, сделаю все, что бы решить вашу задачу.

Translation:

Regular call with number substitution $5

Payment processor call (PayPal / western / skrill) – 10$

Reroute Fedex//UPS – 10-25$ Reroot without a ban, I do not take complex packs with a full ban!

HOLD parcels - $15.

Letter writing / chatting / text translation - $9

Crad balance finding – 6$

Vbiv/Drive-in/Transaction by phone 10-30$ (depending on complexity)

I call anywhere, banks, services, hotels, write me!

Male and female voices.

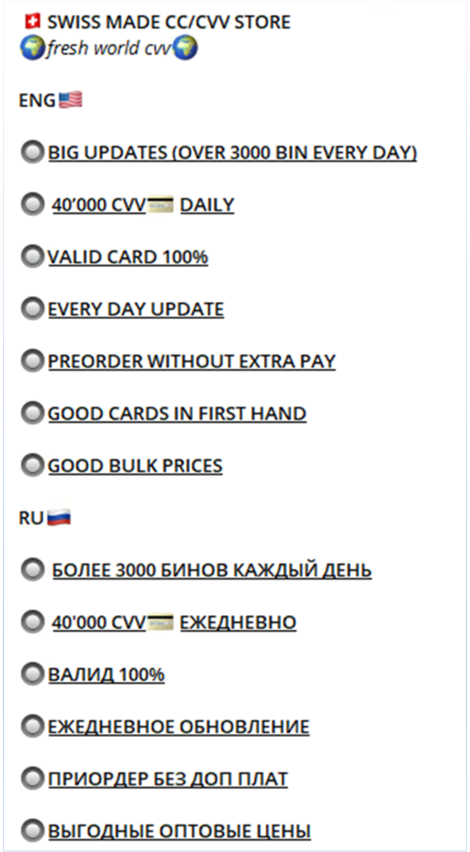
Payment BTC

Access to online banking can also help carders to bypass 3D-Secure authentication such as Verified by Visa or MasterCard Secure Code. This is because some banks allow 3D-Secure codes or tokens to be set up in the cardholder's online banking account. It also allows carders to pass micro-deposit verifications. These are micro transactions of about $1-2 that shops charge a customer's bank account to verify a card. Cardholders need to input the exact amount of the micro deposit charged or confirm the card balance, which they can easily do with access to online banking services.

If the card is already enrolled in online banking, the carder may attempt to perform an account takeover by resetting online banking access using the cardholder's data. This is known as a reroll. Many banks allow cardholders to recover their username and password after verifying their identity. Carders often need more information to reroll than enrol as they may need to answer security questions about the cardholder or provide identity documentation.

Card validation

Credit card validation is the process of confirming that a payment card is genuine and active. Stolen payment card information has a limited lifespan; the card is likely to be deactivated by the bank once the theft or subsequent fraudulent activity is detected. Therefore, when buying cards, one of the most important parameters carders look for is the "valid rate". This is an estimate of the percentage of cards in the set that are still active. However, each card validation attempt bears the risk that an antifraud system detects the activity and subsequently blocks the card. As a result, sellers typically select a small random sample of cards and send them to a specialist card checker service to determine the valid rate.



🇨🇭 SWISS MADE CC/CVV STORE
🌍*fresh world cvv*🌍

ENG 🇺🇸

○ BIG UPDATES (OVER 3000 BIN EVERY DAY)

○ 40'000 CVV💳 DAILY

○ VALID CARD 100%

○ EVERY DAY UPDATE

○ PREORDER WITHOUT EXTRA PAY

○ GOOD CARDS IN FIRST HAND

○ GOOD BULK PRICES

RU 🇷🇺

○ БОЛЕЕ 3000 БИНОВ КАЖДЫЙ ДЕНЬ

○ 40'000 CVV💳 ЕЖЕДНЕВНО

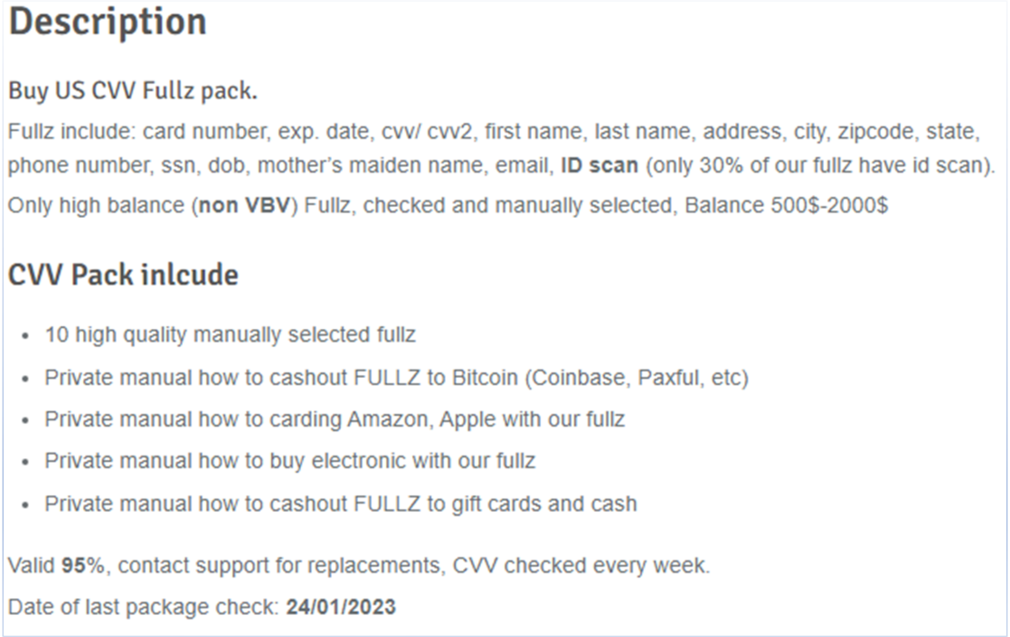
○ ВАЛИД 100%

○ ЕЖЕДНЕВНОЕ ОБНОВЛЕНИЕ

○ ПРИОРДЕР БЕЗ ДОП ПЛАТ

○ ВЫГОДНЫЕ ОПТОВЫЕ ЦЕНЫ

Credit card shop offering 100% card validity



Description

Buy US CVV Fullz pack.

Fullz include: card number, exp. date, cvv/ cvv2, first name, last name, address, city, zipcode, state, phone number, ssn, dob, mother's maiden name, email, **ID scan** (only 30% of our fullz have id scan).

Only high balance (**non VBV**) Fullz, checked and manually selected, Balance 500-2000

CVV Pack inlcude

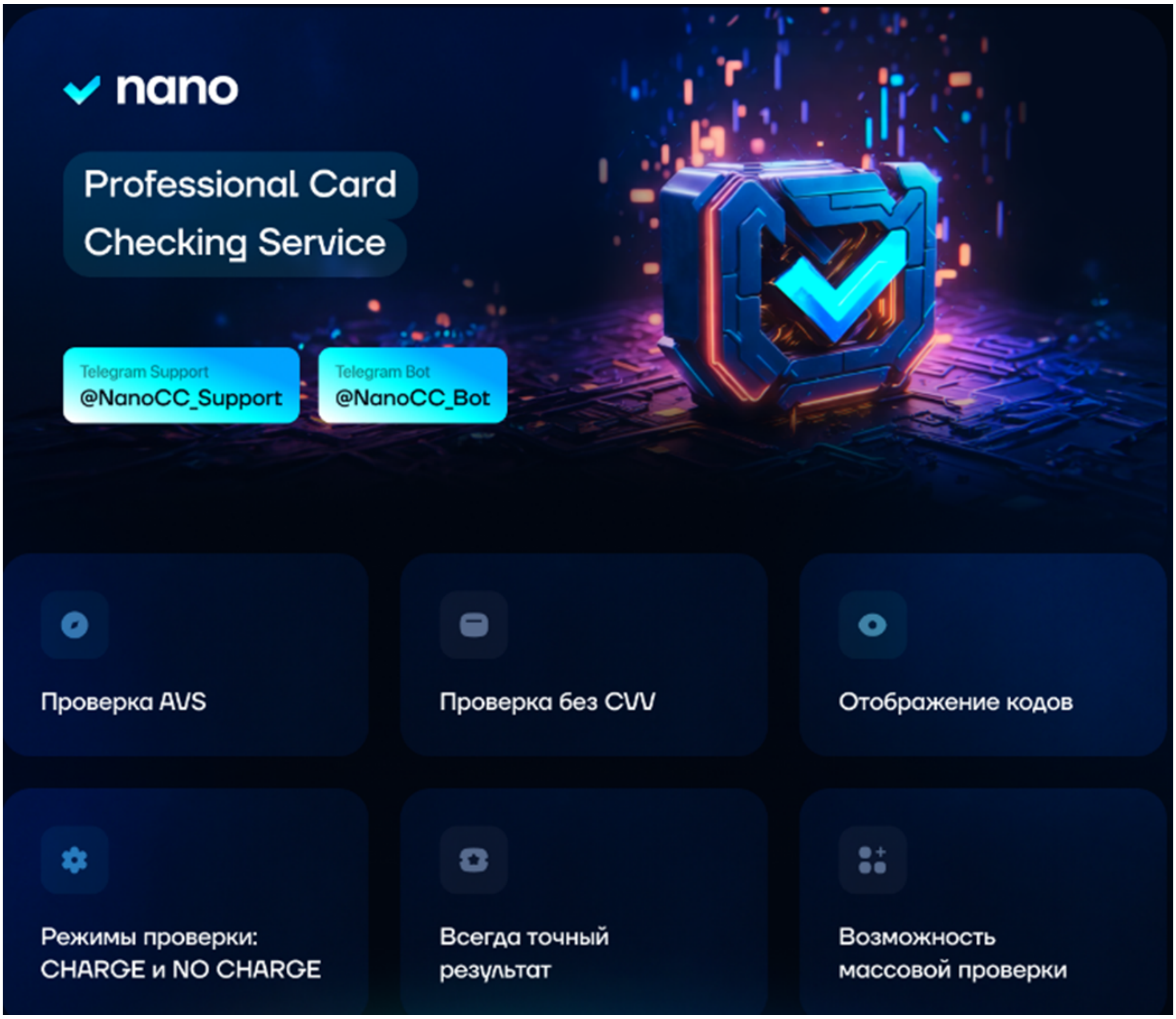
- 10 high quality manually selected fullz
- Private manual how to cashout FULLZ to Bitcoin (Coinbase, Paxful, etc)
- Private manual how to carding Amazon, Apple with our fullz
- Private manual how to buy electronic with our fullz
- Private manual how to cashout FULLZ to gift cards and cash

Valid **95%**, contact support for replacements, CVV checked every week.

Date of last package check: **24/01/2023**

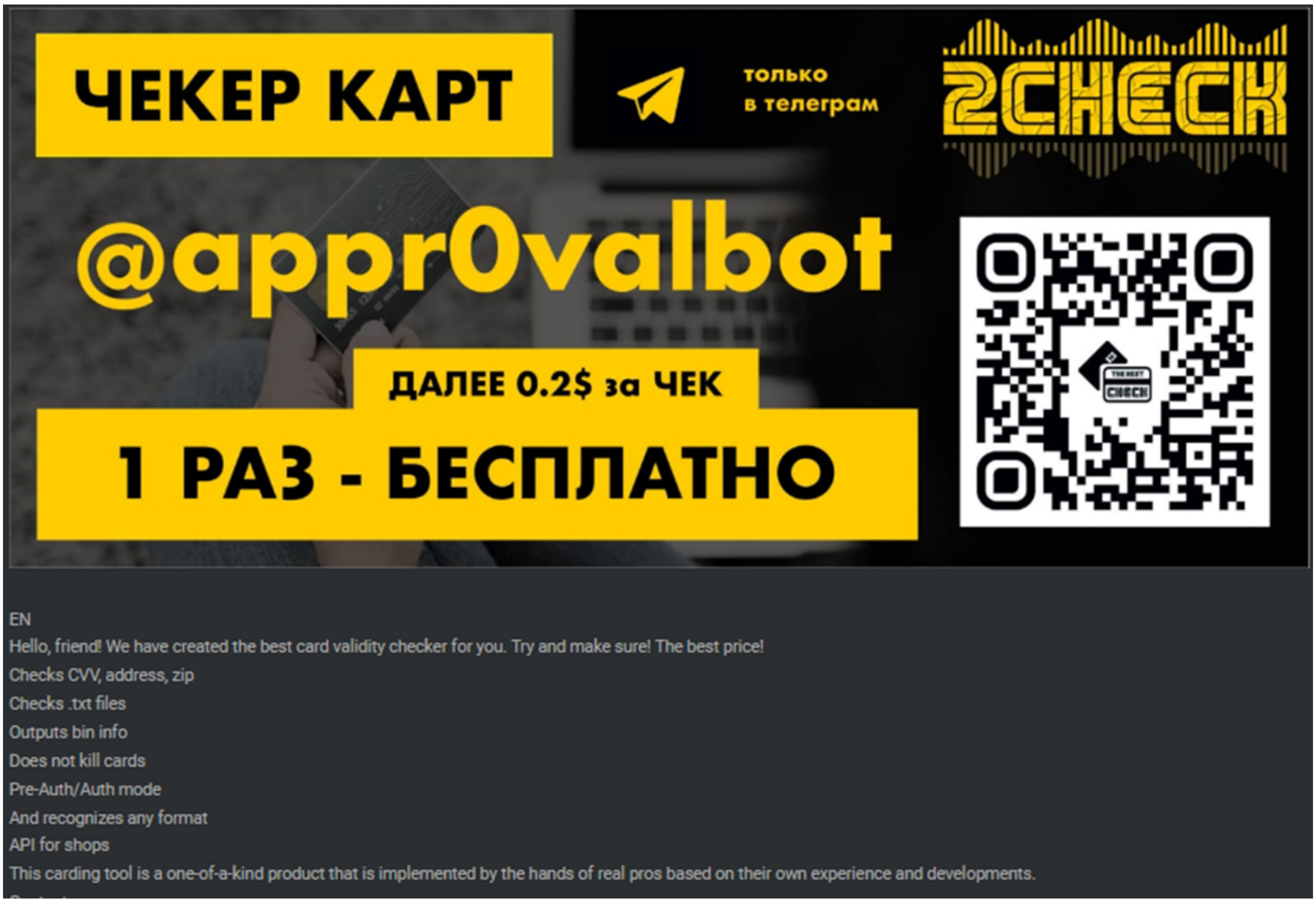
Fullz advertisement with 95% valid rate

Card checker services are third parties that test batches of payment cards for carding marketplaces and vendors. A Russian man allegedly behind one of the most prominent card checker services, Try2Check, was charged by the United States in May 2023 following a ten-year investigation. According to the indictment, Try2Check submitted millions of fraudulent preauthorisation requests to a major US-based payment processor.[11] Preauthorisation requests allow merchants to query a card's validity without charging the card, making them less noticeable to the cardholders.



Professional Card Verification Service includes AVS check, verification without CVV, code display, check modes: charge and no charge, accurate result, mass check ability

[11] https://www.justice.gov/d9/2023-05/kulkov_indictment.pdf [last accessed 19-Jul-23]



EN
Hello, friend! We have created the best card validity checker for you. Try and make sure! The best price!
Checks CVV, address, zip
Checks .txt files
Outputs bin info
Does not kill cards
Pre-Auth/Auth mode
And recognizes any format
API for shops
This carding tool is a one-of-a-kind product that is implemented by the hands of real pros based on their own experience and developments.

Credit card checker, priced at $0.2 for a check

Automated software is also used to check the validity of stolen credit card numbers or guess the missing details (for example, CVV or expiry date). Carders can employ card validation bots to verify credit card information on payment pages at scale, without making fraudulent transactions and tipping off the cardholder. These bots allow carders to test which payment cards are accepted and stored by the e-commerce website, thereby proving that the payment information is valid. Similarly, some carders perform validation by linking cards to paid services, such as social media websites or Google Pay. Successful linkage confirms the cards validity and reduces the risk of card being deactivated, provided that the service also uses chargeless authorisation.

Some carders prefer to employ social engineering techniques to verify cards instead. A popular method is to call the card's issuing bank directly pretending to be the card holder and simply ask about the balance or card limit. Alternatively, carders with access to enough of the cardholder's personal information may choose to enrol the cardholder in online banking and gather the required information from the online banking portal once the card is enrolled.

The consensus on carding forums is that the valid rates for compromised card data are decreasing. In some cases, this is due to vendors selling duplicated card details, giving multiple threat actors access to the same card's information, and resulting in the card becoming deactivated very quickly. Respected carding vendors offer refunds or replacements for invalid cards, under certain conditions. Most vendors give buyers a short window of time after the purchase (for example, two hours) in which to validate the cards and make a claim for any invalid cards. Vendors do not typically take responsibility for, replace or refund cards that have no balance; however, validity of the card is crucial. If a compromised payment card has no balance at the present, it does not mean that funds will not appear in the future. Perhaps the cardholder is waiting for a salary, will take a loan or will receive a money transfer.

Vbiv

Russian carders use the slang term “vbiv” to refer to the process of entering stolen card data into a payment form during an online transaction. Many carders refrain from copying and pasting data into the payment form, as this may trigger fraud detection systems. Instead, they enter the information manually to emulate the behaviour of a real cardholder.

Before the stolen payment card data is used for an online transaction, carders often attempt to match the card’s billing address with the address of their drop to bypass AVS checks. Whilst the address change is being processed, many carders register an account with the merchant using the cardholder’s full name and the drop’s billing and shipping address. The carders then “warm up” the shop by emulating regular customer behaviour to deceive antifraud systems that may be running in the background. Standard activities include browsing products, making inquiries in the live chat and reading reviews.

Many online merchants use 3D-Secure payment authentication services such as Visa Secure or MasterCard Identity Check to add an additional layer of security to the checkout process. When a customer attempts to make a high-risk transaction, they are first redirected to the card provider and must verify their identity before the transaction is completed. To authenticate themself, the customer typically needs to prove knowledge of a secret: either a password associated with the cardholder’s account, or a one-time authentication code, sent via email or text message. Increasingly, biometric authentication through mobile banking apps is also used. This can prevent carders from using stolen payment card data since they do not have access to the secret and should not be able to pass biometric authentication challenges. However, some payment cards, known in carding communities as non VBV or non MSCS cards, do not enforce 3D Secure or allow carders to trivially bypass it. They are therefore less challenging, and as a result, more popular for carders to exploit.

Cashing Out

The ultimate goal for carders is financial gain. Therefore, "cashing out" or extracting monetary value from stolen payment cards is a critical phase in a carding operation. There are many cash out strategies in circulation; some are discussed openly on carding forums, whilst others are offered for purchase. However, highly effective schemes are kept as a closely guarded secret. Once a scheme becomes "saturated", meaning widely known and practiced by carders, its effectiveness diminishes. Therefore, experienced carders prefer to keep details of their schemes private, allowing them to exploit the scheme for as long as possible. In the below sections, we delve into a selection of the most common cash out strategies.

Sale of Card Data

The simplest and least risky method for a carder to cash out stolen payment cards is for them to sell them to other criminals. However, to do this, carders need access to lots of high-quality payment card data. Experienced carding groups leverage their expertise and connections to source fresh compromised payment cards and sell these on carding forums and marketplaces. This is an essential part of the carding value chain, catering to the constant demand for valuable resources by carders and growing number of new carders entering the field.

Online Purchases

With the proliferation of e-commerce platforms and online retailers, carders that possess the necessary expertise can quickly generate income by purchasing high liquidity goods online. These are high value items such as consumer electronics that can easily be resold, either by the carder themselves or through established resellers.

Carders often have the purchased goods shipped to a destination that closely matches the compromised cardholder's billing address to minimise the risk of triggering antifraud systems. To facilitate this, a trusted intermediary known as a "drop" is designated to receive and handle the goods on behalf of the carder until they are resold. Once the goods have been successfully delivered to the drop, the carder or reseller can sell them through multiple channels, including social media groups, e-commerce platforms like Amazon or eBay, regional marketplaces such as Avito, Russia's largest digital marketplace, or acquaintances within their network.

According to many darknet dealers, making online purchases with stolen payment card details is the most popular method of cashing out. It is a versatile and convenient approach, particularly for beginners entering in the world of carding. However, this method has become increasingly complex due to implementation of sophisticated antifraud systems by online retailers. Trusted banks and payment processors incorporate measures such as two-factor authentication (2FA), and 3D-secure authentication schemes such as Verified By Visa and MasterCard SecureCode to fortify their defences. While 2FA does enhance security, it is not foolproof and can bypassed by determined and skilled carders. Common tactics are the use of social engineering to deceive victims into providing their authentication codes, or malware to extract authentication codes from compromised devices.

Evading antifraud systems does not guarantee a successful cash out. If the cardholder notices unauthorised transactions, they can initiate a chargeback claim. Chargebacks result in the freezing of funds and cancellation of orders, preventing the carder from extracting any value from the card. If, upon investigation, the card issuer determines that the transaction was fraudulent or unauthorised, the funds are returned to cardholder, leaving the merchant responsible for covering the chargeback amount and associated fees.

Money Transfer and Payment Services

Money transfer and payment services such as PayPal, Skrill, Zelle, Qiwi and MoneyGram, provide carders with a platform for validating credit card details and facilitating transactions. As a result, they play an important role in carders attempts to cash out.

Account Takeover

One tactic involves exploiting accounts belonging to real users. In this approach, carders gain unauthorised access to legitimate user accounts and then use them to make fraudulent transactions. By leveraging compromised accounts, carders can often bypass some of the security measures implemented by the money transfer and payment services. However, acquiring and maintaining access to such accounts can be complex and risky, as it involves evading detection by the account owner and the service's security measures.

Self-Registered Accounts

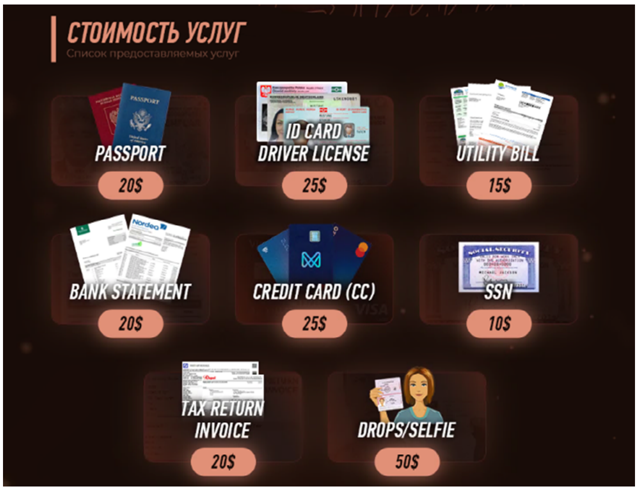
A more common and cost-effective tactic for carders is to use self-registered accounts. This entails creating new accounts within money transfer and payment services using stolen personal information. Carders obtain an individual's personal data from a fullz package and use it to create an account in their name. They can then cash out funds from these accounts to their own designated accounts within the money transfer and payment service. They can also use the self-registered accounts to pay for a wide range of goods, services, and even cryptocurrencies.

Carders need identity documentation that corresponds with the stolen personal data contained in the fullz to execute this cashing out method successfully. This documentation is necessary for authenticating the false identity when creating the self-registered account and must consist of physical documents instead of scans. Document forgery services can provide carders with high-quality forgeries of various identity documentation. An advertisement for a forgery service, Mustang Studio, s shown on the right.

Money Mules

When transferring stolen funds from compromised or self-registered accounts, carders often employ drops to act as intermediaries and obfuscate the money trail. These intermediaries are also known as money mules. Once they receive the funds in their accounts, they transfer them on to the carder or another money mule as instructed for a cut of the transferred value. These subsequent transfers can occur through various channels including wire transfers, cryptocurrency transactions, and even physical cash withdrawals. Money mules can also convert the funds into alternative forms of value such as prepaid cards.

Repeatedly using the same money mule is risky; such patterns can easily be detected by fraud investigators. However, maintaining a network of money mules is difficult for many carders. As a result, third party money-laundering services are in high demand on the dark web. These services offer newly registered banking accounts and credit cards to launder stolen funds through, channelling transactions through an extensive network of money mules. Detecting these funnel accounts presents a challenge for anti-fraud teams, as their activity closely resembles legitimate user behaviour.



Document forgery by Mustang Studio

Merchant Accounts

Russian carders also cash out by creating merchant accounts in payment systems and purchasing non-existent items or services from themselves. This cashing out approach requires the involvement of a reliable drop whose primary responsibility is to register the merchant account under their own name. In the USA, any citizen can open a merchant account by providing the necessary documentation.

The carder creates a fake e-commerce website to purchase goods from. It can be as simple as a publicly accessible blog. The domain and hosting for the website are registered using the drop's information. The website offers a range of goods or services which can be delivered without physical inventory, for example, e-books, software licenses, or online services. The items for sale are carefully chosen to maximise profitability whilst minimising suspicion. The carder then cashes out by making purchases using the stolen card details. Since the items being sold are non-existent, there is no need for actual shipment. The carder simply marks the orders as fulfilled within the merchant account system to complete the transaction and receive the payment directly into their merchant account.

The drop is responsible for withdrawing or transferring the proceeds of the fraudulent sales from the merchant account to the carder or a money mule. Daily withdrawals are common. This is because the fraudulent merchant accounts used for this method have limited lifespans. Banks and payment processors have become increasingly vigilant in detecting them and shutting them down, especially when a high number of chargeback complaints are received. Therefore, carders want to minimise the risk of the account being blocked whilst it still holds a high balance.

Cryptocurrency

Cryptocurrency offers a high degree of anonymity, enabling easy cross-border transfers without attracting the attention of law enforcement agencies. As a result, cryptocurrency exchanges that allow anonymous transactions, particularly those that do not require KYC (know-your-customer) verification, are widely used by carders to cash out. These exchanges allow carders to buy cryptocurrency with stolen payment card information, transfer it to different wallets and sell it for cash. Alternatively, some carders engage in peer-to-peer marketplaces, where they can trade cryptocurrency with individuals directly for cash.

Traceable cryptocurrencies such as Bitcoin are routed through mixer or tumbler services, which combine cryptocurrency from multiple sources to obscure the origin of the funds. This makes it harder to trace the transactions back to the carders. Many Russian carders then use the cryptocurrency to purchase goods on the dark web to resell, or access various services, such as prepaid card providers, VPN services, or online gambling platforms.

Gift Cards

Gift cards offer a higher degree of anonymity than credit and debit cards for making payments. As a result, widely accepted gift cards are easily tradeable, making them a profitable cash out mechanism for carders.

A commonly employed technique is to use compromised debit or credit cards to purchase gift cards directly from legitimate stores. The carder then makes purchases with the gift cards instead of stolen payment cards, allowing them to avoid detection while conducting transactions. Alternatively, the gift cards are resold on underground marketplaces, usually for less than 50% of their face value. The resale price is dependent on the whether the gift card can be used across multiple stores, or is specific to one store, and how in-demand that store is.

Hotels and Flight Tickets

Hotel and flight tickets purchases provide experienced carders with a profitable cash out mechanism. A common scheme consists of the carder operating a fake travel agency, offering discounted flights and hotel accommodation. These are typically priced at around 40-60% of face value. When a customer books a flight or hotel through the fake agency, the carder will use stolen payment cards to make corresponding bookings directly with the hotel or airline in the customer's name.

Alternatively, some carders simply purchase accommodations and flights for use themselves. However, this is highly risky as the carder's personal information can be tied to the fraudulent transaction if booked in their own name.

SIM cards

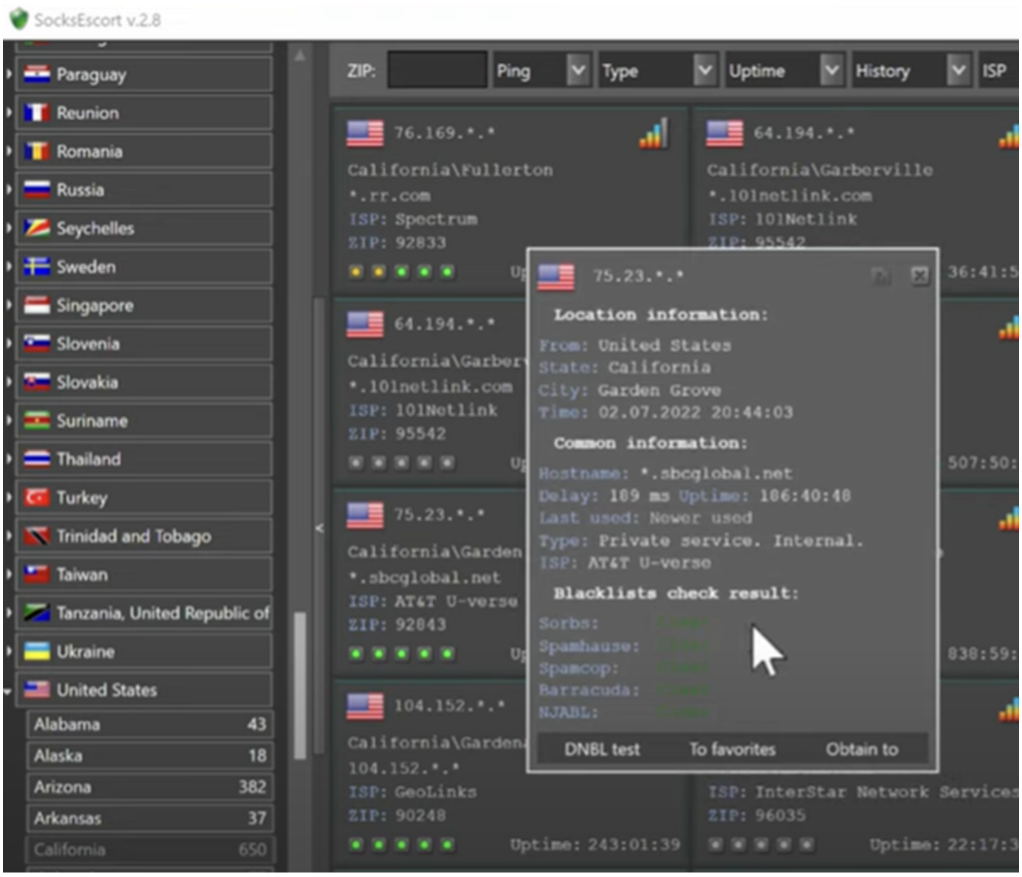
Pay-as-you-go SIM cards hold credit balances, making them potential vehicles for cash out schemes. Russian carders use several international recharge services to top up mobile balances on SIM cards. This allows them to transfer money internationally with less scrutiny. It is also a quicker process than many of the methods discussed earlier, allowing carders to receive funds within hours of acquiring stolen payment card details. The primary downside is that SIM top up amounts are not especially high. Nonetheless, experienced carders can transfer all the available funds from the compromised payment cards before the cards are blocked.

Once a balance has been moved to a SIM card, the carder exploits services that accept payment by mobile phone billing. Examples include online casinos and gambling sites. Some carders employ an advanced version of this method, which bares similarity to the merchant account method discussed above. They register their own premium rate number and make calls using the SIM cards until the balance is exhausted. They can then withdraw the proceeds from their premium rate number's bank account.

Safety, Anonymity and Detection Avoidance

Due to the illegality of carding operations, avoiding prosecution is of paramount importance to carders. Anonymity plays a crucial role in this. However, carders are not operating in a vacuum; they are contending against antifraud and security systems. Therefore, they must not only hide their own identity but present a realistic identity to antifraud and security systems.

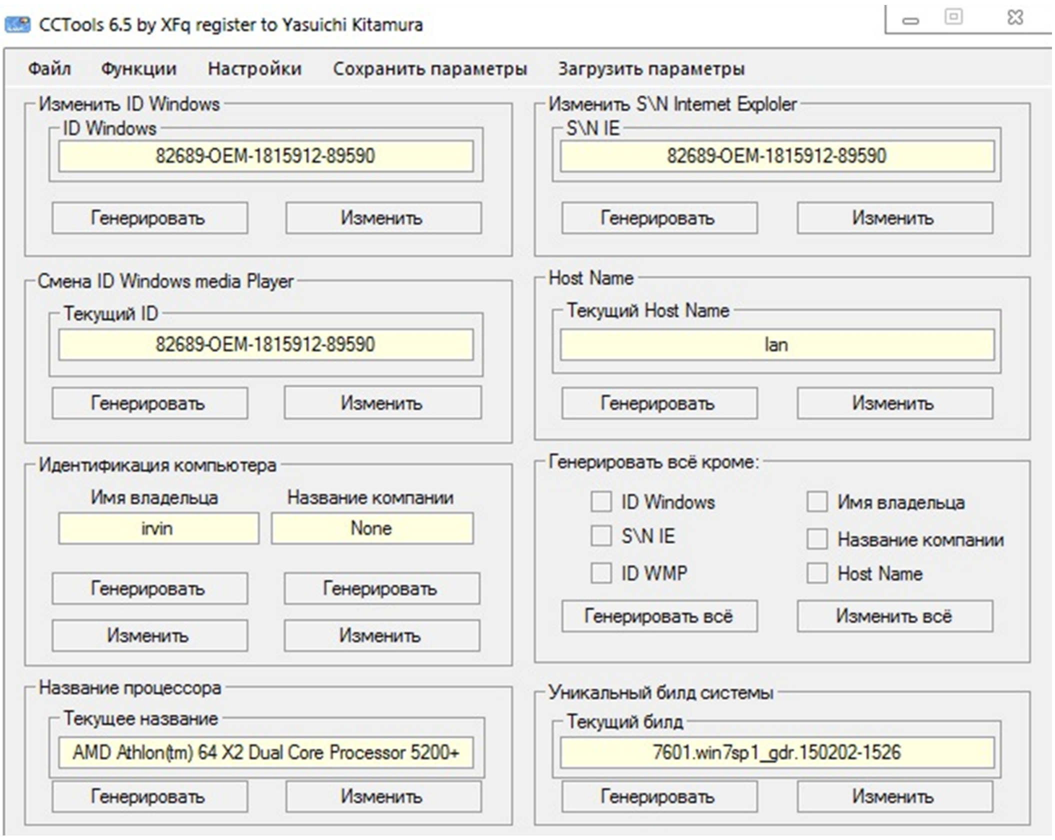
Most carding operations occur digitally, and therefore IP addresses are important identifiers for carders to forge. Almost all carders use VPNs with kill switches to encrypt their internet traffic and hide their true IP addresses and location. The kill switch immediately drops all internet connections if the VPN disconnects, preventing a carder from accidentally leaking their real IP address. From the VPN, connections are routed through a proxy network to present an IP address located in the vicinity of the real card holder. This is to satisfy antifraud systems using IP reputation or location to determine fraud risk.



```
76.169.*.*
California\Fullorton
*.rr.com
ISP: Spectrum
ZIP: 92833

64.194.*.*
California\Garberville
*.101netlink.com
ISP: 101Netlink
ZIP: 95542

64.194.*.*
California\Garber
*.101netlink.com
ISP: 101Netlink
ZIP: 95542

75.23.*.*
California\Garden
*.sbcglobal.net
ISP: AT&T U-verse
ZIP: 92843

104.152.*.*
California\Garden
104.152.*.*
ISP: GeoLinks
ZIP: 90248
Uptime: 243:01:39

ISP: InterStar Network Services
ZIP: 96035
Uptime: 22:17:3

75.23.*.*
 Location information:
From: United States
State: California
City: Garden Grove
Time: 02.07.2022 20:44:03
 Common information:
Hostname: *.sbcglobal.net
Delay: 189 ms Uptime: 186:40:48
Last used: Nower used
Type: Private service. Internal.
ISP: AT&T U-verse
 Blacklists check result:
Sorbs:
Spamhause:
Spamcop:
Barracuda:
NJABL:
```

Many websites and antifraud systems also perform in-depth device fingerprinting. This involves capturing extensive information about a system, including its hardware, operating system, language, fonts, time zone, browser, cookies, and web history. Carding environments are typically locally hosted virtual machines or virtualw private servers, allowing hardware to be configured easily. Russian carders also use software known as CCTools to forge device identifiers and circumvent fingerprinting. It allows them to change system identifiers such as the hardware ID, processor, operating system, and hostname. They also use tools such as CCleaner to delete their browser cookies, history, cache, and plug-ins. Important carding material that is not deleted is encrypted.

The third tactic carders employ to circumvent antifraud systems is behavior emulation. Antifraud anomaly detection systems can flag unusual activity on accounts. Therefore, carders often try to imitate real user actions before and while making transactions.



CCTools 6.5 by XFq register to Yasuichi Kitamura

Изменить ID Windows
ID Windows: 82689-OEM-1815912-89590

Изменить S\N Internet Exploler
S\N IE: 82689-OEM-1815912-89590

Смена ID Windows media Player
Текущий ID: 82689-OEM-1815912-89590

Host Name
Текущий Host Name: Ian

Идентификация компьютера
Имя владельца: irvin
Название компании: None

Генерировать всё кроме:
□ ID Windows
□ S\N IE
□ ID WMP
□ Имя владельца
□ Название компании
□ Host Name

Название процессора
Текущее название: AMD Athlon(tm) 64 X2 Dual Core Processor 5200+

Уникальный билд системы
Текущий билд: 7601.win7sp1_gdr.150202-1526

Prevention measures

Payment card fraud has a significant negative impact on individuals, businesses, and entire economies. The necessity for the robust preventative measures to counteract these threats is undeniable. The Payment Card Industry Data Security Standard (PCI-DSS) imposes a set of 12 principal requirements on entities that store, process, or transmit cardholder data or sensitive authentication data.[12] These requirements aim to prevent the initial acquisition of card data, and are as follows:

1. Install and maintain network security controls.
2. Apply secure configurations to all system components.
3. Protect stored account data.
4. Protect cardholder data with strong cryptography during transmission over open, public networks.
5. Protect all systems and networks from malicious software.
6. Develop and maintain secure systems and software.
7. Restrict access to system components and cardholder data by business need to know.
8. Identify users and authenticate access to system components.
9. Restrict physical access to cardholder data.
10. Log and monitor all access to system components and cardholder data.
11. Test security of systems and networks regularly.
12. Support information security with organisational policies and programs.

[12] PCI-DSS v4.0 - https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

Whilst widespread PCI-DSS compliance can help to stem the tide of compromised card data reaching carding marketplaces, these marketplaces are already flooded with stolen card data. Therefore, preventative measures must extend to preventing validation and use of this stolen card data. A comprehensive and holistic prevention strategy will be challenging for even the most experienced carder to circumvent. Measures to consider include:

- **Location checks** – AVS and IP geolocation checks should be used in tandem to confirm that the shipping address, billing address and IP geolocation match the cardholder's address. Since Russian carders typically attack foreign targets, it is likely that discrepancies will appear between the cardholder's location and the carder's forged location, providing an indicator that organisations can use to detect carding attacks.
- **Velocity checks** – Monitoring for changes in the number of transaction attempts made within a certain timeframe can help organisations detect card validation and cash out attempts. Whilst a sharp increase in failed transactions may be immediately obvious, other increases may require data analysis to see. Organisations should review transaction attempts by BIN, IP address and device fingerprint to uncover signs of carding attacks.
- **Fraud Detection Systems** – Specialist fraud detection solutions can fingerprint and assess users and transactions to help organisations protect themselves from carding activity. Leading solutions employ machine learning to analyse user behaviour patterns and flag suspicious activity, allowing organisations to effectively identify and prevent fraudulent transactions.
- **Bot Management** – Advanced bot management solutions, especially those powered by machine learning and real time behavioural analysis, can help organisations protect themselves against carding related bot activity. This includes card cracking, where carders enumerate missing card details, as well as card validation and credential stuffing. It reduces the scale at which carders can operate, and as a result, the profitability, and the damage they can cause.

It is also important to educate cardholders on how to quickly identify suspicious activity and keep their payment card data safe. Cardholders should be kept informed about common scams that may be perpetrated against them, and the signs to look out for, as well as security measures they can take to protect themselves.

Conclusion

In this whitepaper we have delved into the murky underworld of Russian carding operations and explored the sophisticated techniques they employ. By dissecting the various facets of this cybercrime, we have gained invaluable insights into Russian carding methods and schemes, and the severe impacts they cause.

Russian carding operations are a serious and growing threat, whose prevalence can be attributed to several factors. The underground economy in Russia, characterized by a well-established network of cybercriminals, provides a prolific ground for the development and dissemination of carding techniques. The availability of skilled hackers, advanced technology infrastructure, and a thriving black market also contribute to the growth and sophistication of their operations. However, the impacts of Russian carding operations are not limited to Russia. They are a threat globally. The Western market is their primary target due to its widespread use of credit cards, the reduced chance of prosecuting overseas and the lack of effective security measures in place to protect sensitive financial information.

From initial compromise to exploitation and cashing out, Russian carders are prominently involved in every stage of the carding attack and value chain. They employ social engineering and phishing, skimmers and infostealer malware and even insider access to obtain sensitive payment card and personal information. They steal money and identities, with no regard from their victims. They exploit vulnerabilities in payment systems to launder the stolen funds through intricate networks of money mules in both fiat and cryptocurrency. Their activities can result in significant losses for both customers and businesses.

Consumers may lose their life savings, incur financial charges or have their personal information used for identity theft. Businesses, on the other hand, may suffer financial losses due to fraudulent transactions, and may also incur costs associated with responding to customer complaints and investigating security breaches.

It is important for consumers to take steps to protect their financial information. This includes regularly monitoring bank and credit card statements, using strong unique passwords and two-factor authentication, and being cautious about suspicious emails and phone calls. For businesses, it is vital to invest in robust security measures and resources to prevent and respond to credit card fraud and mitigate the impact of Russian carding. The adoption of advanced technology solutions, such as Netacea Bot Management, can significantly bolster carding prevention efforts. Netacea's machine learning algorithms can analyse vast amounts of data in real-time, detecting anomalies and behavioural patterns indicative of carding activities. By leveraging these technologies, organizations can proactively identify and block suspicious transactions, minimizing financial losses and reputational damage.

Russian carding operations are a persistent threat in the digital landscape, requiring constant vigilance and proactive measures. However, through a holistic and collaborative security approach, we can build a secure and resilient payment ecosystem that safeguards the integrity of financial transactions and builds trust amongst consumers and businesses.

NETACEA

Take the next step

Fix the problem of sophisticated bots with the Netacea platform which combines edge computed analysis with advanced malicious detection and response for 30 times better results.

Book Your Demo

About Netacea

Netacea prevents sophisticated, high-volume, bot attacks that drain value from online businesses. Situated on the far edge of technical infrastructure, the platform combines unrivalled visibility of all traffic across APIs, applications and websites with evolved detection, response and threat intelligence capabilities. The result is more effective automated protection for highly trafficked businesses.

netacea.com