Global Leader
In Cybersecurity

Bitdefender®
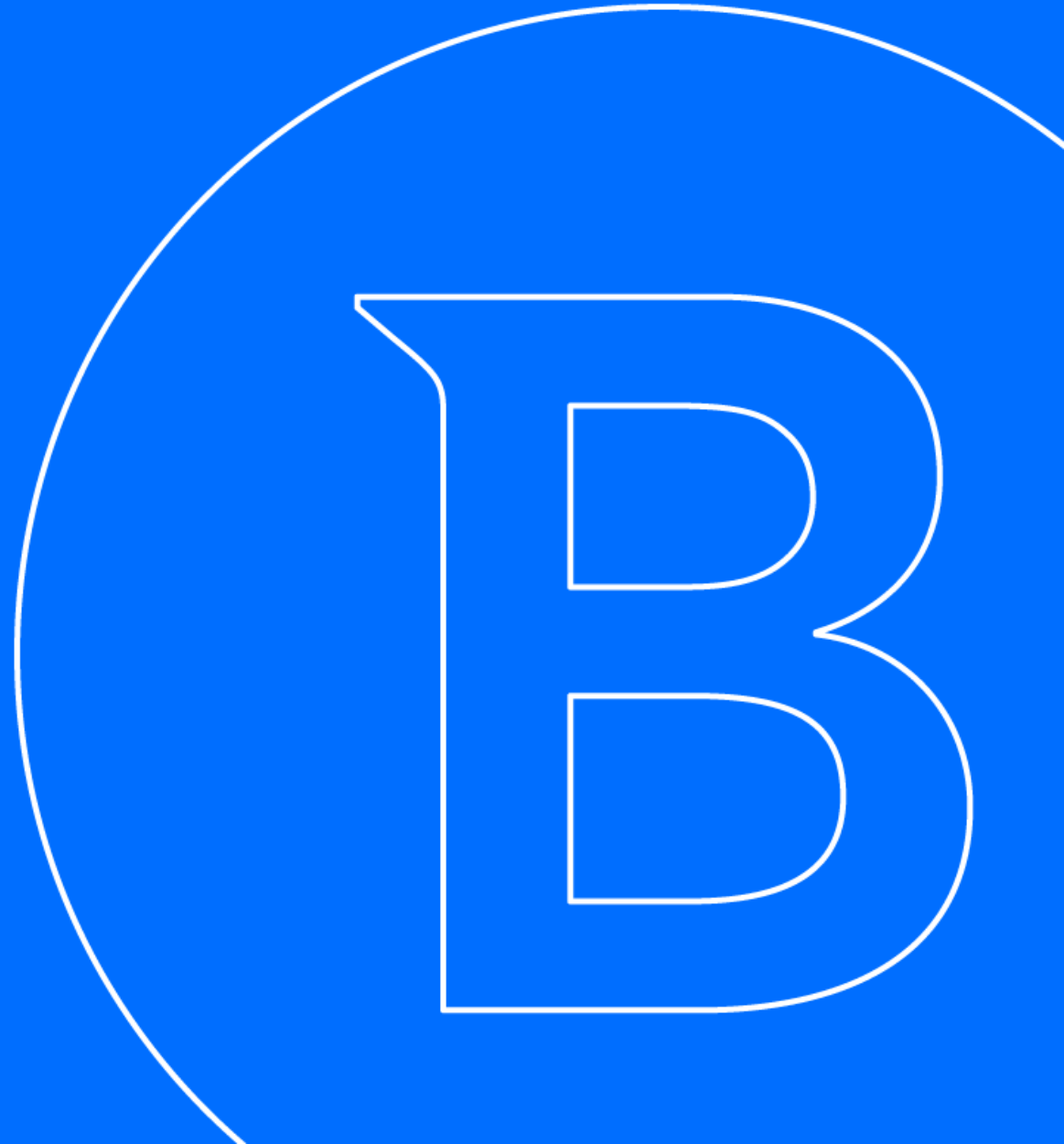
Darknet Report

Everything ends up on the darknet

Bitdefender
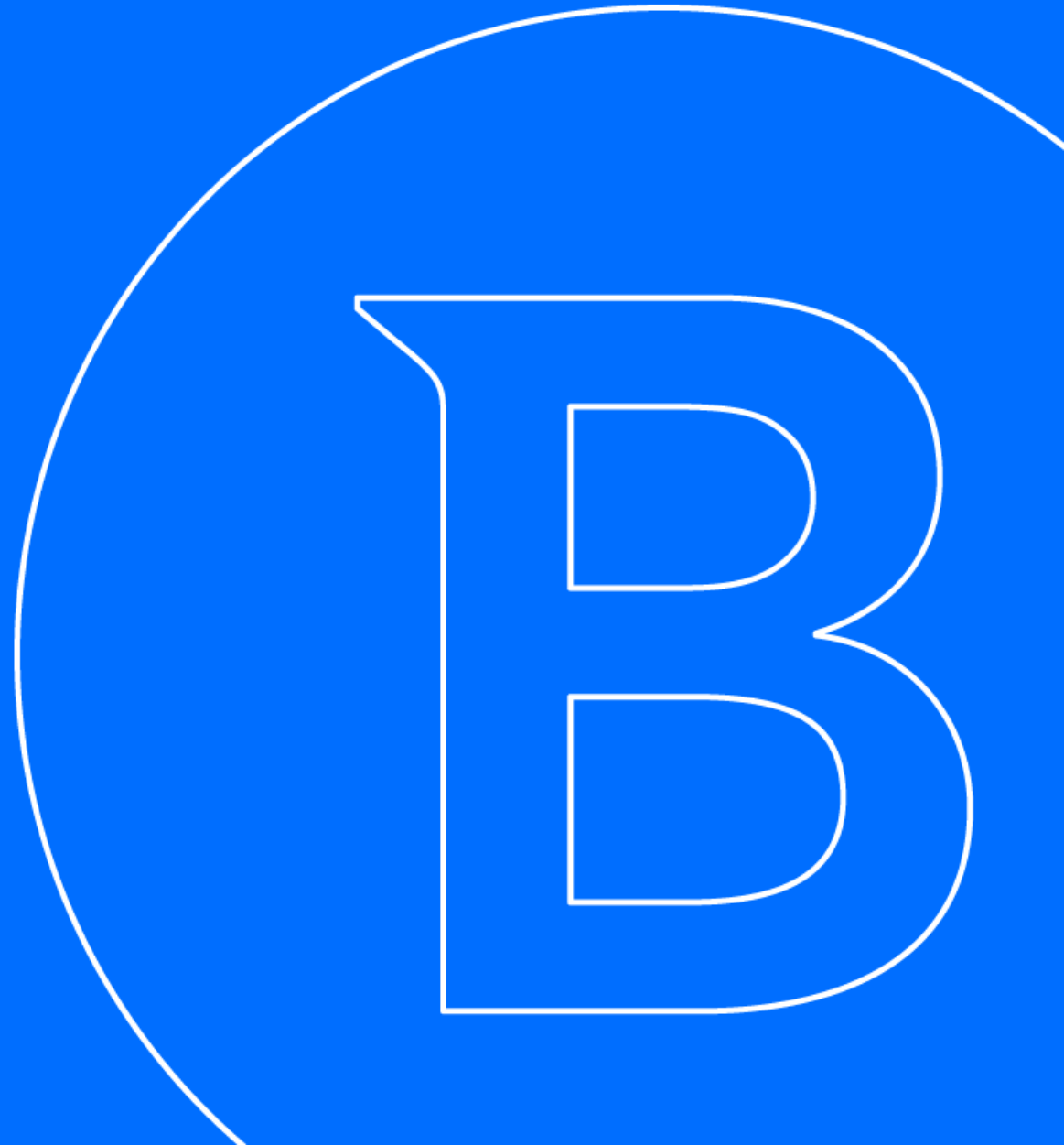
We shouldn't be afraid of the darknet

The darknet in simple terms:

↳ A hidden layer of the Internet, not indexed by traditional search engines

↳ Accessible through specialized software (e.g., Tor, I2P)

↳ Prioritizes anonymity and privacy

↳ Hosts both legitimate content and illegal marketplaces

Why It Matters:

↳ The privacy it offers is attractive to criminals

↳ The darknet is often used for malware distribution, data trade, and other illegal services

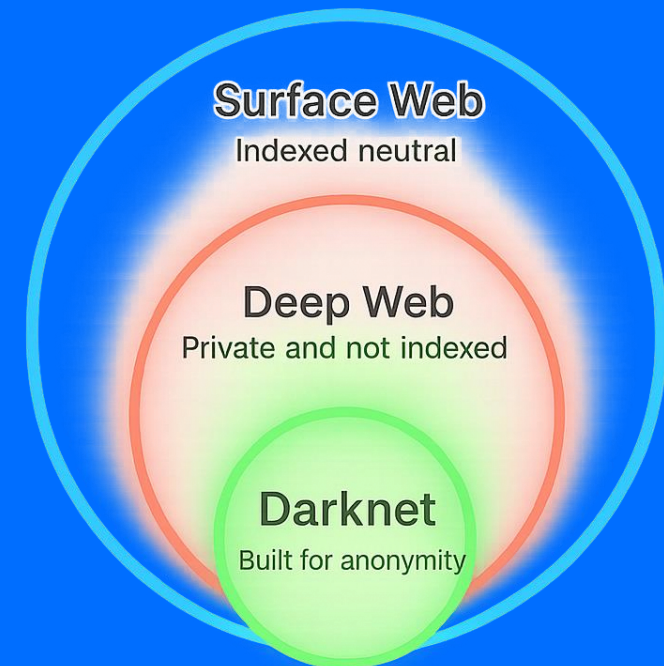↳ Still supports legitimate use cases (e.g., journalism, whistleblowing)

Surface Web

Deep Web

Darknet

Bitdefender
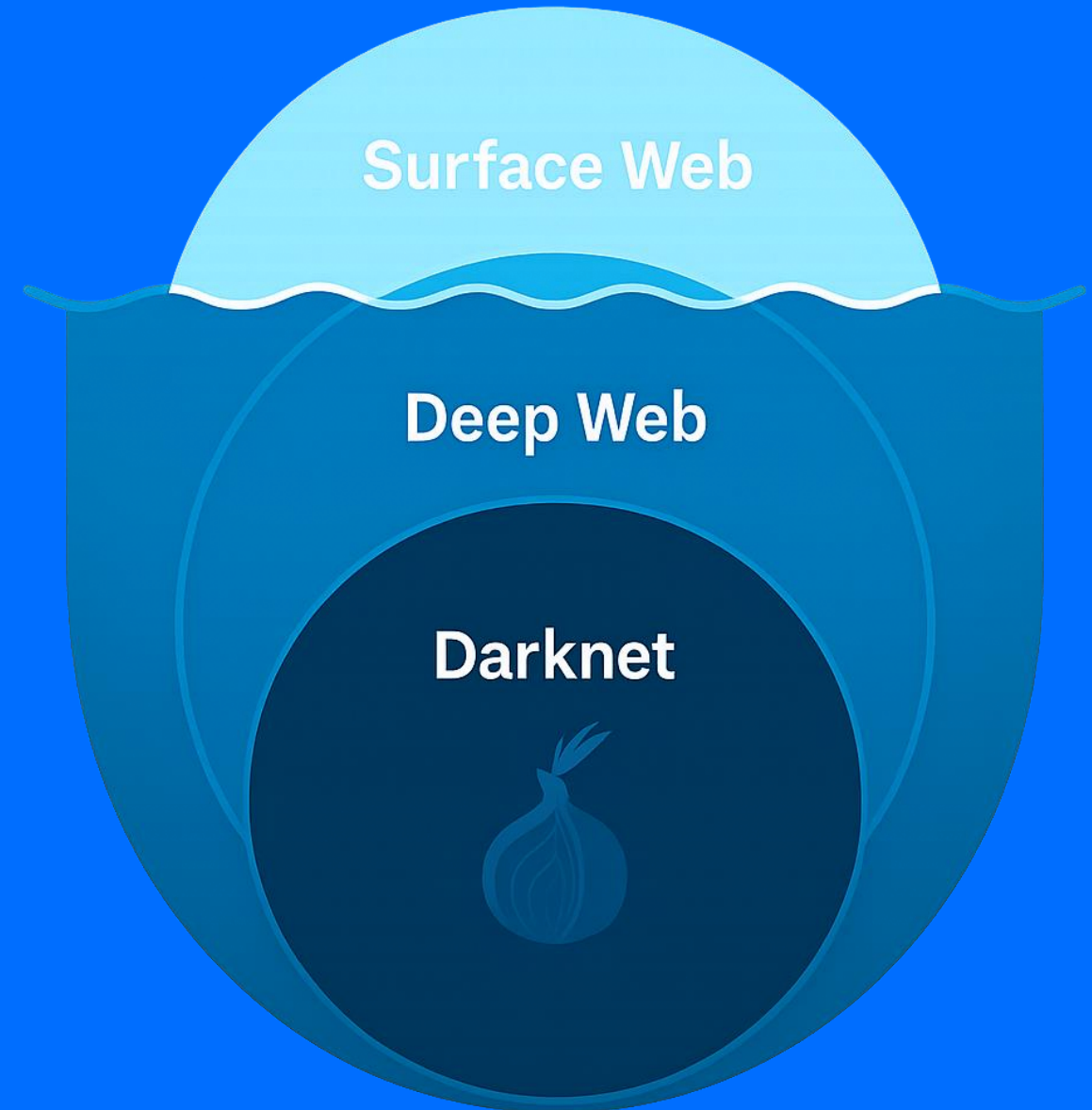
The darknet is not inherently illegal

It sounds ominous, but it shouldn't

↳ The darknet started out as a hidden network from the precursor of the Internet, ARPANET.

↳ It's not inherently evil or bad – it's what people make of it.

↳ There's more than one darknet in existence, but Tor has taken the spotlight.

↳ Criminals are using it because it offers more privacy than the regular internet, but it's far from bulletproof. It's still vulnerable and users can still be found.

Understanding the Darknet

Surface Web
Indexed neutral

Deep Web
Private and not indexed

Darknet
Built for anonymity

Bitdefender

What can you find?

If it's illegal, it's likely for sale.

The darknet hosts sprawling marketplaces where criminals buy and sell:

- ↳ Ransomware kits
- ↳ Stolen credit cards
- ↳ Account credentials
- ↳ Drugs, fake IDs, counterfeit goods
- ↳ Hacking services and exploit tutorials

Some offerings are technically legal — like guides or pentesting tools — but are sold in shady contexts.

And yes, scams are everywhere. Buyers are often scammed by other criminals.
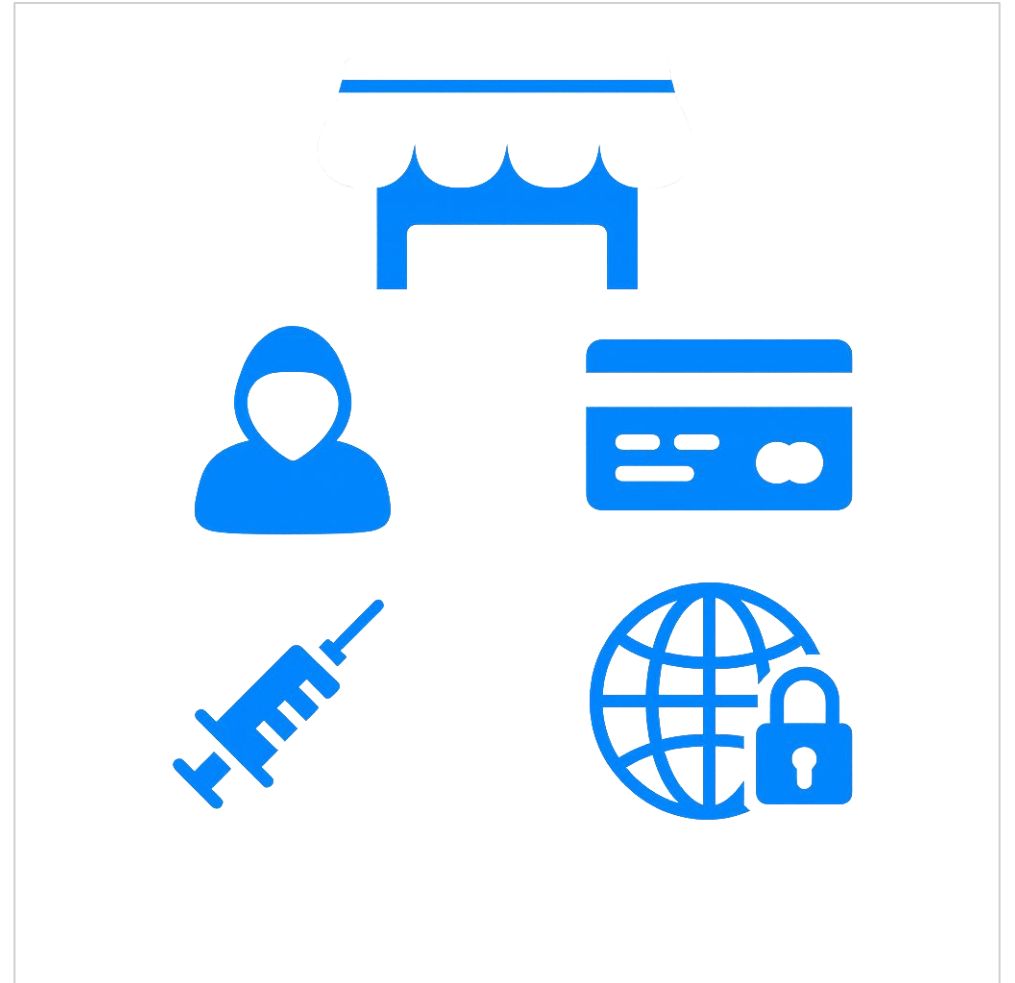
Wannabe hackers and job offers

↳ While the darknet is a place where illegal items and services can be bought and sold, it's also a place where people look for guidance to become hackers themselves.

↳ One reason cybercriminals have become so prevalent today is that it's no longer the sole province of the technologically literate. With a bit of effort and the right tools, becoming a cyber-attacker has become a lot easier.

↳ The darknet is full of people trying to learn to become more proficient, seeking manuals and guidance, and, more importantly, looking to take the first step.

↳ Here are just a few examples of what people might look for on the darknet.

Looking for a rat to steal seed phrases from browser extensions including metamask, exodus, trust wallet the rat…

We are looking for a technically skilled individual who can help us obtain the contents of a specific email without direct access to the mailbox

Hello brothers, I've been trying to teach myself how to code pages from which I can extract information and cookies. I know HTML and CSS pretty well, but I'm not very good with a backend language yet.

Bitdefender

Bitdefender

Ransomware-as-a-Service (RaaS): Weaponizing the darknet

Ransomware-as-a-Service lowers the barrier to entry for cybercriminals. For a subscription fee, attackers get access to:

↳ Payload builders
↳ Hosting infrastructure
↳ Dedicated dashboards
↳ Evasion tools
↳ Customer support

Ransomware is now primarily distributed via RaaS platforms and the darknet remains a key hub for its sale.

Credit cards

- Criminals sell stolen or cloned credit cards through slick marketplaces that mimic legitimate e-commerce shops
- Listings include balance guarantees, card types, and refund policies
- Sites often offer filtering by country, issuer, or card value
- Some vendors provide "customer service" and even money-back guarantees
- To the buyer, it can feel like a normal online shopping experience

Money hub
Credit Cards Money Transfers Gift Cards

Visa Digital Prepaid x1 (3200$)
105 usd
Total Price:

105 usd

Add to cart

VISA
ONLINE CARD
Money hub

We send digital card by email within 1 hour after placing the order.

It is a digital prepaid card for customers who do not need a physical card.

Once you purchase, we will put by email:
1) Information about prepaid card (name, number, exp date, cvv2)
2) Full Guide
3) Proxy and Software

Thus, you will not have any problems with checking security on online shops (3-D Secure).

WASHINGTON
PASSPORT
Bonus Guide included
Non-VBV balance over $8k

All Cards products from Vendor
SNIFFED CC | USA SNIFFED CALIFORNIA
CC NON-VBV | USA CA + DL SCAN
CC USA CA + DL + PASS AND ADDRESS SCAN
SNIFFED CC | USA SNIFFED OHIO
NON-VBV CC | USA OH + PASSPORT SCAN
CC NON-VBV | USA OH + DL SCAN
[Show all 55 products]

Product Description | Terms and Refund Policy | Feedbacks (1)

Product Description

US WA STATE +FULLZ SNIFFED CC + SCAN balance +$8k

Solid card non-VBV with carding guide included + Passport scan included - USA - WASHINGTON STATE

Your order will contain :
- Your CC number + expiry + CVV digits
- Your CC owner's First name and last name
- Your CC owner's date of birth
- Your CC owner's SSN number
- Your CC owner's address
- Your CC owner's phone number
- Your CC owner's Passport scan

...purchasing cryptocurrencies/tokens online and fill your wallet anonymously, use a good VPN ...ng a coinmixer.

...dd the type of card, bin regarding your card on the order message, then I will select what you ...

...ds we provide are sniffed so the validity rate is more than decent.

...d live. No refunds, buy only if you know how to use a card otherwise please : don't buy

Pictures

Postbank

Listing

The account is fully verified and ready to work.
Before ordering, you can select the verification country you need.
If you need other bank accounts, please contact us and we will create you an account at the lowest price on the

Accounts: Before selling all accounts are tested for performance !
If you have problems with the order you need to prove it:
- After purchase record a video of logging into the account
- Date and time must be the same after receiving the order
- Verification takes 1 hour after purchase

Documents: There are no refunds for this product !

Online Business » Drops - Bank
Price (USD): 990.00   Price (XMR): 3.079028395484   Listing type: Escrow   Viewed: 279 times
Stock: Available   Shipping from Dig   :e   Unit: Drop
Minimum order amount: XMR 3.079028395484 | USD 990.00
Vendor: broker01 74 %   Vendor   :les: 18   Disputes: 2 won 1 lost   Open Orders: 0 disputed 0 open

Our Prices

USD cards

1 card with $700 guaranteed and up to $1000 - 60 USD
1 card with $1000 guaranteed and up to $2000 - 140 USD
1 card with $2000 guaranteed and up to $3000 - 210 USD

EUR cards

1 card with 700EUR guaranteed and up to 1000EUR - 60 EUR
1 card with 1000EUR guaranteed and up to 2000EUR - 140 EUR
1 card with 2000EUR guaranteed and up to 3000EUR - 210 EUR

Bitdefender

Bitdefender

Online accounts are highly sought after

Here's why you should never store credit cards in online shops

↳ Online accounts, especially shopping platforms, often store credit card information for convenience. This convenience becomes a security liability when accounts are stolen or sold.

↳ Criminals can resell accounts with full wallets attached, making them far more valuable than login credentials alone.

This example shows an Amazon account with multiple stored cards —a key selling point for darknet buyers

Bitdefender.
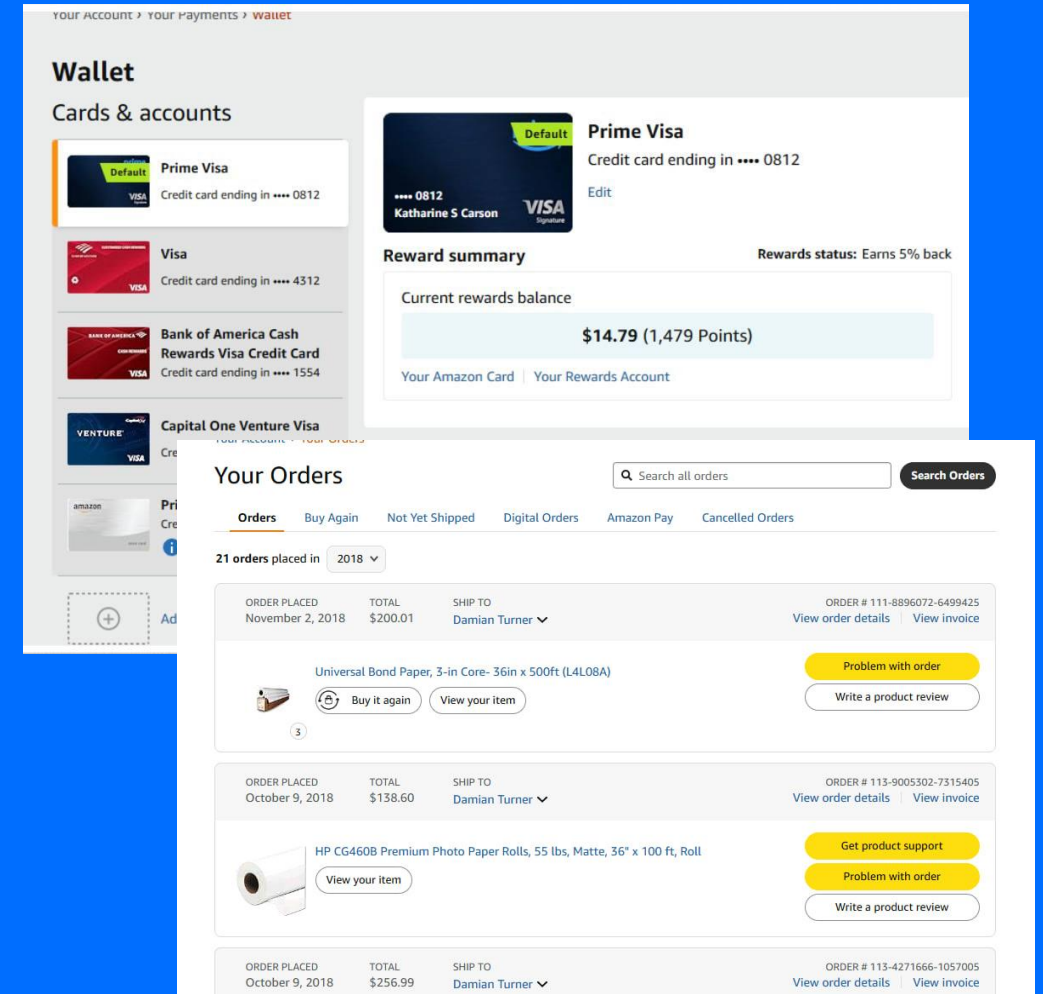
Counterfeiting

The darknet is a hub for counterfeit goods — from fake currency and designer bags to forged documents and IDs.

Listings often include:

↳ Fake US dollars and Euros

↳ Replicas of luxury handbags

↳ Scannable fake driver's licenses and passports

These products are frequently bundled with tutorials, shipping options, and "satisfaction guarantees."

There's a lot of fake stuff; expect to get scammed

Many darknet marketplaces are filled with listings that look legitimate but are outright scams.

They seem to target people who stumble upon the darknet, and who don't realize they're about to get scammed.

Common red flags include:

↳ Prices far below realistic market value

↳ No proof-of-function or vendor history

↳ Listings that spoof government tools (e.g. "FBI hacking toolkits")

These scams often target inexperienced users who land on marketplaces through search or invitation links — not knowing they're being conned.

Bitdefender

Drugs, drugs everywhere

Online drug markets are among the most active areas of darknet commerce, offering illegal narcotics, prescription medications, and counterfeit pills.

⤷ Most darknet marketplaces feature dedicated drug sections with detailed categories.

⤷ Listings include shipping origin, strength, quantity, and stealth packaging options.

⤷ Criminals don't just sell illicit narcotics — prescription-only meds are a growing category.

⤷ Some platforms offer hundreds of listings per vendor, complete with reviews, filters, and payment options in XMR and BTC.

Bitdefender

Hire a hacker or a hack

↳ The darknet is full of listings offering targeted hacks — from phone unlocking and social media breaches to full penetration of cloud or banking platforms.

↳ These services appeal to non-technical buyers who want results without doing the work.

↳ ⚠️ Not every listing is real. Many vendors pose as pentesters or legitimate researchers to disguise their intent, and many buyers get scammed.

Bitdefender.

Streaming services accounts: cheap, disposable, and risky

↳ Darknet marketplaces offer access to stolen Netflix, HBO, Disney+, and other premium accounts for as little as $5–$15.

↳ These accounts are often purchased with stolen credit cards, meaning buyers may unknowingly participate in money laundering.

↳ There's no guarantee these credentials will work for long — sellers rarely offer support, and accounts are recycled constantly.

↳ In some cases, listings are outright scams targeting users looking for "cheap access" without realizing the risk.
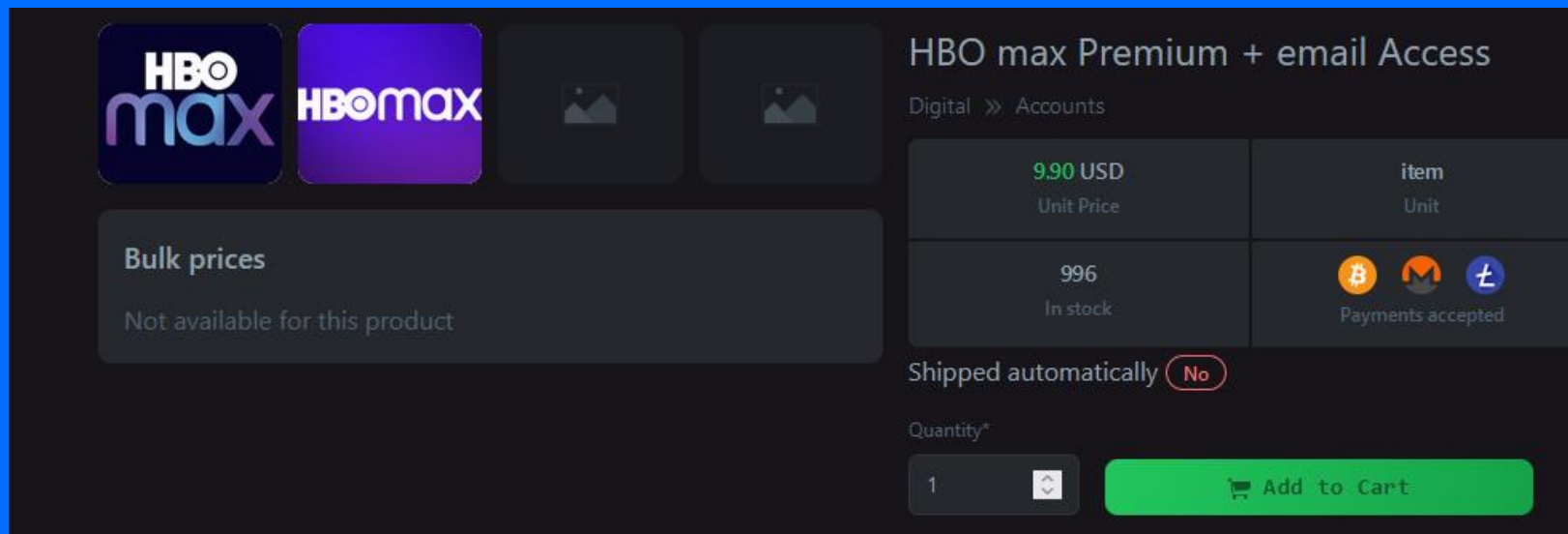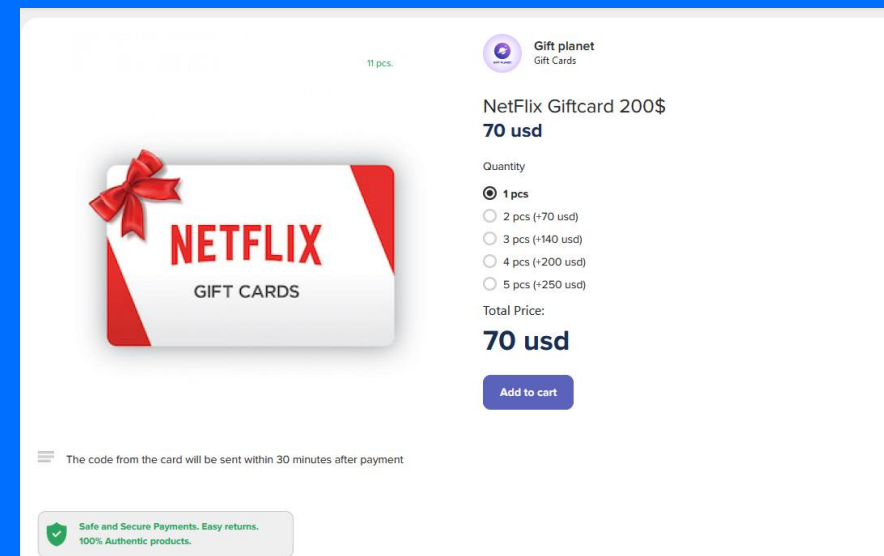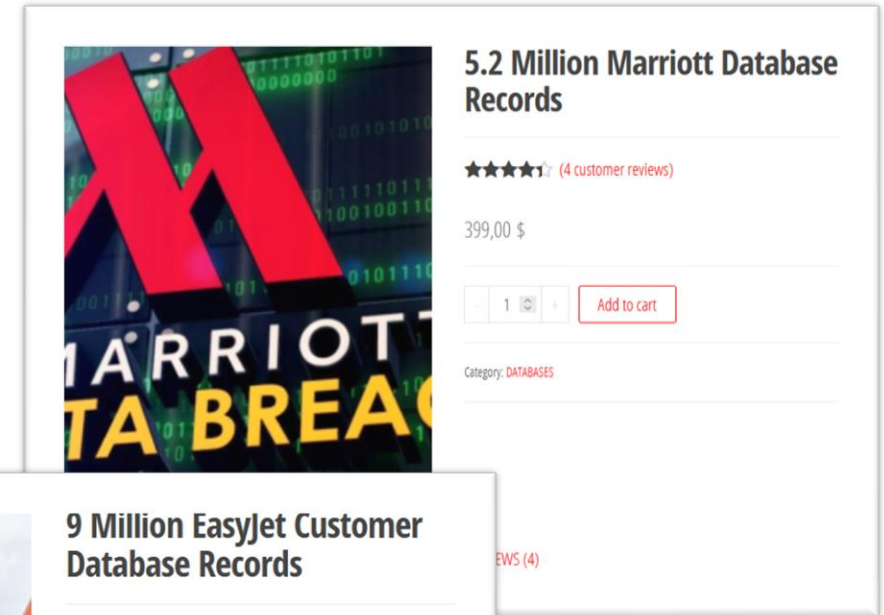
Databases are a dime a dozen

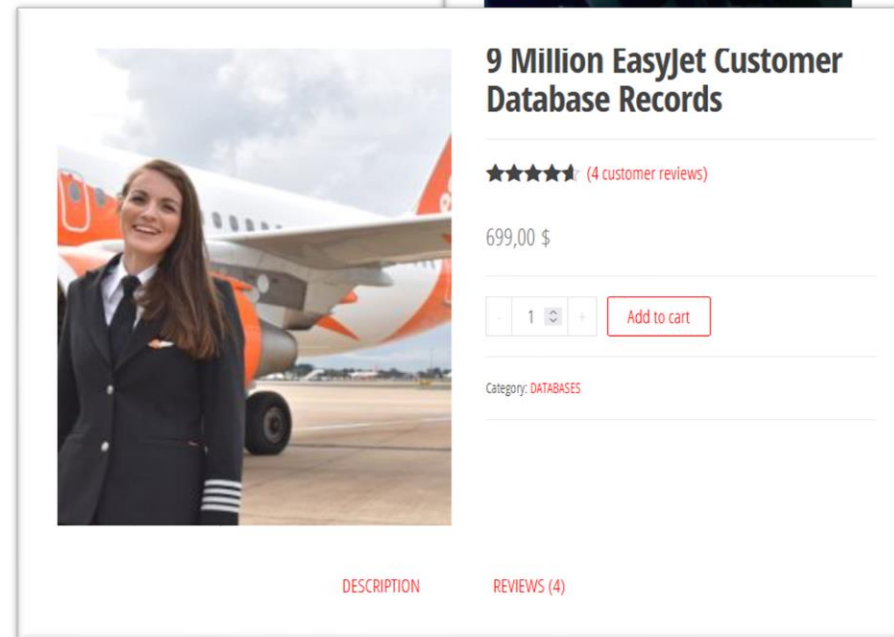Stolen databases from past breaches are among the most commonly sold items on the darknet.

Sellers often bundle:

↳ PII, emails, passwords, and phone numbers

↳ Credential dumps from multiple breaches

↳ Collections totaling billions of records

Even old leaks remain useful for phishing, identity theft, and credential stuffing attacks.

Living off the land

According to Bitdefender Labs, 84% of high-severity incidents in 2025 involved attackers using <u>LOTL (Living off the Land)</u> techniques — tools already built into operating systems.

Just like ransomware, LOTL frameworks are rented on darknet markets. Below is a real-world example offering a PowerShell-based stealer and control panel:

Here are some of the selling points for a *PowerShell Bot Auto Obfuscation Stealer, Grubber, Socks, TV, Shell, HBR HVNC analog* (we list them via text because the ad is in Russian):

↳ Fully written in PowerShell, with C# components for WinAPI interaction

↳ Automatic obfuscation for all modules and builds

↳ Proxy routing to conceal panel address

↳ Detection evasion via network signature manipulation

↳ Modern UI with bot tagging, filtering, and multi-status views

↳ Enhanced security: login requires a password and a pre-assigned user-agent string

💰 Pricing: $4,000 per month with only 5 concurrent licenses available

🌎 Geo restriction: Tool does not work in CIS countries

Something for everyone

↳ Want a $2,000 Amazon gift card for $120? This is the place.

↳ Want to track someone's IP address? Somebody will do it for you.

↳ The latest phone model for a fraction of the price? Look no further!

↳ Need a skimmer kit for ATMS? There's something for everyone.

Bitdefender

Conclusion

↳ Parts of the darknet operate like a full-featured e-commerce ecosystem — but for fraud, malware, and identity theft.

↳ The darknet remains a complex space: originally built for privacy and anonymity, it's now overrun by criminal marketplaces. That abuse distorts the original intent and fuels illicit economies.

↳ Despite high-profile takedowns, illegal forums and vendors thrive, and enforcement has yet to significantly slow the demand.

↳ Cybercrime-as-a-Service has lowered the barrier to entry; anyone can rent tools to cause real harm.

↳ But not all users are winning. One surprising insight: scammers targeting other criminals are often more active than legitimate darknet sellers, proof that cybercriminals can't even trust each other.

B

Trusted.
Always.