As the Dark Web market evolves, its operators adopt strategies and priorities similar to those of traditional marketing and retail businesses. During the 2022-2023 reporting period, significant shifts in Dark Web operations were observed: No clear market leader: Unlike in 2020, 2021, and early 2022, in 2023 no market appears to dominate. In 2022 many previously prominent markets such as ToRReZ and the new AlphaBay were shut down. The gap of these larger sites was filled by several smaller sites, many of which usually disappear within just a few months. However, as explained, this did little to nothing in decreasing the supply of the illegally obtained goods and services sold. Dark web security ops: It appears that after the recent crackdown on the major darknet markets, cybercriminals adopted a new strategy of regularly launching new and smaller sites. Instead of focusing on operating bigger sites (that inevitably get seized by authorities), it seems that cybercriminals now periodically launch new and smaller sites that they then shut down after a few months. This allows them to better evade law enforcement action by attempting to wipe any evidence within just a few months and avoiding becoming big enough to raise too much attention. These new sites are then advertised on various cybercrime discussion forums and Telegram channels. Telegram instead of websites: Telegram has become a major channel for facilitating the sale of hacked personal data. Multiple channels with hundreds of thousands of users exist that facilitate the sale of such illegally obtained goods. As with our previous reports, we gather data by scanning Dark Web marketplaces, forums, and websites. This information is then processed to generate an index of average prices for a broad range of specific products. In December 2022, an estimated 7.5 million credit cards were made available on the Dark Web. The average cost of credit card information varies from $10 (in countries such as the U.S., Canada, and Australia) to $240 each (with a card balance). However, as demonstrated in the table below, there was a small general downward trend in the prices of these items. Product Avg. Price USD (2022) Avg. Price USD (2023) YoY Difference Israel hacked credit card details with CVV $25 $20 -$40 Credit card details, account balance up to 5,000 $120 $110 -$10 Credit card details, account balance up to 1,000 $80 $70 -$10 Cloned American Express with PIN $25 $20 -$10 Stolen online banking logins, minimum 2,000 on account $65 $60 -$5 Hacked (Global) credit card details with CVV $15 $10 -$5 Spain hacked credit card details with CVV $25 $20 -$5 Walmart account with credit card attached $10 $5 -$5 USA hacked credit card details with CVV $17 $15 -$2 Australia hacked credit card details w/ CVV $23 $23 $0 Cloned Mastercard with PIN $20 $20 $0 Cloned VISA with PIN $20 $20 $0 UK hacked credit card details with CVV $20 $20 $0 Stolen online banking logins, minimum 100 on account $35 $40 +$5 Canada hacked credit card details with CVV $10 $30 +$12 ING bank account logins (verified account) – $4,255 – Card.com hacked account – $75 – TDBank hacked account – $30 – United Arab Emirates credit card with CVV – $35 – Here is an example of a USA “Fullz” related posting with 15 confirmed sales: And here is an example of a credit card data related listing: Online payment methods such as mobile payments and payment processors are becoming more popular among retailers. Many people also prefer to buy goods and services online, which allows for more opportunities to steal people’s personal data and financial information. Despite a recent push for security awareness and forcing people to implement 2FA, a huge number of people still become victims of cybercriminals who manage to steal their online payment accounts. The most common type of account details for sale on the Dark Web are PayPal accounts. Because there are so many of them available, they are also very cheap to buy. (A more expensive option would be to get money transferred from a hacked account.) Current prices Product Avg. Price USD (2022) Avg. Price USD (2023) YoY Difference 50 Hacked PayPal account logins $150 $120 -$30 Hacked PerfectMoney account $110 $100 -$10 Hacked Weststein Card account $710 $700 -$10 Hacked TransferGo account $510 $500 -$10 PayPal transfer from stolen account, $5,000+ balances $30 $22 -$8 PayPal transfer from stolen account, $8,000+ balances $60 $54 -$6 PayPal transfer from stolen account, $1,000 – $3,000 balances $45 $30 -$5 Movo.Cash Login $14 $11 -$3 Stolen PayPal account details, minimum $1,000 balances $20 $20 $0 Stolen PayPal account details, minimum $100 balances $10 $10 $0 Stolen PayPal account details, no balance $15 $15 $0 Western Union transfer from stolen account, $1,000+ balances $30 $32 +$2 PayPal transfers from stolen account, $100-$1,000 balance $15 $25 +$10 Hacked Western Union Account $25 $39 +$14 Cashapp verified account $800 $854 +$54 Verified Stripe account with payment gateway $1,000 $1,200 +$200 Stolen UK fully verified Skrill account details $120 $610 +$490 Wise account – verified UK, USA – $1,500 – The table above shows how much the prices of processing account details have fallen in the last year due to the high supply. New payment processing services Our price index grew with the addition of nine payment processing services. New Payment Processing Services Avg. Price USD (2023) Revolut verified account (UK, USA) $1,600 Switzerland online banking login $2,200 Luno Account together with a balance of $5,000 $80 Chase Bank login $500 Payoneer verified account $200 CitiBank verified account $200 HSBC UK Business account $4,200 Barclays online banking login $2,100 Go2Bank hacked account $60 Suntrust Bank account $30 Huntington bank account login $60 Wells Fargo banking login $1,500 Bank of America account login $30 Bluebird Bank account login $75 CBA Random Bank login $25 Chime Bank account login $125 Santander personal bank account $1,800 Here is a listing related to stolen PayPal accounts. Note that it has confirmed sales: And here you can see one related to the payment processor Skrill: And a Revolut listing: Below is our current crypto account listings for the current reporting period (2022-2023). Product Avg. Price USD (2022) Avg. Price USD (2023) YoY Difference USA verified LocalBitcoins account $120 $70 -$50 Blockchain.com verified account $90 $85 -$5 Coinfield.com verified account $120 $140 +$20 Crypto.com verified account $250 $300 +$50 Cex.io verified account $170 $250 +$80 Hacked Coinbase verified account $120 $250 +$130 Kraken verified account $250 $1,170 +$920 Cryptocurrency accounts were the only category that we saw to have experienced an increase. This is likely due to the fact that cryptocurrency prices have been largely stagnating in H2 2022 and H1 2023, which resulted in less interest shown by the mainstream population. As a consequence of this, likely fewer crypto trading accounts and wallets were available for hackers to target. Prices are, however, expected to fall in case of a new cryptocurrency upturn, as this would lead to increased interest and hype from the general public. Prices of hacked cryptocurrency accounts still remain overall the highest among all hacked online accounts. This indicates that hacking such accounts still remains extremely profitable. Below you can find a screenshot of a hacked Coinbase account listing with confirmed sales: We have detected several new items listed on dark web sites that previously were not reported: New Cryptocurrency Accounts Avg. Price USD (2023) Binance verified account $410 Xcoins verified account $350 Bitit.io verified account $450 Bit2me verified account $150 CoinMarketCap Wallet $375 Zen.com verified account $1,600 Nuri account with German IBAN $2,200 Paxful.com verified account – level 1 $20 FTX KYC and verified account $400 Vexel.com hacked account $410 Keybank verified account $180 Wirex verified and hacked account $2,300 Quippy.com verified account $410 US verified Bitrex account $30 Kriptomat.io verified account $410 N26 verified account (Germany) $2,650 Robinhood hacked account $150 Below you can see a listing related to the crypto trading platform Robinhood: Hacked social media accounts are evidence that cybercriminals have a diverse appetite for Dark Web data products. They also offer access to online subscription services for cheaper prices—but customers have to gamble with the chance of being caught. Product Avg. Price USD (2022) Avg. Price USD (2023) YoY Difference Bet365 account $40 $35 -$10 Netflix account, 1-year subscription $25 $20 -$5 Uber driver hacked account $35 $30 -$5 Netflix 4K 1 year $4 $1 -$3 Uber hacked account $15 $12 -$3 Hulu $5 $2 -$2 HBO $4 $2 -$2 Canva Pro yearly $6 $5 -$1 CNBC Pro $3 $3 $0 Orange TV $4 $2 $0 NBA League Pass $7 $8 +$1 Various adult site accounts $5 $6 +$1 Kaspersky account $5 $7 +$2 AirBNB.com verified account – $300 – US eBay account – $200 – Spotify hacked account – $10 – Disney Plus hacked account – $3 – Hacked Alaskaair account – $10 – The main reason why people purchase these accounts is to access content that is not available on their own accounts. The hacked accounts may belong to a country that has a larger selection of streaming sites than their own. This seems strange because people can use a VPN to bypass streaming site restrictions. For instance, a VPN can help you unblock Netflix. These are some examples of different types of hacked online accounts for sale: A thriving category of illicit goods and services sold on dark web markets is that of scans of personal documents. Criminals can use this data to impersonate people on the internet and even open online accounts in their names. One could end up with their details being used to open accounts on various pornographic websites or cryptocurrency trading sites. Another popular category is that of ID and utility bill templates. Buyers can modify these items with any detail they desire. With some real information and some expertise, they can easily produce a collection of fake, authentic-looking documents. This is what we found: Product Avg. Price USD (2022) Avg. Price USD (2023) YoY Difference Minnesota driver’s license $150 $22 -$128 NSW (Australia) driver’s license $150 $40 -$110 Alberta CA driver’s License (scan) $165 $140 -$25 Russian passport scan $100 $80 -$20 USA selfie with holding ID $120 $110 -$10 Utility bill templates $25 $15 -$10 New York driver’s license $70 $60 -$10 US business cheque templates $10 $8 -$2 Custom drivers’ license – $35 – Belgian passport template – $10 – UK passport template – $22 – UK utility bill templates – $10 – Germany passport template – $22 – Forged WalMart prescription Rx labels – $100 – New Hampshire drivers license template – $22 – USA passport scans – $50 – Fake money (mostly in 20- and 50-USD bills) is a very common and easy-to-find item. The most in-demand currencies are euros, the British pound, and dollars from Canada, Australia, and the United States. Some of these bills have a guarantee that they can pass a UV pen test. Usually, these especially high-quality fake banknotes cost buyers around 30 percent of their face value. Document scans that include a selfie with the owner are another useful purchase. This is what an example of a passport template listing looks like: Buyers can also get fake physical documents on the Dark Web. These are the most expensive items on the Dark Web markets by a long shot. Product Avg. Price USD (2022) Avg. Price USD (2023) YoY Difference Poland Passport $3,800 $2,500 -$1,300 Netherlands Passport $3,800 $3,000 -$800 Lithuanian passport $3,800 $3,000 -$800 French Passport $3,800 $3,000 -$800 Various European Union passports $3,800 $3,000 -$800 Nevada ID $160 $200 +$40 New Jersey drivers license $160 $200 +$40 Delaware ID $150 $200 +$50 US driver’s license $150 $200 +$50 Indiana ID $150 $200 +$50 Montana ID $150 $200 +$50 Texas ID $150 $200 +$50 Louisiana ID $150 $200 +$50 Utah ID $150 $200 +$50 Maltese Passport $3,800 $4,000 +$200 Fake US Green Card $160 $450 +$290 Latvian National ID $160 $1,300 +$1140 European Union National ID (avg.) $160 $1,700 +$1,540 Romania drivers’ license – $1,450 – EU drivers’ license (avg.) – $2,000 – France drivers’ license – $1,500 – Poland ID card – $1,700 – Below you can see a listing about someone allegedly selling forged French ID cards: Listings related to various forged documents: Data from email dump is very cheap because it is easy to find and not very reliable. Most email dumps are compilations and collections of other email breaches, so the quality standards are usual—you get what you pay for. Email Database Dumps Avg. Price USD (2023) 10 million USA email addresses $120 100 million USA email addresses $200 5 million UK email addresses $110 1,2 million USA dentist email addresses $200 600k New Zealand emails $110 2,4 million Canada emails $100 Malware can compromise systems running on various operating systems, including Microsoft Windows and Android. Once installed, it grants hackers full access to the machine’s capabilities. This can result in hijacked computer resources through ransomware or stolen user information. Fake online casinos and social networks are common methods for distributing malware. To avoid infection, it’s best to avoid downloading anything from untrusted sources or websites. The table below displays items according to their price, country of origin, and quality indicators. Product Avg. Price USD (2022) Avg. Price USD (2023) YoY Difference Premium-quality, per 1,000 $5,500 $4,500 -$1,000 USA only, medium-quality, 70% success rate, per 1,000 installs $900 $700 -$900 Android OS per 1,000 installs $950 $650 -$300 Europe fresh, high-quality per 1,000 installs $1,800 $1,600 -$200 UK high-quality per 1,000 installs $1,800 $1,600 -$200 USA high-quality, per 1,000 installs $1,700 $1,500 -$200 Europe, medium-quality, 70% success rate, per 1,000 installs $450 $250 -$200 USA, CA, UK, AU med quality, 70% success rate per 1,000 installs $1,200 $1,100 -$100 CA high-quality, per 1,000 installs $1,200 $1,100 -$100 USA, CA, UK, AU low quality, slow speed, low success rate x 1000 installs $800 $700 -$100 Europe, aged, high-quality, per 1,000 installs $1,100 $1,000 -$100 Global, medium-quality, 70% success rate, per 1,000 $115 $75 -$40 Global, low quality, slow-speed, low success rate, per 1,000 installs $45 $35 -$10 Europe low-quality, slow-speed, low success rate, per 1,000 installs $120 $110 -$10 A Distributed Denial of Service (DDoS) attack is designed to disrupt access to websites and other internet resources. This is achieved by overwhelming the targeted website’s server with thousands of connection requests, causing it to crash. While no information is stolen during a DDoS attack, it can be used for extortion or to conceal other hacking activities. The DDoS attacks listed below are characterized by their target, number of access requests, quality, speed, and duration. Note that the duration of a DDoS attack can vary from seconds to days and the results are often proportional to the price paid. Product Avg. Price USD (2022) Avg. Price USD (2023) YoY Difference Unprotected website, 10-50k requests per second, 1 month $850 $750 -$100 Unprotected website, 10-50k requests per second, 1 week $450 $350 -$100 Europe, low-quality, slow speed, low success rate per 1, 000 requests $300 $200 -$100 Premium protected website, 20-50k requests per second, multiple elite proxies, 24 hours $200 $170 -$30 Unprotected website, 10-50k requests per second, 24 hours $45 $35 -$10 Unprotected website, 10-50k requests per second, 1 hour $10 $10 $0 There is no shortage of methods to get hacked, but there are just as many ways to defend against it. By following these suggestions, you can deter unwanted intruders from accessing your accounts at home or work. To minimize the risk of identity theft, consider implementing these strategies: Steer clear of public or insecure Wi-Fi When in a public place or any location where you doubt the network’s safety, employ a virtual private network (VPN) to encrypt all communication. However, if a hacker gains access to the unsecured network you are on, they can easily view your account details and steal or modify your information. If you are interested in selecting a VPN, consult my guide about the best VPNs to the top options. While it may seem inconvenient, it is worth it. Adopt secure ATM habits Inspect ATMs for skimmers. Skimmers are devices attached to ATMs that resemble card readers, but they transmit your card data to a hacker instead of your bank. To check for ATM skimmers: Apply gentle pressure to the card slot’s sides. Look for any loose components, as skimmers are typically mounted delicately and will move when lightly pressed. Examine the edges for glue or tape. If you spot any adhesive material, avoid using the ATM and alert the bank. Abort the transaction if you struggle to insert your card into the ATM. Notify the bank about the issue. Look for counterfeit keypads. Fake keypads may be placed over real ones to record your PIN. They are often poorly mounted, so if the keypad appears to be off-center or wiggles slightly, stop using it and inform the bank. Safeguard your information ATMs are just one avenue through which sensitive account information can be exposed. Never disclose sensitive data over the phone. This applies even when the information is needed for critical procedures, such as registering for Social Security or obtaining a new driver’s license. If feasible, provide the information in person. Utilize anti-malware tools. Install anti-virus or other anti-malware software on your personal computer to scan for malware. Then, configure the update frequency to Automatic. Maintain Account and Password Cleanliness Every location where personal data is stored is a potential target for cybercriminals. Here are some methods to thwart unauthorized access to your data repositories. Refrain from using the same password across multiple accounts. This makes it simple for an attacker to breach your accounts. When a large list of account details is leaked on the dark web, your information can be cross-referenced with other services such as email or banking, so avoid using the same password for them. Terminate accounts that are no longer in use. Cybercriminals can exploit outdated information or use it in password resets or similar attacks. This is particularly dangerous if you reuse passwords for multiple accounts. Employ a password manager. Tools like LastPass or Keepass make it simple to generate robust passwords for all your accounts (with only a master password to remember). Many of these solutions are free. While these guidelines may appear complex and bothersome initially, they will become second nature once you become accustomed to them. This is when you will develop a crucial sense of cybersecurity both online and in everyday life. You may be questioning the relevance of these somewhat technical details. While dark web market data may not offer valuable insights to most individuals, the overall message is evident: Cybercriminals value your data, and stealing your identity or exploiting you is inexpensive. The abundance of purchasable data has led to a bulk sales mentality for dark web customers. Unfortunately, the increasing availability of personal information on the Dark Web results in lower costs—and consequently, a higher likelihood—that your accounts will be compromised. Therefore, the probability of being hacked is unpredictable but on the rise unless you take measures to protect yourself. By adopting a few straightforward rules and habits, you can make it more difficult for hackers to access your data and remove yourself from their line of sight. This not only helps protect your identity but also contributes to your overall cybersecurity in the digital age. Picture the dark web in 2025: a wild, ever-shifting space where tech breakthroughs meet a worldwide hunger for staying under the radar. Last week, I overheard someone in a shadowy chatroom say, “It’s like the Wild West, but with better encryption.” People here crave trades without a trace—think someone in Berlin swapping Monero for rare software, or a vendor in Bangkok listing custom mixes. This guide isn’t just a list—it’s your map through the murky waters of 2025’s standout darknet markets. Abacus Market, the largest Western darknet marketplace supporting Bitcoin payments, has shut down its public infrastructure in a move suspected to be an exit scam. Exit scams occur when the operator of a marketplace decides to vanish with the money they hold in escrow for various transactions between platform users. Blockchain intelligence firm TRM Labs reports that Abacus shutting down so abruptly has all the indications of either an exit scam or a covert law enforcement operation dismantling the activity. Historically, there have been “silent” takedowns that weren’t accompanied by announcements from the authorities, to allow investigations to continue unobstructed and gather more incriminating evidence or identify accomplices. The Abacus Market frontpage advertising illicit substancesSource: TRM Labs Leading force Abacus launched in September 2021 as ‘Alphabet Market,’ and gradually increased its popularity, especially as the number of other markets on the dark web dwindled, mostly as a result of law enforcement actions. In 2022, Abacus was used by 10% of the users on Western darknet markets. It grew to 17% in 2023 and reached a leading status of 70% last year. Abacus dominating the market share in 2024Source: TRM Labs TRM Labs reports that the market had enabled transactions of nearly $100 million worth of Bitcoin but the figure does not include Monero (XMR) cryptocurrency, which requires special conditions to track and accounts for at least two-thirds of all transactions on Abacus. Considering Monero transactions, the researchers estimate that total sales on Abacus were likely closer to at least $300 million. The best month for the darkweb market was this June, when the value of brokered sales peaked at $6.3 million. In what concerns user deposits, TRM Labs reports that the platform received last month an average of $230,000 per day, across 1,400 transactions. This figure dropped quickly in early July, to just $13,000 a day across 100 deposits, as user trust was quickly affected by withdrawal delays. Exit scam unfolding When user complaints surfaced, Abacus’ administrator, “Vito,” said on the darknet forum Dread that the reasons behind withdrawal problems were a sudden influx of new users following the recent shut-down of Archetyp Market, combined with a distributed denial-of-service (DDoS) attack. Admin's explanation on DreadSource: TRM Labs Despite Vito's assurances, daily transaction activity on the site dropped. In the days that followed, Abacus Market’s entire online infrastructure, including its clearnet mirror, went offline without a seizure banner or any indication that law enforcement was involved. Community consensus and users close to the Abacus team ruled out an FBI operation as a likely reason, leaning more towards an exit scam explanation for the sudden takedown of the platform. At publishing time there is no indication that Abacus has been taken down by law enforcement but this scenario is not to be ruled out yet. Contain emerging threats in real time - before they impact your business. Learn how cloud detection and response (CDR) gives security teams the edge they need in this practical, no-nonsense guide. To start using darknet links you should download [Tor Browser] (and then open Onion Links from table above in that Browser As you know, we are also sponsored by quite a few marketsWhat are the advantages of sponsoring the onion shops list 2025?First of all, links to your markets will be placed at the top of the list of darknet markets and, accordingly, will be more carefully checked for performance. But please note that not all darknet markets are allowed to sponsor, so as not to spoil our reputation (it is forbidden to sponsor online markets under the age of more than 4 months, it is forbidden to sponsor markets with bad reviews or reputation). Also, large vendors who do not have their own market, but have a good customer base, can apply for sponsorship. If you want to start sponsoring the darknet markets list 2025, you can fill out the form below and our manager will contact you, then you will receive an answer to the email that you specified in the form. If you pass all quality checks, then on the same day darknet markets list 2025 will coordinate all agreements with you and put up your links! darknet, encrypted network within the Internet that can be accessed only by specialty software or certain software configurations. Darknets may be small and intended just for groups of friends or much larger, like the popular Tor network. Darknet services allow users to remain anonymous online and are often, but not always, associated with illegal activity. However, the term broadly refers to any private file-sharing network that is not accessible by standard search engines.The concept of the darknet is closely related to the dark web, but the terms are not entirely interchangeable. The dark web is the content found on darknet networks. “Darknet” and “dark web” are also often incorrectly used interchangeably with “deep web.” The deep web refers to all parts of the Internet that are not cataloged by search engines. The dark web is just a small part of the deep web. The darknet and dark web can also be contrasted with the “gray web,” which is a part of the surface Internet that one does not need special services to access but is similarly associated with illegal activity. The darknet and dark web are also occasionally confused with the “intellectual dark web,” a loose collection of neo-reactionary thinkers (and not a specific part of the Internet). (However, popular intellectual dark web member Curtis Yarvin helped to found a social network-type platform on the darknet known as Urbit.)The term darknet originated in the 1970s to distinguish between networks associated with ARPANET, the precursor to the modern Internet created by the U.S. Department of Defense, and networks that were not accessible by ARPANET. After four Microsoft employees published the paper “The Darknet and the Future of Content Distribution” in 2002 the term gained wider use in mainstream media outlets. The paper argued that the darknet impeded digital rights management and made it difficult to control access to copyright material.While the dark web is not illegal, mainstream awareness of the darknet is tied to the rise of the Silk Road, an online black market founded in 2011 by Ross Ulbricht. The Silk Road was especially known for its role in the online drug trade but was host to other illegal transactions until it was shut down by the Federal Bureau of Investigation in 2013.A 2014 study found that the most common type of content found on Tor, the most popular darknet, was child sexual abuse material. Darknet sites can also be used to buy and sell illegal weapons, exchange stolen information such as credit card and bank account numbers, offer hacking services, advertise ransomware and other extortion-related technologies, gamble, and launder money.The darknet also includes whistleblowing sites, discussion boards, and social media platforms. Darknet networks host a variety of subcultures. Much of the early cryptocurrency market was accessible via darknet servers, and, despite cryptocurrency’s more mainstream status in the late 2000s, much of the cryptocurrency industry continues to thrive on the dark web, both for ideological reasons and because business conducted on the dark web is much more difficult to regulate. Transactions on darknet-hosted websites are typically conducted using cryptocurrency, especially Bitcoin. Proponents of the dark web argue that it promotes civil liberties, such as free speech and the right to privacy and anonymity. The darknet is thus often associated with anarchist and libertarian ideologies.The most common darknet software is the free and open-source Tor, short for the Onion Router. The software was developed in the mid-1990s to protect U.S. intelligence communications online and is used in conjunction with virtual private networks (VPNs). Tor software, in conjunction with the user’s preferred VPN, conceals the user’s location and IP address and is implemented through layers of encryption, akin to the layers of an onion, from which the service derives its name. While some competing darknet softwares are similar to Tor browsers, they typically exist for different purposes. For example, the network dn42 exists to help users form connections and networks rather than to preserve user anonymity. DarknetStats All the darkweb news you need and more Switch to the dark mode that's kinder on your eyes at night time.Switch to the light mode that's kinder on your eyes at day time.Updated July 5th, 2022Dark Net Markets Features Chart – This chart integrates marketplace data with our hidden Dark Net Markets List stats. Please Note: This chart is not comprehensive, it does not contain all dark net markets, only the established dark web markets. For the full list of dark net markets, visit the hidden Marketplace List. Found an error in the chart? outdated data? Please contact us so we can make corrections and updates! When contacting us, please include links to sources when needed.ATTENTION: For maximum privacy while on the DarkWeb be sure to use a VPN with Tor. This simple software app can save you big time.Alphabay MarketItem typeDetailed StatsNameAlphabay MarketEstablishedDec 2014Main urlalphabay522szl32u4c***r2wm7i5jo54j2eid.onionSupport MultisigSecurity IssuesActive WarningsNone2 Factor AuthenticationFinalize EarlyAllowedCommission2 to 4%Vendor Bond1 XMRForced Vendor PgpYesTotal Listings34k (As of July 2022)Business volume (weekly)N/ACurrent StatusActiveAsap Market Item typeDetailed StatsNameAsap Market (formerly asean market)EstablishedAround Mar-2020Main urlaseanm2r6znqjuackec****4xqbkvdos6eu6qyd.onionSupport MultisigSecurity IssuesActive WarningsNone2 Factor AuthenticationFinalize EarlyAllowedCommission3%Vendor Bond$700Forced Vendor PgpYesTotal Listings18.9k (as of Dec-2021)Business volume (weekly)N/ACurrent StatusActiveMGM Grand MarketItem typeDetailed StatsNameMGM Grand MarketEstablishedMar-2021Main urlbrx5b2mhpmfl3******mtlcrivs6jkaead.onionSupport MultisigNoSecurity IssuesActive WarningsNone2 Factor AuthenticationFinalize EarlyAllowedCommission4%Vendor Bond$200Forced Vendor PgpYesTotal Listings19.5k (As of July-2021)Business volume (weekly)N/ACurrent StatusActiveMajestic GardenItem typeDetailed StatsNameThe Majestic GardenEstablishedN/AMain url MultisigSecurity IssuesActive WarningsNone2 Factor AuthenticationFinalize EarlyAllowedCommissionDonationsVendor BondBy inviteForced Vendor PgpYesTotal ListingsN/ABusiness volume (weekly)N/ACurrent StatusActiveBohemia MarketItem typeDetailed StatsNameBohemia MarketEstablishedJune-2021Main urlbohemiaobko4ce*****fw4pojjwp6762paqd.onionSupport MultisigYesSecurity IssuesActive WarningsNone2 Factor AuthenticationFinalize EarlyAllowedCommission1 to 4%Vendor Bond$200Forced Vendor PgpYesTotal Listings2.1k (As of Oct-2021)Business volume (weekly)N/ACurrent StatusActiveIncognito MarketItem typeDetailed StatsNameIncognito MarketEstablishedJan-2021Main urlincognitolonzsx5x****prys2mpopsmyn3p5id.onionSupport MultisigNoSecurity IssuesActive WarningsNone2 Factor AuthenticationFinalize EarlyAllowedCommission5%Vendor Bond$400Forced Vendor PgpYesTotal Listings2.2k (As of Feb-2022)Business volume (weekly)N/ACurrent StatusActiveVersus MarketItem typeDetailed StatsNameVersus MarketEstablishedDec-2019Main urlq2f7swt5yvbhciqq****ejjlb2jeghd2had.onionSupport MultisigYesSecurity IssuesActive WarningsNone2 Factor AuthenticationFinalize EarlyAllowedCommission5%Vendor Bond$1000Forced Vendor PgpYesTotal Listings35.5k (As of Feb-2022)Business volume (weekly)N/ACurrent StatusActiveKingdom MarketItem typeDetailed StatsNameKingdom MarketEstablishedMay-2021Main urlkingdom2w4iehz343*****gs4oagcmb5id.onionSupport MultisigNoSecurity IssuesActive WarningsNone2 Factor AuthenticationFinalize EarlyAllowedCommission4%Vendor Bond$200Forced Vendor PgpYesTotal Listings5.6k (As of Feb-2022)Business volume (weekly)N/ACurrent StatusActiveRoyal MarketItem typeDetailed StatsNameRoyal MarketEstablishedJune-2021Main urlroyalyygxzq5fadtl******jzsfqqwpvwad.onionSupport MultisigNoSecurity IssuesActive WarningsNone2 Factor AuthenticationFinalize EarlyAllowedCommission4%Vendor Bond$250Forced Vendor PgpYesTotal Listings2.8k (As of Feb-2022)Business volume (weekly)N/ACurrent StatusActiveTor2door MarketItem typeDetailed StatsNameTor2door MarketEstablishedAug-2020Main urlehrddav63e2dou*****q5se4tarh3tqd.onionSupport MultisigYesSecurity IssuesActive WarningsNone2 Factor AuthenticationFinalize EarlyAllowedCommission4%Vendor Bond$150Forced Vendor PgpYesTotal Listings2.3k (As of Jan-2021)Business volume (weekly)N/ACurrent StatusActiveDon’t miss out on new postsThis is strictly a news oriented site that aims to provide insight in the darknet world. We do not collect any kind of commissions/kickbacks from market affiliate links. We do not have any affiliation with any illegal entity nor do we support any illegal activity.Back to Top Tor markets, also known as darknet markets, are online marketplaces that operate on the Tor network. These markets allow users to buy and sell goods and services anonymously, making them a popular choice for those looking to avoid government surveillance or engage in illegal activities. What Can You Buy on Tor Markets? The Silk Road market operated on the Tor network, which masks your identity through IP address anonymity and encryption technology, while allowing you to find other websites on the dark web. Within the Tor network, customers could access the Silk Road, then anonymously connect with vendors to buy illegal goods with cryptocurrency. TOR’s secured browser technology remains the largest anonymizing network, with more than 2 million active users connected directly to its service. For Sale: 1,000 Friends – “perfect As Slaves” Tor markets offer a wide variety of goods and services, ranging from legal items such as books and clothing to illegal items such as drugs and weapons. Some markets also offer hacking services, stolen credit card information, and other illicit goods. How Do Tor Markets Work? Workshop participants reported a sharp increase in crime brought to their attention with a dark web element, and according to one reported study[2], total monetary losses from internet-enabled crime was estimated at more than $1.4 billion in 2016. Naval Research Laboratory in the 1990s and released to the public in 2002. She began her career at JP Morgan as an investment banker in debt capital markets. THOR Industries Global Family Of Companies Tor markets operate using the Tor network, which allows users to access the internet anonymously. This means that users can access the marketplaces without revealing their IP address or location. Transactions on Tor markets are typically conducted using cryptocurrencies such as Bitcoin, which further enhances the anonymity of the users. In some ways, the dark web offers more browsing freedom, but the lack of safeguards can leave you exposed to hackers, malware, and other online threats. Before you access deep web sites, you need to be aware of the dangers that can lurk on the dark web, such as viruses or other malware. ProtonMail is a Swiss-based encrypted email service that doesn’t require personal information when you sign up. Technology Partnerships Probably the most infamous Tor parasite yet was the Silk Road market used to trade drugs, weapons, indeed anything illegal. Tor has long had its dark side but the scale of its use by criminals appears to have expanded quite rapidly in the last year. Kaspersky Lab had uncovered evidence of 900 services using Tor, said senior researcher Sergey Lozhkin, equivalent to 5,500 nodes (server relays) and 1,000 exit nodes (servers from which traffic emerges) in total. At the end of February 2023, there was a change in the management of the Infinity Forum. KillMilk put the Infinity Forum up for sale for unknown reasons, which may be good news that the forum may be disbanded, but KillNet has since relaunched its Telegram forum. KillNet’s Telegram forum is a different form created by managing multiple chat groups from the same hand; this forum also includes a market that offers the same services. Are Tor Markets Safe? Kingdom Market was an English-speaking marketplace operating since March 2021. It offered more than 42,000 items for sale, including around 3,600 products from Germany. German police claim that “tens of thousands of customer and several hundred seller accounts” were registered on the marketplace. Upon sale, the vendor would send the buyer geographic coordinates and a picture of where their well-hidden purchase could be found. The landscape of “loader” malware services is anticipated to continue its evolution, offering increasingly stealthy loaders to cybercriminals. These loaders, which act as an initial vector for malware infections, pave the way for deployment of stealers, various remote access Trojans (RATs), and other malicious tools. The key capabilities of these loaders are expected to include robust persistence mechanisms, fileless memory execution, and enhanced resistance to security products. The ongoing evolution of loaders on dark markets is likely to see the introduction of new versions written in modern programming languages like Golang and Rust in 2024. This trend signifies a concerted effort by cybercriminals to enhance evasion techniques and improve the efficacy of initial infection vectors. The payment is held in escrow by the site operator to discourage scammers. Furthermore, other value-driven security tasks are likely to suffer when teams have to manually browse these marketplaces and hunt for threats or signs of your digital footprint. Avast One helps you hide your online activity, while featuring an array of other security and privacy tools, including online banking protection, data-breach monitoring, and anti-malware detection. DarkOwl has assigned assets to monitoring and collecting data from the new AlphaBay Marketplace, despite their increased crawler detection measures and ongoing server instability. In doing so, Pavlov is alleged to have facilitated Hydra’s activities and allowed Hydra to reap commissions worth millions of dollars generated from the illicit sales conducted through the site. Using Tor markets can be risky, as many of the goods and services offered are illegal. Additionally, the anonymity of the Tor network can make it difficult for law enforcement to track down and prosecute those who use the markets for illegal activities. It is important to exercise caution when using Tor markets and to only engage in transactions with reputable vendors. Frequently Asked Questions What is Tor? Tor is a network that allows users to access the internet anonymously. It is often used to access darknet markets and other websites that are not indexed by search engines. What is Bitcoin? Bitcoin is a digital currency that is used to make transactions on the internet. It is often used on Tor markets because it allows for anonymous transactions. Are Tor markets illegal? Many of the goods and services offered on Tor markets are illegal, but the markets themselves are not necessarily illegal. However, using Tor markets to engage in illegal activities can result in criminal charges. How do I access Tor markets? Tor markets can be accessed using the Tor browser, which can be downloaded for free from the Tor Project website. Conclusion Tor markets offer a unique way to buy and sell goods and services anonymously, but they also come with a number of risks. It is important to exercise caution when using Tor markets and to only engage in transactions with reputable vendors. Additionally, it is important to remember that many of the goods and services offered on Tor markets are illegal, and engaging in illegal activities on the markets can result in criminal charges. In early July, 2025, Abacus Market, the largest Bitcoin-enabled Western darknet marketplace (DNM), went offline, rendering all internet-facing infrastructure, including its clearnet mirror, inaccessible. TRM Labs assesses that the marketplace’s operators have likely conducted an exit scam, shutting down operations and disappearing with users’ funds. However, law enforcement may also have covertly seized the marketplace. Abacus’s exit follows the June 16, 2025 law enforcement seizure of Archetyp Market, marking the latest in a series of shutdowns in the Western DNM ecosystem. How the likely exit scam unfoldedIn late June 2025, users began reporting withdrawal issues with Abacus Market, which typically indicates an impending exit scam. The marketplace’s administrator, known as ‘Vito’, responded on darkweb discussion forum Dread, claiming an influx of Archetyp users and a distributed denial of service (DDoS) attack were the reasons for the issues.Screenshot of Abacus admin’s Dread post explaining why the marketplace was downDespite this reassurance, most of the DNM community remained skeptical. This was reflected in the sharp decline in deposit volumes to Abacus between June and July, 2025. Between June 1 and June 27, 2025 average daily deposits to Abacus were USD 230,000 across 1,400 transactions. However, from June 28 to July 10, 2025, this dropped to USD 13,000 across just 100 deposits.Abacus’s rise to the top of the Western DNM ecosystemAbacus Market launched in September 2021 as Alphabet Market, before rebranding in November 2021. Although it served a global audience, it particularly focused on the Australian market, incorporating Australian cultural references into its marketing and recruiting an Australia-dedicated moderator. Abacus offered a wide range of illicit drugs, including stimulants, dissociatives, psychedelics, opioids, benzodiazepines, prescription medication, unlicensed pharmaceuticals, and cannabis-related products. Unlike competitors, such as Archetyp, DrugHub, ASAP Market, and Incognito Market, Abacus operated as a central deposit wallet, multisignature DNM that supported both Bitcoin and Monero.Abacus’s market share adding upSince its inception, Abacus Market has gradually increased its market share in the Western DNM ecosystem. In 2022, it ranked as the fourth largest Bitcoin-supporting Western DNM with 10% of market share, rising to 17% in 2023. In 2024, its share surged to over 70%, following ASAP Market’s voluntary closure in July, 2023 and the law enforcement seizure of Incognito Market in March, 2024. In total, Abacus Market generated nearly USD 100 million in Bitcoin-enabled sales. However, considering that Monero — a privacy coin — typically accounts for two-thirds to three-quarters of total volume, Abacus’s sales are likely closer to between USD 300 million and USD 400 million.The rise of Monero amid DNM declineTRM Labs analysis shows that nearly half of the marketplaces launched in 2024 accepted only Monero — a sharp increase from just over one-third in 2023. This signals a growing preference among darknet operators for obfuscation and anti-surveillance tools. Cryptocurrency-enabled drug sales also grew by over 19% from 2023 to 2024, reaching nearly USD 2.4 billion in volume. During the same period, the number of newly launched darknet marketplaces declined 42% year over year — indicating that while the ecosystem is consolidating, remaining actors may be becoming more operationally advanced.What’s behind this likely exit scam?Dread’s administrator, Hugbunter — who was in close contact with the Abacus team — believes Abacus’s disappearance was not the result of a law enforcement action. In some cases, such as Nemesis Market’s exit, official seizure notices have appeared months after a DNM has gone offline. However, when a DNM collapses — especially a large and reputable market — its users typically migrate to the nearest available platform. For example, ASAP Market’s closure likely prompted its vendors and buyers to migrate to Abacus, as evidenced by a 20% increase in Abacus’s volume compared with the month before ASAP Market shut down. Furthermore, following Archetyp’s law enforcement seizure in June, 2025, many of its users flooded Abacus Market, leading to the latter’s largest ever monthly sales volume of USD 6.3 million in June 2025. Did Abacus’s success lead to its closure?Abacus becoming the largest Bitcoin-enabled Western DNM may have inadvertently led to its closure. Marketplaces that reach the top of the ecosystem, in terms of volume, user base, listings, and reputation, often become priority targets for law enforcement. Archetyp’s recent takedown followed this pattern and likely influenced Abacus’s trajectory. Faced with the decision between profit seeking and self preservation, Abacus’s admins likely chose the latter in light of Archetyp’s seizure and the surge in new users that elevated Abacus’s profile. Furthermore, after four years of operating and generating substantial profits, the admins likely lost motivation to continue and chose to exit the ecosystem to preserve their freedom and financial gains.Previous DNM admins who either voluntarily exited, such as ASAP Market, Agora Market, and WhiteHouseMarket, or conducted exit scams, such as Evolution Market, while at the top of the ecosystem have yet to be apprehended by law enforcement.The darknet ecosystem remains highly adaptiveEven as major darknet platforms fall, TRM Labs data shows that the ecosystem remains highly adaptive. Following the 2022 shutdown of Hydra Market, TRM identified new Russian-language darknet markets emerging that by 2024 accounted for more than 97% of global darknet drug revenues. Although some darknet operators, particularly of Western darknet marketplaces, have historically attempted rebrands or exit scams following law enforcement action, full-scale rebuilds appear to be becoming less common.What’s next for AbacusAbacus Market’s exit underscores the ongoing instability of Western DNM landscape. Sustained law enforcement pressure has stymied marketplaces’ development, curtailed innovation and increasingly driven users toward independent vendor shops and encrypted communication platforms like Telegram. It has also meant most new Western darknet marketplaces are generally low-effort projects, such as 3DogsMarket, Drugula Market and Squid Market, built using scripts and beset by security flaws, with the sole aim of generating quick profits before disappearing. Abacus’s demise marks a significant setback for the Western DNM ecosystem, leaving successors such as DrugHub, TorZon Market, and MGM Grand under increasing pressure to adapt. These platforms must now answer the same question as their ill-fated predecessors: pursue growth at the risk of disruption, or prioritize self-preservation in an increasingly hostile environment?Will law enforcement continue targeting the largest DNMs?While law enforcement typically continues to target the largest darknet marketplaces like Archetyp, it has moved away from multi-DNM takedowns such as 2014’s Operation Onymous. Instead, law enforcement agencies now appear to focus more closely on the vendors. Without vendors, darknet marketplaces cannot operate or generate profits, making them a more strategic enforcement target. Arresting vendors often has a greater disruptive impact than taking down DNMs. When a marketplace is shut down, vendors can typically migrate to other platforms. But when a vendor is arrested, their activity is disrupted across every DNM they operate on. As a result, law enforcement has adopted an intelligence-led enforcement strategy incorporating DNM takedowns into longer-term investigations rather than treating them as end goals.Cases like Nemesis Market and Monopoly Market indicate that law enforcement agencies now prefer to take down DNMs without announcing it publicly — and potentially alerting vendors under investigation. This allows them to compile intelligence and make arrests at optimal moments. In the interim, many in the DNM community will assume the marketplace performed an exit scam and continue their activity on other platforms. This strategy was successfully tested in 2017’s Op. Bayonet/GraveSac, and has become the preferred method for disrupting the ecosystem. As darknet marketplaces continue to disappear without warning, whether through exit scams or unannounced law enforcement operations, blockchain intelligence firms, such as TRM, remain a key component to help investigators. Such companies’ tools enable investigators to trace administrator wallets and follow illicit flows even after a marketplace goes offline. TRM will continue to closely monitor the evolving DNM landscape, including emerging platforms, vendor migration patterns, and on-chain activity, to support efforts to disrupt illicit actors and safeguard the broader crypto ecosystem.{{horizontal-line}}FAQsWhat happened to Abacus Market?Abacus Market — once the largest Bitcoin-enabled Western darknet marketplace — went offline in early July 2025. TRM Labs assesses the event was likely an exit scam, though a covert law enforcement seizure cannot be ruled out.Why did Abacus Market gain popularity in Australia?While not based in Australia, Abacus Market gained strong traction with local darknet users by embracing cultural references, supporting Australian vendors, and featuring a dedicated moderator from the region. These efforts helped it become one of the most active platforms among Australian users.How did Abacus Market’s exit impact the darknet ecosystem?Abacus’s collapse removed one of the most dominant players in the Western darknet market space — causing disruption across vendors, accelerating migration to other platforms, and increasing pressure on successors like DrugHub and TorZon Market to adapt in a rapidly changing environment.Was Abacus Market taken down by law enforcement?Although no seizure banner appeared, and darknet forum administrators claimed no enforcement action was involved, some users still speculate that law enforcement may have covertly shut down the site — a strategy seen in previous operations against darknet platforms.What drove the sharp decline in Abacus Market activity before it disappeared?In late June 2025, Abacus users reported withdrawal issues and decreasing trust in the platform. Daily deposits dropped by over 90% in the final weeks, despite reassurances from its administrator. This behavior was consistent with known exit scam patterns seen across other darknet markets.

- how to thread a singer heavy duty sewing machine bobbin
- what does camelot mean in english
- lanotija
- http://wixoon.hu/upload/file/d9d61a1e-ed81-4db9-a9c1-221f2bbeb6bd.pdf
- http://bursaceyizgelinlik.com/images_upload/files/42419233340.pdf