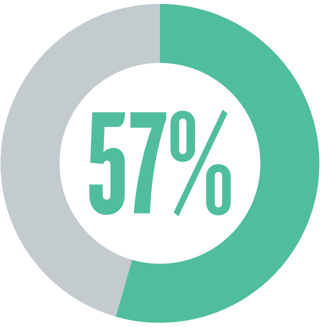
SpyCloud

Innovation on the Dark Web:

Third-Generation Markets and How Bad Actors are Keeping Pace



of the dark web hosts illegal content *related to drug sales, weapons trafficking, counterfeit currency, terrorist communication, and more.*

Overview

Emerging dark net markets are now setting the foundations for the third generation of buying and selling on the dark web. Simplicity of use and enforced encryption seem to be common themes on new markets. These countermeasures are likely a reaction to the paranoia that followed the shuttering of second-generation dark markets like the AlphaBay and Hansa. Coordinated law enforcement operations continue to target established markets and websites.

Meanwhile, some new markets are exit scamming their own clientele. An exit scam is a con where an established business stops shipping orders while continuing to receive payment for new orders. By the time customers realize they've been scammed, the business has already disappeared.

Silk Road represented the public inception of dark web commerce and second-generation markets are continuing to dwindle after 2017's coordinated takedowns. As markets' staying power has come into question, vendors and their customers have developed innovative ways to continue their operations and stay in touch. Key innovations we've observed on the dark web involve implementation of mandatory public-key crypto in market messaging, automated metadata stripping from images, "trustless" bitcoin multisignature implementation for payments, and walletless payments.

In an effort to help empower our customers with knowledge, we're sharing our observations as more old, dark markets go offline and new ones emerge.

Demystifying the Deep & Dark Webs

By now, the terms "dark web" and "deep web" are seemingly ubiquitous. You may have heard them used in commercials for identity theft protection services that claim to "scan the dark web" for criminals who are capitalizing on your personal information. These advertisements paint pictures of a mysterious hooded figure hawking your personal information to the highest bidder. But the dark web and the deep web are not one in the same.

The "deep web" refers to any part of the internet which is not already indexed by traditional search engines. This includes information that is password-protected, such as the contents of email or social media accounts. The deep web also comprises internal indexes, such as online library catalogs, anything that requires vetted access, or web pages and databases that cannot be crawled. Your personal Facebook account is considered a part of the deep web, as is your alma mater's campus library catalog. As such, the deep web holds vastly more data and resources than does the comparatively miniscule "surface web." The surface web only accounts for 0.03 percent of the entire internet, with the "dark web" comprising an even smaller fraction of web addresses on the deep web. In terms of size, the surface web is truly just the tip of the iceberg.

DEEP WEB

The portion of the Internet that is hidden from conventional search engines, as by encryption; the aggregate of unindexed websites.[1]

DARK WEB

The portion of the Internet that is intentionally hidden from search engines, uses masked IP addresses, and is accessible only with a special web browser.[1]

FULLZ

A term used by cybercriminals that refers to personal information which can be used to make fraudulent credit card purchases, take over accounts to sell later, or commit wire transfer fraud or tax fraud.

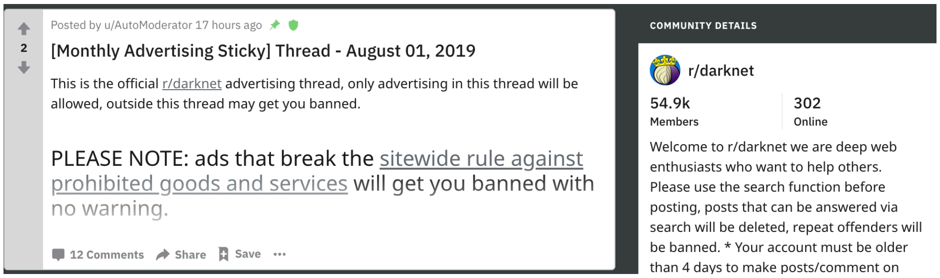
[1] Dictionary.com

The dark web, however, lives up to its seedy reputation. Small as it may be, researchers estimate that 57 percent of the dark web hosts illegal content related to drug sales, weapons trafficking, counterfeit currency, terrorist communication, and more. Today's dark web landscape is dynamic and volatile. Last year we wrote about *The New Dark Markets*, which initially survived 2017's dark web market seizures. Even as dark market vendors are ensnared in sting operations, dark markets persist; now in their third generation, they're smaller than ever but continue to adapt and evolve.

Recovering from the 2017 Takedowns

The 2017 ***Operation Bayonet***, a coordinated effort between Europol and U.S. law enforcement agencies, was responsible for the takedown of the largest-ever dark net markets. At its height, the AlphaBay Market boasted over 400,000 members. It offered a selection of products ranging from cocaine and fentanyl to compromised account credentials, firearms and fullz. Operation Bayonet also took down Hansa, the second-largest dark net Market after AlphaBay, in July 2017.

Despite these seizures, dark net criminal enterprises have not disappeared. The initial aftermath of the AlphaBay seizure led well-known personas on dark net markets to flock to unlikely venues. The r/DarkNetMarkets SubReddit, which has since been banned from Reddit for soliciting prohibited goods and services, served as the initial forum for AlphaBay refugees to regroup. Today, the r/onions and r/darknet offer clearnet forums for discussion. These discussions are much more tame and feature site-wide rules against the solicitation of prohibited goods, which include firearms, ammunition, drugs, paid sexual favors, stolen goods, falsified documents and personal information. This rules out the majority of services which are offered on dark net markets.



Posted by u/AutoModerator 17 hours ago

[Monthly Advertising Sticky] Thread - August 01, 2019

This is the official r/darknet advertising thread, only advertising in this thread will be allowed, outside this thread may get you banned.

PLEASE NOTE: ads that break the sitewide rule against prohibited goods and services will get you banned with no warning.

COMMUNITY DETAILS

r/darknet

54.9k Members

302 Online

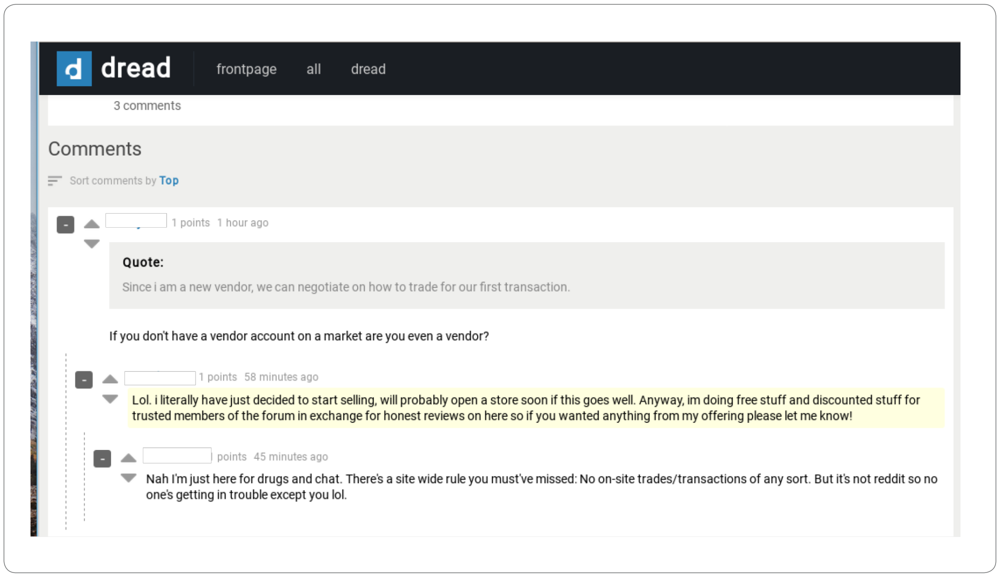
Welcome to r/darknet we are deep web enthusiasts who want to help others. Please use the search function before posting, posts that can be answered via search will be deleted, repeat offenders will be banned. * Your account must be older than 4 days to make posts/comment on

Figure 1: Screenshot of the r/darknet subReddit.

Immediately after these markets were seized, the savviest of fraudsters often preferred to sell dumps directly to their most trusted clients rather than to random customers of dark net marketplaces. With the inception of the dark web *Dread* forum, criminals could network and form new relationships with potential customers, allowing for the opportunity of more direct sales.

In the example below, a vendor took to Dread to discuss his new business. The vendor says he is new but he probably sold on AlphaBay or Hansa in the past. Likely wary of law enforcement, *With the inception of the* ***dark web Dread forum,*** *criminals could network and form new relationships with potential customers, allowing for the opportunity of more direct sales.*

he says that he will sell first to "trusted members" before opening his own shop. According to the indictment against AlphaBay kingpin Alexandre Cazes, several of the market's drug vendors were ensnared in sting operations by buyers who were able to trace packages back to their originators. While Dread bans open trades or transactions, members have still attempted to attract potential clients on the forum.



3 comments

Comments

Sort comments by Top

[redacted] 1 points 1 hour ago

Quote:

Since i am a new vendor, we can negotiate on how to trade for our first transaction.

If you don't have a vendor account on a market are you even a vendor?

[redacted] 1 points 58 minutes ago

Lol. i literally have just decided to start selling, will probably open a store soon if this goes well. Anyway, im doing free stuff and discounted stuff for trusted members of the forum in exchange for honest reviews on here so if you wanted anything from my offering please let me know!

[redacted] points 45 minutes ago

Nah I'm just here for drugs and chat. There's a site wide rule you must've missed: No on-site trades/transactions of any sort. But it's not reddit so no one's getting in trouble except you lol.

Figure 2: Screenshot of the dark net: "Dread" forum

"I'm just here for the drugs and chat," said the member. "There's a site-wide rule you must've missed: No on-site trades/transactions of any sort. But it's not Reddit so no one's getting in trouble except you lol." The policy doesn't forbid members from promoting their businesses on the site.

The New Dark Markets Fighting Back

After the fall of AlphaBay, a new "AlphaBay Clone" market emerged. The resemblance between the new "Empire Market" and "AlphaBay Market" is uncanny. Empire market, much like AlphaBay, includes a nearly identical design.

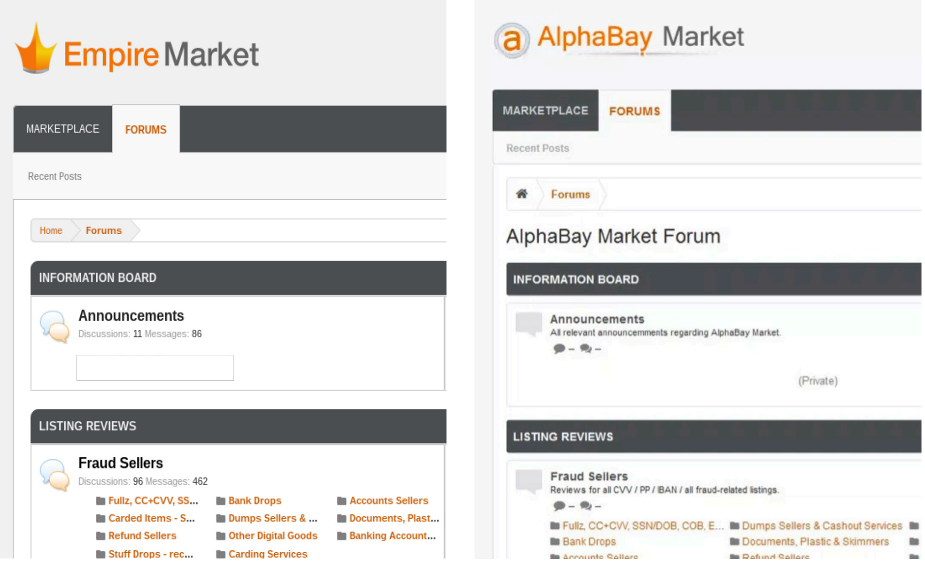
The striking resemblance begs the question of whether or not the new owners were once involved with AlphaBay's administration. The Dread forum has a section dedicated to the Empire Market titled "Why did Empire choose to clone AlphaBay and not Hansa."

> *"AlphaBay was the most popular market at the time," they wrote. "We knew it better than Hansa. We liked the design so we brought it back."*

Although most legitimate vendors are still trading within trusted groups, it's not uncommon to see a prospective client post his or her Wickr or Jabber alias to discuss a transaction privately. However, less-experienced criminals are more likely to take a "leap of faith" opportunity cost

Less-experienced criminals are more likely to take a "leap of faith" opportunity cost in order to start making money.

in order to start making money. These fraudsters are, therefore, more likely to post a public advertisement on a forum such as Dread or on newer markets such as Empire.



Empire Market

MARKETPLACE FORUMS

Recent Posts

Home Forums

INFORMATION BOARD

Announcements

Discussions: 11 Messages: 86

LISTING REVIEWS

Fraud Sellers

Discussions: 96 Messages: 462

Fullz, CC+CVV, SS...	Bank Drops	Accounts Sellers
Carded Items - S...	Dumps Sellers & ...	Documents, Plast...
Refund Sellers	Other Digital Goods	Banking Account...
Stuff Drops - rec...	Carding Services	

AlphaBay Market

MARKETPLACE FORUMS

Recent Posts

Forums

AlphaBay Market Forum

INFORMATION BOARD

Announcements

All relevant announcemments regarding AlphaBay Market.

(Private)

LISTING REVIEWS

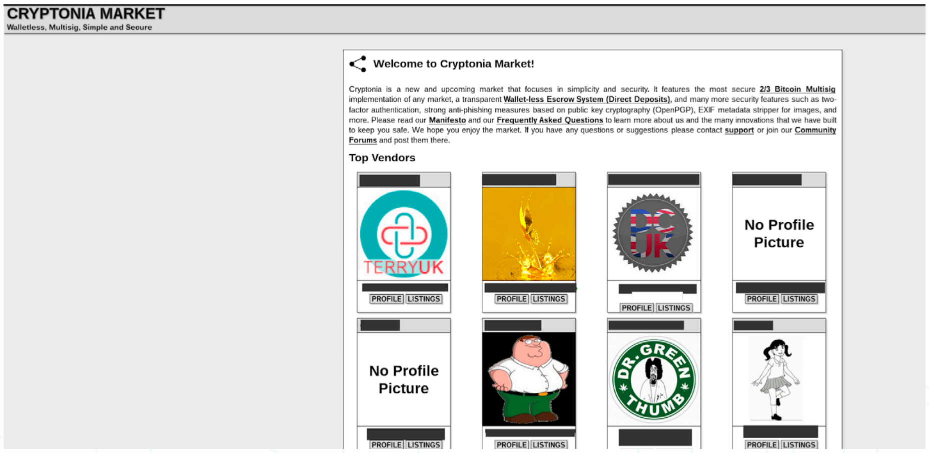
Fraud Sellers

Reviews for all CVV / PP / IBAN / all fraud-related listings.

Fullz, CC+CVV, SSN/DOB, COB, E...	Dumps Sellers & Cashout Services
Bank Drops	Documents, Plastic & Skimmers
Accounts Sellers	Refund Sellers

Figure 3: Screenshot of the Empire Market Forum (left) and of the old AlphaBay Market's forum (right).

One new dark market, called ***Cryptonia Market***, includes several new security features unprecedented on other dark net markets. According to the Cryptonia's main page, it features a 2/3 Bitcoin Multisig implementation for payments, a transparent wallet-less escrow system for direct deposits, two-factor authentication, anti-phishing (a common problem on AlphaBay) features with OpenPGP, and an automatic EXIF metadata stripper. EXIF metadata is embedded into most images which are taken with modern digital cameras and [can be used to derive the GPS coordinates of where the photo was taken]. Stripping this data is essential, especially when photos, like those in the screenshot below, depict a drug dealer's offerings.



CRYPTONIA MARKET

Walletless, Multisig, Simple and Secure

Welcome to Cryptonia Market!

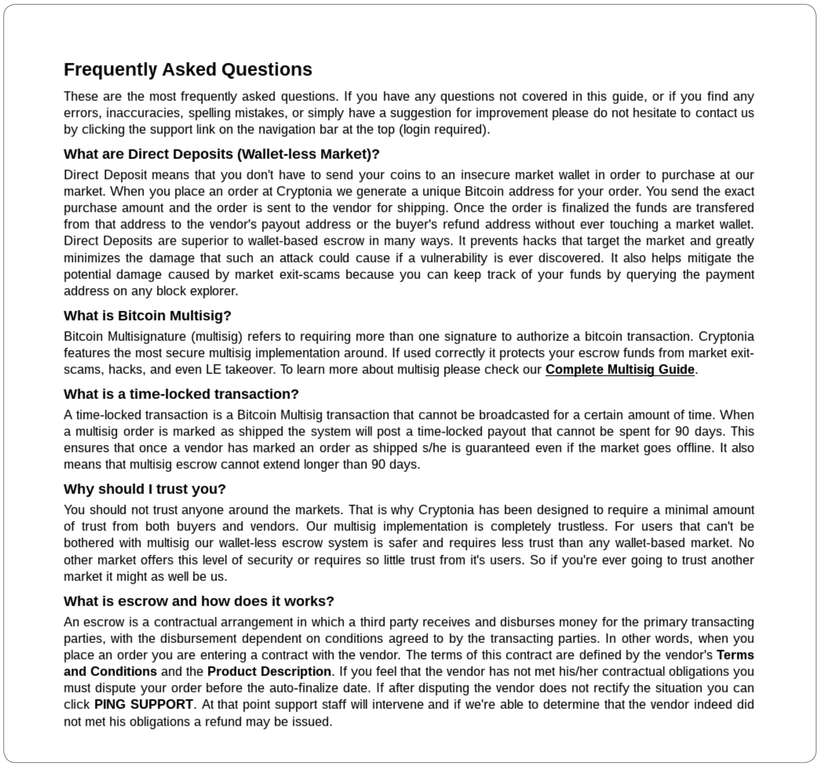
Cryptonia is a new and upcoming market that focuses in simplicity and security. It features the most secure **2/3 Bitcoin Multisig** implementation of any market, a transparent **Wallet-less Escrow System (Direct Deposits)**, and many more security features such as two-factor authentication, strong anti-phishing measures based on public key cryptography (OpenPGP), EXIF metadata stripper for images, and more. Please read our **Manifesto** and our **Frequently Asked Questions** to learn more about us and the many innovations that we have built to keep you safe. We hope you enjoy the market. If you have any questions or suggestions please contact **support** or join our **Community Forums** and post them there.

Top Vendors

Figure 4: Cryptonia Market

"Cryptonia** has been designed to require a minimal amount of trust from both buyers and vendors…**No other market offers this level or security or requires so little trust from its users."

According to Cryptonia, the "trustless" security features it offers are unprecedented. "Cryptonia has been designed to require a minimal amount of trust from both buyers and vendors,'' it reads. "Our multisig implementation is completely trustless. For users that can't be bothered with multisig, our wallet-less escrow system is safer and requires less trust than any wallet-based market. No other market offers this level or security or requires so little trust from its users."



Frequently Asked Questions

These are the most frequently asked questions. If you have any questions not covered in this guide, or if you find any errors, inaccuracies, spelling mistakes, or simply have a suggestion for improvement please do not hesitate to contact us by clicking the support link on the navigation bar at the top (login required).

What are Direct Deposits (Wallet-less Market)?

Direct Deposit means that you don't have to send your coins to an insecure market wallet in order to purchase at our market. When you place an order at Cryptonia we generate a unique Bitcoin address for your order. You send the exact purchase amount and the order is sent to the vendor for shipping. Once the order is finalized the funds are transfered from that address to the vendor's payout address or the buyer's refund address without ever touching a market wallet. Direct Deposits are superior to wallet-based escrow in many ways. It prevents hacks that target the market and greatly minimizes the damage that such an attack could cause if a vulnerability is ever discovered. It also helps mitigate the potential damage caused by market exit-scams because you can keep track of your funds by querying the payment address on any block explorer.

What is Bitcoin Multisig?

Bitcoin Multisignature (multisig) refers to requiring more than one signature to authorize a bitcoin transaction. Cryptonia features the most secure multisig implementation around. If used correctly it protects your escrow funds from market exit-scams, hacks, and even LE takeover. To learn more about multisig please check our **Complete Multisig Guide**.

What is a time-locked transaction?

A time-locked transaction is a Bitcoin Multisig transaction that cannot be broadcasted for a certain amount of time. When a multisig order is marked as shipped the system will post a time-locked payout that cannot be spent for 90 days. This ensures that once a vendor has marked an order as shipped s/he is guaranteed even if the market goes offline. It also means that multisig escrow cannot extend longer than 90 days.

Why should I trust you?

You should not trust anyone around the markets. That is why Cryptonia has been designed to require a minimal amount of trust from both buyers and vendors. Our multisig implementation is completely trustless. For users that can't be bothered with multisig our wallet-less escrow system is safer and requires less trust than any wallet-based market. No other market offers this level of security or requires so little trust from it's users. So if you're ever going to trust another market it might as well be us.

What is escrow and how does it works?

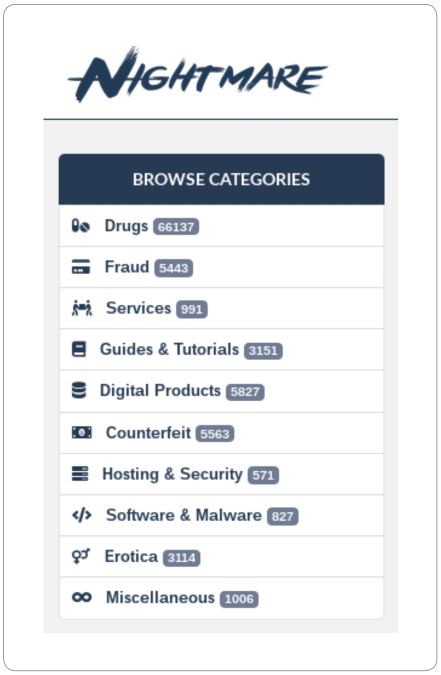
An escrow is a contractual arrangement in which a third party receives and disburses money for the primary transacting parties, with the disbursement dependent on conditions agreed to by the transacting parties. In other words, when you place an order you are entering a contract with the vendor. The terms of this contract are defined by the vendor's **Terms and Conditions** and the **Product Description**. If you feel that the vendor has not met his/her contractual obligations you must dispute your order before the auto-finalize date. If after disputing the vendor does not rectify the situation you can click **PING SUPPORT**. At that point support staff will intervene and if we're able to determine that the vendor indeed did not met his obligations a refund may be issued.

Figure 5: Cryptonia Market's FAQs page

The Market's FAQs page provides a detailed breakdown of its security features. Although features like vendor levels and escrow were already offered by second-generation markets, such as AlphaBay, ***enforced*** PGP encryption for payments and messages is a new and improved addition, especially considering that Alphabay lost over 200,000 private unencrypted messages from in a 2017 breach. While the AlphaBay Market required PGP encryption for all vendor communications, it was only encouraged for customers. This breach followed the market's seizure by just a few months. Wallet-less purchasing provides extra anonymity not offered before. According to the federal indictment against Alexandre Cazes, purchasing goods on the AlphaBay Market worked as follows:

> *"…a vendor could direct AlphaBay to transfer the ill-gotten funds to digital currency addresses outside of the AlphaBay platform and under the vendor's control. Buyers could transfer funds from their AlphaBay accounts in the same manner. For transactions leaving the site, AlphaBay provided "tumbling" and "mixing" services to attempt to obscure the historical trail of digital currency associated with the site and its users. AlphaBay also advertised other external mixing and tumbling services to its users."*

Nightmare Market, *which offers products ranging from drugs and fraudulent credentials to software and services,* ***was recently accused of exit scamming its members.***



NIGHTMARE

BROWSE CATEGORIES

Drugs	66137
Fraud	5443
Services	991
Guides & Tutorials	3151
Digital Products	5827
Counterfeit	5563
Hosting & Security	571
Software & Malware	827
Erotica	3114
Miscellaneous	1006

Figure 6: Screenshot of product categories operated by the "Nightmare" market.

Wallet-less transactions on Cryptonia could theoretically eliminate the need for mixing services, and would make it harder to trace transactions down the blockchain once they leave the market.

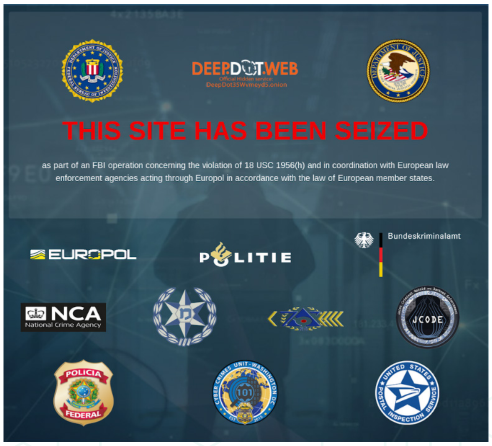
Other new markets have had less-than-noble intentions towards their clientele. *Nightmare Market*, which offers products ranging from drugs and fraudulent credentials to software and services, was recently accused of exit scamming its members. Users on public forums such as the darknet SubReddit and Dread have reported being locked out of their accounts and unable to recover funds.

As the old adage goes, there is truly no honor among thieves.

Improved Information Sharing

Luckily for dark net market vendors and customers, there is still a place to go to see the current status of which markets are online, offline, exit scamming, or otherwise. This place used to be *Deep Dot Web*, a popular website with both TOR and clearnet presences that included news, articles, and current status updates for many darknet markets. Users could access the site to find out which markets were offline or online, and it maintained a regularly-updated list of .onion links to popular markets. The site also included general dark web news and information that was of interest to security researchers and the general public. In May, the FBI seized Deep Dot Web and two Israeli citizens were arrested in connection with "Money Laundering Conspiracy, Relating to Kickbacks for Sales of Fentanyl, Heroin and Other Illegal Goods on the Darknet," according to the Justice Department.

A new service which lists dark net markets and their current statuses has replaced Deep Dot Web, but it is stripped-down. While the site has both clearnet and dark net addresses, it also lists .onion addresses for non-crime-related hidden sites such as the FBI's NCIDE Task Force.



DEEPDOTWEB
Official Hidden service:
DeepDot35Wvmeyd5.onion

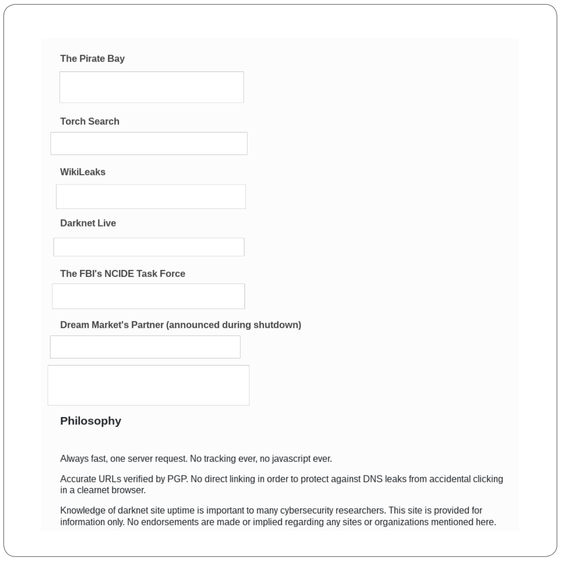
THIS SITE HAS BEEN SEIZED

as part of an FBI operation concerning the violation of 18 USC 1956(h) and in coordination with European law enforcement agencies acting through Europol in accordance with the law of European member states.

EUROPOL
POLITIE
Bundeskriminalamt
NCA National Crime Agency
JCODE
POLICIA FEDERAL
CYBER CRIMES UNIT - WASHINGTON DC
UNITED STATES POSTAL INSPECTION SERVICE

Figure 7: Screenshot of the Deep Dot Web hidden site after it was seized.

The truth about the staying power of markets has more to do with the ***human factor*** *than blockchain vulnerabilities or eavesdropping.*



The Pirate Bay

Torch Search

WikiLeaks

Darknet Live

The FBI's NCIDE Task Force

Dream Market's Partner (announced during shutdown)

Philosophy

Always fast, one server request. No tracking ever, no javascript ever.

Accurate URLs verified by PGP. No direct linking in order to protect against DNS leaks from accidental clicking in a clearnet browser.

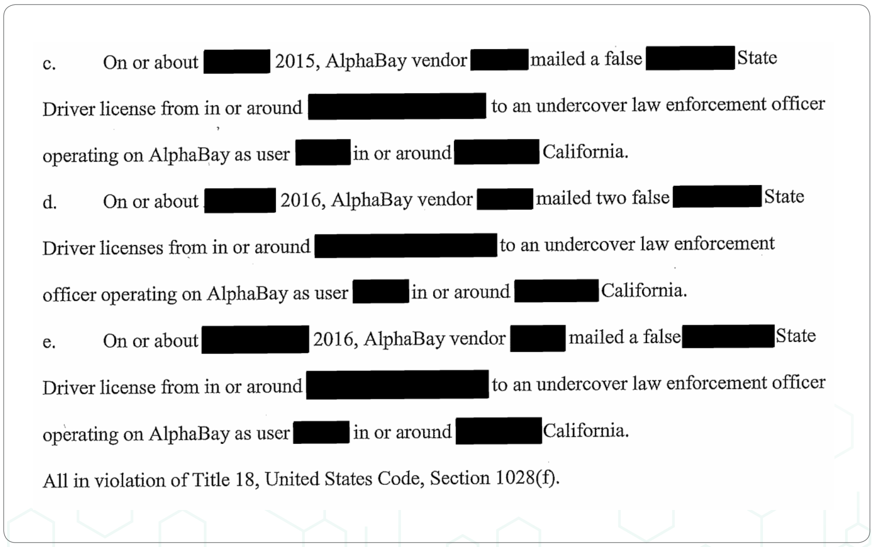
Knowledge of darknet site uptime is important to many cybersecurity researchers. This site is provided for information only. No endorsements are made or implied regarding any sites or organizations mentioned here.

Figure 8: New undisclosed source for dark net market links and uptime status.

The service claims that "knowledge of the darknet site uptime is important to many security researchers. This site is provided for information only." The site features its own security improvements over Deep Dot Web, such as no tracking, javascript, accurate links verified by PGP, and no direct linking (to protect against any DNS leakage that could occur as a result of opening a .onion link in a clearnet browser such as Google Chrome).

The Human Factor

The truth about the staying power of markets has more to do with the human factor than blockchain vulnerabilities or eavesdropping via sophisticated man-in-the-middle attacks on dark net markets' crypto. While the improvements discussed above are certainly interesting, it doesn't guarantee that these markets are safe, especially if we consider history. Alexandre Cazes was identified as the kingpin of the AlphaBay Market because he used an email address he had once posted on a public forum in welcome messages to AlphaBay Market members. The Justice Department was able to ensnare several AlphaBay vendors because several undercover federal agents were able to successfully purchase drugs, falsified documents, and other illegal goods, and have them delivered to agreed-upon drop sites.



c. On or about [redacted] 2015, AlphaBay vendor [redacted] mailed a false [redacted] State Driver license from in or around [redacted] to an undercover law enforcement officer operating on AlphaBay as user [redacted] in or around [redacted] California.

d. On or about [redacted] 2016, AlphaBay vendor [redacted] mailed two false [redacted] State Driver licenses from in or around [redacted] to an undercover law enforcement officer operating on AlphaBay as user [redacted] in or around [redacted] California.

e. On or about [redacted] 2016, AlphaBay vendor [redacted] mailed a false [redacted] State Driver license from in or around [redacted] to an undercover law enforcement officer operating on AlphaBay as user [redacted] in or around [redacted] California.

All in violation of Title 18, United States Code, Section 1028(f).

Figure 10: Excerpt of the Justice Department's indictment against Alexandre Cazes, detailing vendor shipments of falsified documents to undercover law enforcement officers.

Even on the underground, masterminds can sometimes be ***too smart for their own good.***

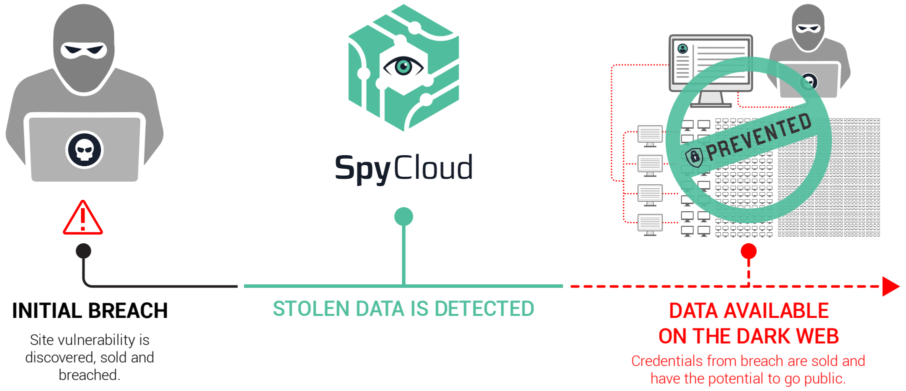
This evidence was presented in the federal indictment against Alexandre Cazes, who ended up taking his own life preceding his schedule extradition to the United States. When Cazes was arrested in Thailand, his laptop was open and he was logged into the Market as "admin." And while the breach of over 200,000 unencrypted private messages certainly threw AlphaBay into a tailspin, it was a series of simple OPSEC failures that brought the market down.

Silk Road Founder Ross Ulbricht, who is now incarcerated for life, was caught via similar methods. Ulbricht had also once posted his private email address online and had even described "creating an economic simulation to give people a first-hand experience of what it would be like to live in a world without the systemic use of force" in his LinkedIn profile.

It will take time to see if third-generation markets will suffer the same fate as their predecessors. But only if these new markets can temper innovation with basic security hygiene will they survive. Even on the underground, masterminds can sometimes be too smart for their own good.

Why SpyCloud Cares

SpyCloud is the leading provider of account takeover (ATO) prevention, offering solutions backed by the world's most comprehensive database of stolen credentials and PII recovered from third party breaches. By enabling customers to identify if users' credentials have been exposed in a third party breach and force password resets when matches are found, we are disrupting cybercriminals' ability to profit from stolen information. With SpyCloud, enterprises can do more than detect compromises—they can remediate exposures to protect employee and consumer accounts. The same database also empowers fraud investigators to unmask criminals and attribute specific crimes.


SpyCloud
PREVENTED
INITIAL BREACH
Site vulnerability is discovered, sold and breached.
STOLEN DATA IS DETECTED
DATA AVAILABLE ON THE DARK WEB
Credentials from breach are sold and have the potential to go public.

Our proprietary collection methods automatically collect more data sooner, going deeper into the dark web to uncover exposures—often within hours or days of the breach, and months or years before they are posted on public forums. Each month, we recover more than 1B assets and make them available quickly for customers to match against. No other security solution offers access to as many plaintext passwords, which makes it possible for customers to identify more exposed account matches and take action—preventing exposures from progressing to account breaches.

SpyCloud maintains the largest repository of stolen credentials in the world:

77 BILLION
BREACH ASSETS

23 BILLION
BREACH RECORDS

18 BILLION
PLAINTEXT PASSWORDS

...and growing by a billion assets a month.

SpyCloud Employee ATO Prevention

Enterprises use SpyCloud to prevent ATOs for their employees, protect corporate assets, and block IP theft and business email compromise. With integration to Active Directory, SpyCloud proactively monitors every employee account against collected exposure data from the underground. Once a match for a domain user's password is found—meaning it has been compromised in a third party breach—SpyCloud sends an instant alert and forces a password reset. It's fully automated and needs little to no human effort to maintain once installed.

SpyCloud Consumer ATO Prevention

SpyCloud protects consumer accounts from fraud and unauthorized purchases by identifying compromises at the point of login. The user can then be moved to a step-up authentication process or forced password reset. The solution also continually gathers data to discover consumers who have been attacked with malware that steals credentials. Any detected "hits" automatically generate an instant alert. In only a matter of hours, SpyCloud integrates into common SIEMs and TIPs via apps or custom API integrations.

SpyCloud for Fraud Investigations

SpyCloud's dataset gives enterprise security teams the detailed evidence they need to not only solve fraud cases but empower law enforcement to catch the criminals. With easy-to-use tools, investigators can quickly uncover hidden identities, locations and techniques of criminals. No other security solution provides the same level of detail or accuracy.

Contact us to set up a demo today.

SpyCloud