



| Brief |

The Underground Economist: Volume 5, Issue 11

B-2025-06-06a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Threat Actor

June 6, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 7:00 AM (EDT) on June 6, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

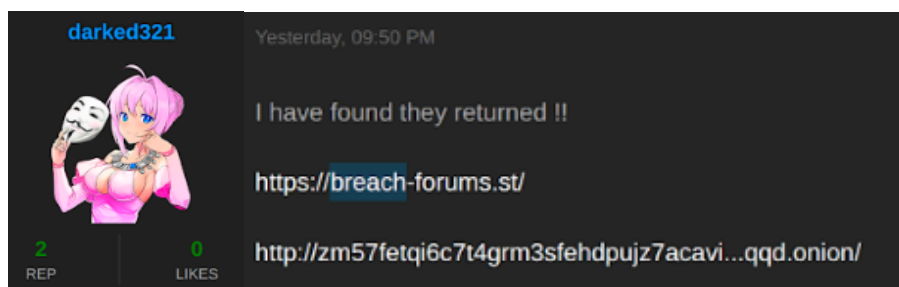
Brief | The Underground Economist: Volume 5, Issue 11

BreachForums and Notorious Actors Announce Re-emergence

On June 3, 2025, an actor using the alias “darked321” posted in the deep web forum DarkForums claiming its counterpart, BreachForums, has been relaunched. According to darked321, BreachForums is once again accessible via two separate domains: one clearnet (breach-forums[.]st) and one onion-based (zm57fetqi6c7t4grm3sfehdpuzj7acavi4y7ubye3pugenyhktzxjqqd[.]onion/).

- On April 15, 2025, BreachForums became inaccessible, with the breachforums[.]st domain displaying an error code; at the time of this writing, ZeroFox has confirmed that this domain remains inaccessible.
- Significant speculation surrounding this event took place within deep and dark web (DDW) forums and Telegram channels at that time, with many speculating law enforcement (LE) involvement.
- Discussion also centered around the possible arrest of IntelBroker—an actor prominent within the forum both for publishing numerous prominent data leaks and having previously carried out a moderator role.
- The hacktivist collective “Dark Storm” claimed responsibility for the BreachForums outage in its Telegram channel, though without any substantiation.

Darked321's DarkForums post quoted a longer message from actor "ShinyHunters", who provides an explanation as to the status of the original BreachForums domain and alleged plans for the new one. According to the post, the newly launched breach-forums[.]st is the "new, official" domain, and efforts to restore legacy infrastructure and member ranks are ongoing—as is the rectification of security flaws identified during an "audit and rebuilding process." ShinyHunters also referred to the disruption of the previous domain, claiming a PHP vulnerability had been exploited. While the actor did not specify the identity of the alleged attacker, they did reference attempts by "various agencies" to access a BreachForum database—almost certainly alluding to LE entities.



darked321's DarkForums post quoting ShinyHunters' message

Source: ZeroFox Intelligence

Prior to this post, ZeroFox had not observed activity from ShinyHunters since April 28, 2025, when they posted a PGP-signed message to the front end of breachforums[.]st claiming that the disruption had been caused by a zero-day vulnerability affecting MyBB software. In this post, ShinyHunters also blamed unnamed LE entities, as well as warned BreachForums frequenters to avoid "clone" forums.

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

Hello everyone,

We would like to provide an update on recent events over the past two weeks. In or around April 15, we received confirmation of information that we had been
suspecting since day 1 - a MyBB 0day. This confirmation came through trusted contacts that we are in touch with, which revealed that our forum
(breachforums.st) is subject to infiltration by various agencies and other global law enforcement bodies.
```

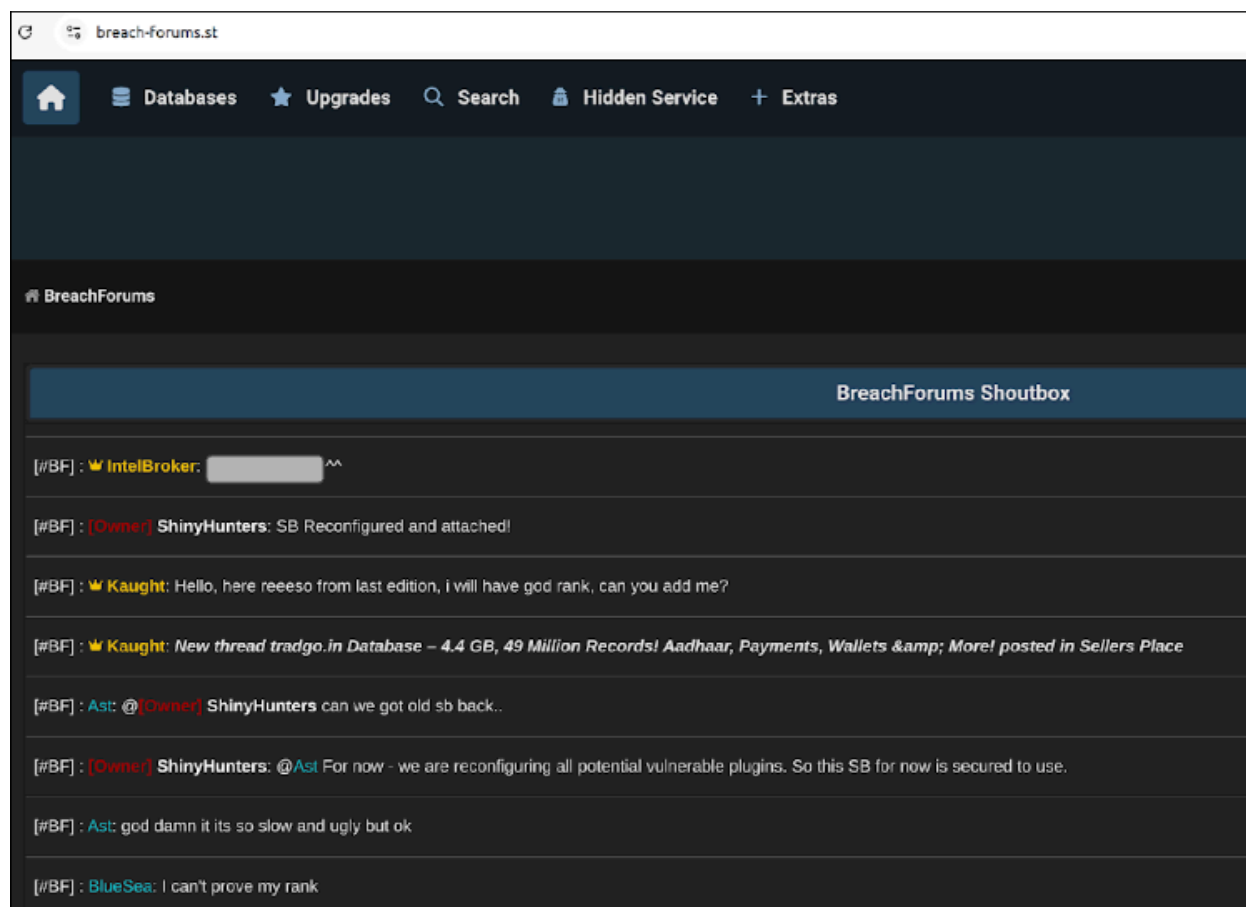
Portion of ShinyHunters' statement posted to BreachForums front end on April 28, 2025

Source: ZeroFox Intelligence

- ShinyHunters is an English-speaking threat collective that has been operational in DDW forums since approximately 2020. The group has since been responsible for

numerous data breaches and has also been widely viewed as the owner of BreachForums since the March 2023 arrest of previous moderator “Pompompurin.”

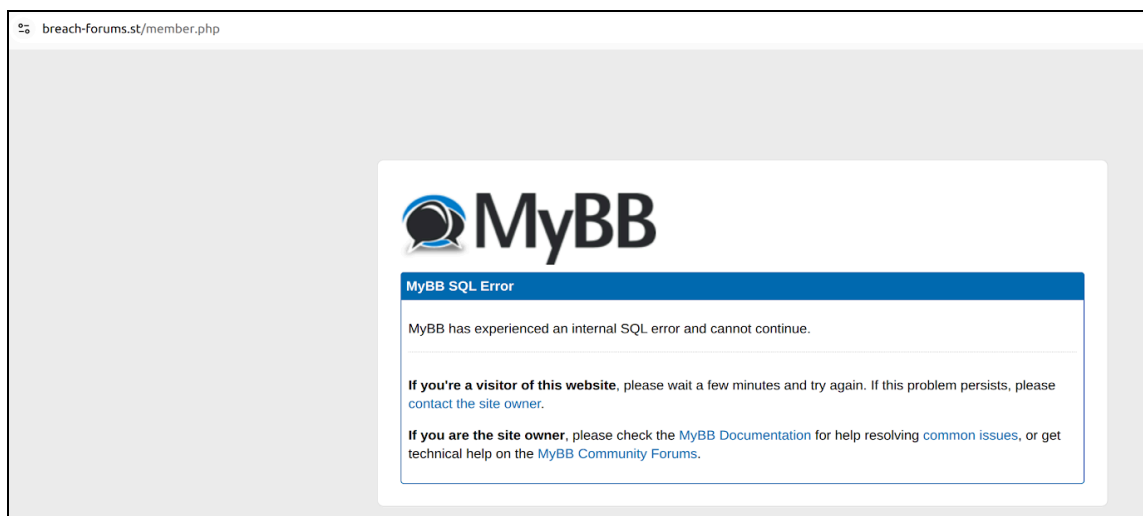
- In addition to ShinyHunters, ZeroFox also observed posts within breach-forums[.]st’s new Shoutbox feature from IntelBroker—the first activity observed from the actor since April 15, 2025.



Front page of BreachForums[.]st, with profanities redacted

Source: ZeroFox Intelligence

ZeroFox’s attempts to register an account on breach-forums[.]st were unsuccessful due to a MyBB SQL error. This likely indicates that the forum is unable to connect to its user SQL database, suggesting configuration efforts are in progress. Despite this, the forum search feature appears to be functional, with new discussions and topics posted by users that have successfully registered. Notably, the new domain has undergone a significant overhaul, with many features redesigned.



Breach-forums[.]st registration error

Source: ZeroFox Intelligence

Since the outage of BreachForums[.]st, numerous other forums have surfaced, with some claiming to offer a like-for-like replacement and others attempting to scam users wishing to register new accounts by masquerading as an “official” replacement. ZeroFox previously reported on the launch of BreachForums[.]fi, announced by actors “Normal” and “Anastasia” (the latter has previously fulfilled a moderator role within the original forum). This domain likely reflected attempts to offer a replacement but was seemingly unable to gain traction and remains inaccessible as of the writing of this report.

Given the presence of ShinyHunters and IntelBroker, there is a likely chance that breach-forums[.]st represents a relaunch effort led by actors in possession of digital infrastructure associated with the original domain. This is further supported by the presence of historic content within the new domain, much of which dates back to as early as 2023. There is a very likely chance that breach-forums[.]st will quickly gain traction and restore functionality, though it is also likely that users will remain active within peer domain DarkForums—where many actors migrated upon BreachForum’s disruption.


| U.S. Property Data Advertised for Sale on Dark Web Forum



On May 27, 2025, an actor using the alias "Sentap" posted on the predominantly Russian-speaking dark web forum xss advertising the sale of 1.02 terabytes of property data, the price of which is negotiable and subject to direct contact with the seller. Sentap claims to have obtained "unprecedented" access to this data from the cloud infrastructure of a U.S.-based title company that specializes in property record search services.


- ZeroFox's observations of Sentap's recent online activity indicate that the actor has been involved in an array of malicious cyber activities that include website cloning, bypassing Web Application Firewalls (WAF), and crypto draining.




According to the advertisement, the stolen data includes:

- Title search documents outlining the ownership and legal history of properties, which contain information about deeds, owners, taxes, mortgages, and liens (legal claims on a property to secure payment of a debt or obligation).
- Other documents associated with a property, such as tax documents, court filings, and survey maps.
- According to Sentap, the quality of the documents equates to an optical character recognition (OCR) error rate of approximately 10 percent, which is considered "correctable."

 **Applications**

-  Real estate market and valuation trend analysis.
-  Investment strategies (targeting properties with legal risks).
-  Competitive research and legal analysis.
-  Advanced exploitation (buyers are responsible for compliance with local laws).

 **Technical Details**





-  **Size:** 1.02 TB, compressed in ZIP/RAR files.
-  **Organization:** Sorted by state, county, and document type.
-  **Access:** Secure, password-protected download link.
-  **Support:** Sample datasets available for vetted, established clients.

Sentap's description of allegedly available data

Source: ZeroFox Intelligence

In the advertisement, Sentap attempted to provide justification for the unspecified value of the information, highlighting the alleged prominence of the compromised organization within its sector, alongside its partnerships with reputable banks. Sentap also claims that the data encompasses "strategic" regions of Illinois, Indiana, Wisconsin, Minnesota, Iowa, Colorado, and Kansas but offers no further context. The alleged documents are dated from "the 1990s to 2025", a timeframe which Sentap claims can facilitate long-term analysis.

Why This Data Is Valuable

-  **High Credibility:** Extracted from a top-tier firm with partnerships including ServiceLink and reputable banks.
-  **Extensive Coverage:** Encompasses strategic regions like Cook County, IL, Pierce County, WI, and Vanderburgh County, IN.
-  **Historical Depth:** Documents from the 1990s to 2025, ideal for long-term analysis.
-  **Sensitivity:** Personal, financial, and legal data with potential for advanced applications.

Sentap's description of why the available data is valuable

Source: ZeroFox Intelligence

If the data is as-advertised, its diverse nature would almost certainly appeal to a wide array of mostly financially motivated threat actors. If title searches are available, there is a likely chance that the following personally identifiable information (PII) could be

obtained from such documents:

- Names
- Addresses
- Dates of Birth
- Social Security numbers
- Phone numbers
- Email addresses
- Mortgage details
- Property descriptions and ownership information

Such information could be used to facilitate targeted social engineering campaigns leveraging regionally pertinent lures to generate phishing communications or to target organizations via business email compromise (BEC). Given the apparent comprehensiveness of the PII, it could also be leveraged to conduct various fraudulent activities such as identity theft, real estate fraud, or title theft, all of which can result in the theft of funds from a victim. However, the majority of threat actors very likely perceive real estate-related fraud as a high-effort, high-payoff activity, lessening its broader appeal.

The combination of addresses and other personal information also poses a physical threat to individuals and organizations that are associated with the implicated properties. Financially motivated buyers could use this information to seek high pay-off burglary opportunities, while socially or politically motivated buyers could use it to sabotage or otherwise disrupt sensitive or critical infrastructure.

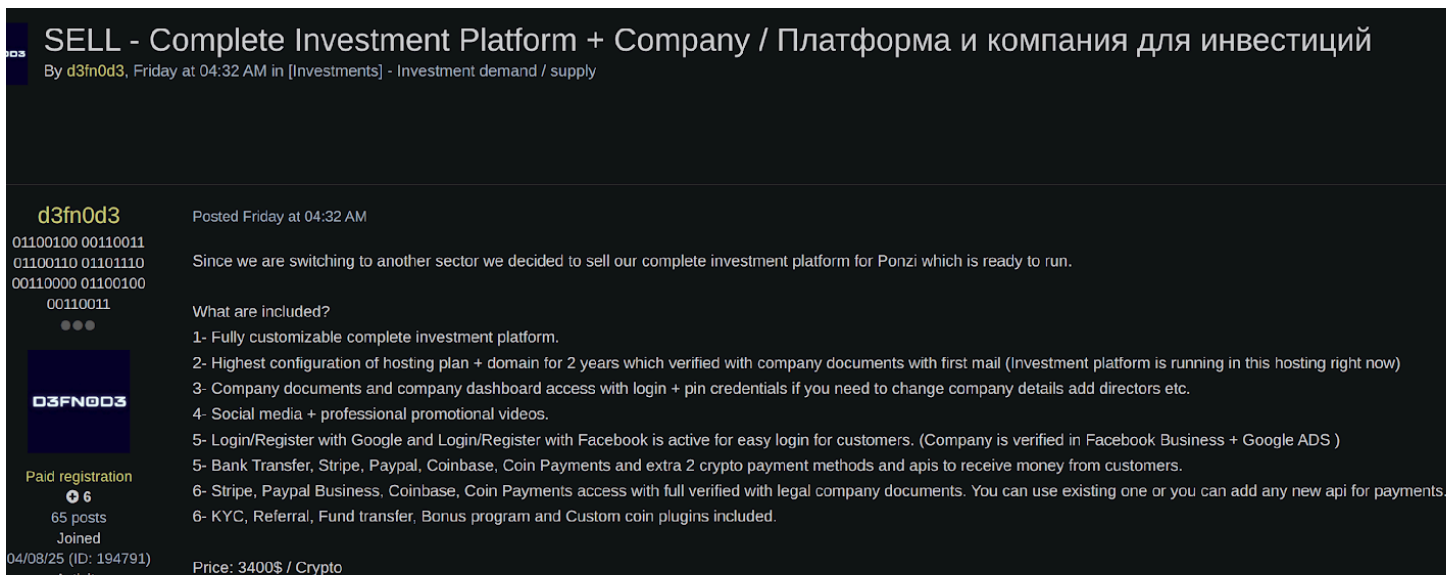
There is also a less likely chance that the information could be acquired by actors seeking to inform a strategic understanding of the region's financial and property trends, enabling activities such as mis and dis-information campaigns, political influencing and interference, market manipulation, or the pursuit of a corporate advantage.

As of the writing of this report, the xss thread has gained minimal traction, and ZeroFox has observed no evidence that the data has been sold. However, there is a very likely chance that any interested parties will contact Sentap via XMPP messaging protocol Jabber using the email address provided in the post or via direct message in the forum rather than responding publicly in the thread.

Comprehensive Ponzi Scheme Platform Advertised for Sale

On May 23, 2025, the actor “d3fn0d3” posted on the predominantly Russian-speaking DDW forum Exploit advertising the sale of a “complete investment platform” designed to facilitate a Ponzi scheme. According to the post, the platform can be purchased for USD 3,400 and is ready to become operational.

- A Ponzi scheme is a type of investment fraud whereby victims are encouraged to invest in a seemingly appealing fabricated or exaggerated business model promising low risk and high returns. However, rather than investing the funds as promised, scammers often use them to pay previous investors under the guise of dividends, while also paying themselves. The scheme can continue until the threat actors are no longer able to attract new investors, upon which the majority of the existing investors lose their money.



SELL - Complete Investment Platform + Company / Платформа и компания для инвестиций
By d3fn0d3, Friday at 04:32 AM in [Investments] - Investment demand / supply

d3fn0d3
01100100 00110011
01100110 01101110
00110000 01100100
00110011
● ● ●

03FN0D3

Paid registration
6
65 posts
Joined
04/08/25 (ID: 194791)
Activity

Posted Friday at 04:32 AM

Since we are switching to another sector we decided to sell our complete investment platform for Ponzi which is ready to run.

What are included?

- 1- Fully customizable complete investment platform.
- 2- Highest configuration of hosting plan + domain for 2 years which verified with company documents with first mail (Investment platform is running in this hosting right now)
- 3- Company documents and company dashboard access with login + pin credentials if you need to change company details add directors etc.
- 4- Social media + professional promotional videos.
- 5- Login/Register with Google and Login/Register with Facebook is active for easy login for customers. (Company is verified in Facebook Business + Google ADS)
- 5- Bank Transfer, Stripe, Paypal, Coinbase, Coin Payments and extra 2 crypto payment methods and apis to receive money from customers.
- 6- Stripe, Paypal Business, Coinbase, Coin Payments access with full verified with legal company documents. You can use existing one or you can add any new api for payments.
- 6- KYC, Referral, Fund transfer, Bonus program and Custom coin plugins included.

Price: 3400\$ / Crypto

d3fn0d3's Exploit post on May 23, 2025

Source: ZeroFox Intelligence

Since joining Exploit on April 8, 2025, d3fn0d3 has established a positive reputation in the forum. ZeroFox observed at least 65 previous posts associated with the actor, the majority of which are related to various types of scamming and social engineering activity. D3fn0d3 is heavily active within two predominantly Turkish-speaking cybercrime

forums, [hactiviz\[.\]org](https://hactiviz[.]org) and [spyhackerz\[.\]org](https://spyhackerz[.]org). This, along with Turkey-related posts, indicates d3fn0d3 is likely located in Turkey.

According to the advertisement, the investment platform includes the following features and services:

- A fully customizable, complete investment platform.
- “Highest configuration” of domain hosting plan available for at least two years. D3fn0d3 provided no further detail, but this very likely refers to dedicated hosting, whereby the buyer can exercise a high degree of control over associated servers.
- Access to a dashboard feature, which is likely intended to mimic a legitimate environment wherein investors can manage their portfolios and view investment opportunities. This dashboard is almost certainly intended to increase perceived legitimacy.
- Social media and “professional” promotional videos. No examples of these were provided in d3fn0d3’s post, though they are likely intended for advertisement purposes.
- Logins for both Google Ads and Facebook Business, likely indicating that d3fn0d3 has already completed the process of providing verification information such as business name and website URL, government-issued identification, and various aspects of company policy.
- “Easy login” procedures for victims, likely referring to Google and Facebook logins that are intended to increase perceived legitimacy and security.
- Verified logins for numerous payment platforms, including Coinbase, Coin Payments, Stripe, and PayPal Business, as well as two other unspecified cryptocurrency services. These are likely intended as a means by which to receive payment from victims, as well as provide payment to existing investors. The platforms also allegedly facilitate customized application programming interfaces (APIs).
- Other additions such as unspecified Know Your Customer (KYC) security protocols and “referrals”—likely alluding to financial incentives available for victims referring new investors.

Although scam-related services are very common in DDW marketplaces and forums, ZeroFox has rarely observed the sale of comprehensive platforms such as the one

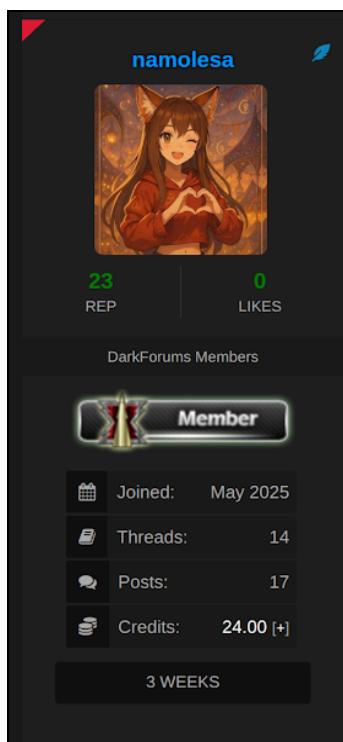
advertised by d3fn0d3. The advertised price of USD 3,400 is unusually low—particularly if the service sold is as described by the actor, inclusive of all the alleged features (many of which likely required significant effort to establish). However, d3fn0d3 claimed in the post that the reason for selling the product is that they are “changing sectors”, reflecting a likely chance that they seek a quick sale.

As of the writing of this report, d3fn0d3’s post has received several positive comments from other actors within Exploit, though the majority are discussing general advice for conducting scamming activity rather than an imminent purchase. However, the platform is very likely to appeal to some financially motivated actors—particularly those familiar with conducting Ponzi schemes who are willing to invest time in managing, growing, and advertising the platform. Due to the limited detail provided by d3fn0d3, ZeroFox cannot ascertain the threat posed by the platform, though it is almost certainly heavily dependent upon its post-purchase management.

| Threat Actor Advertises 2.3 Million Medi-Cal Records on the Dark Web

On May 9, 2025, an actor using the alias “namolesa” advertised a database containing 2.3 million records associated with MediCal, California’s Medicaid program, on the predominantly English-speaking deep web forum DarkForums. According to the advertisement, the information includes PII associated with the “holders” of the healthcare program. Namolesa specified that the data is “exclusive”, which is likely an attempt to portray it as new data rather than information recycled from historic data dumps.

- Namolesa joined DarkForums in May 2025 and has since accumulated 44 reputation points on the forum—a relatively good reputation considering the short time period.
- The actor is likely a data broker, offering data for sale from various regions, including Russia, the United States, Hong Kong, Vietnam, and Israel.

**namolesa's account on DarkForums**

Source: ZeroFox Intelligence

The alleged data set, which spans numerous county jurisdictions within California, contains information such as full names, addresses, email addresses, phone numbers, Medicaid IDs, dates of birth, and Social Security numbers (SSNs). Namolesa claims that the data is “clear and structured”, indicating that the set has likely undergone some extent of parsing, categorization, or enrichment to increase its appeal to potential buyers.

- The dataset does not appear to include medical records, which—due to their personal and sensitive nature—are often coveted by financially motivated threat actors seeking to conduct fraud, extortion, or social engineering activity.

The full data set can be obtained for USD 5,000, though options for partial purchase were also outlined. Namolesa did not specify whether this information is to be sold only to a single party or if it would remain available for subsequent buyers.

Selling a clean and structured dataset containing 2.3 million Medicaid records, all from the state of California, USA, covering various counties and cities within the state.

"A government health insurance program in the United States, established in 1965, that aims to provide free or low-cost health care."

Fields Included:
First Name, Last Name, Address (Street), City, State (CA), ZIP Code, Email Address, Home Phone, Medicaid ID, Date of Birth, Social Security Number (SSN)

Format:
- CSV / XLSX

Contact:
Telegram: <https://t.me/namolesa>
Session: 059811a214935979dccc02838b14a2425a6cb9779a4deb5f30f19945ac982d52

Pricing:

Quantity	Price	Price per Record
100K	\$500	\$0.005
250K	\$1,000	\$0.004
500K	\$1,800	\$0.0036
1M	\$3,000	\$0.003
Full 2.3M	\$5,000	\$0.0022

namolesa's DarkForums advertisement*Source: ZeroFox Intelligence*

Namolesa's post has not gained significant traction as of the writing of this report, though any full or partial sales would likely take place either via the actor's Telegram or Session channels as requested. Though namolesa did not specify the origin of the data, there is a likely chance that it is at least partially recycled from historic data breaches implicating U.S. healthcare organizations, which are commonly targeted by financially motivated threat actors.

Despite the absence of medical records, the presence of Medicaid IDs alongside SSNs and other PII found within the database can be used to facilitate an array of different malicious cyber activities. Fraudsters could attempt to leverage this information to submit reimbursements for fabricated medical services or products, obtain controlled drugs via illicitly obtained prescriptions, or conduct identity theft. However, significant hurdles would likely be encountered by any attacker, as many medical institutions vulnerable to being targeted by such activity would almost certainly utilize established security protocols, such as identity verification via government-issued documentation or multi-factor authentication (MFA), before services can be acquired.

| Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Implement secure password policies, phishing-resistant MFA, and unique credentials.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in DDW forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).

| Appendix A: Traffic Light Protocol for Information Dissemination

WHEN SHOULD IT BE USED?

HOW MAY IT BE SHARED?

Red

Sources may use

TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

Recipients may NOT share

TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

Amber

Sources may use

TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

Recipients may ONLY share

TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Note that

TLP:AMBER+STRICT restricts sharing to the organization only.

Green

WHEN SHOULD IT BE USED?

HOW MAY IT BE SHARED?

Sources may use

TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

Recipients may share

TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.

Clear

Sources may use

TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

Recipients may share

TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%