



# **| Brief |**

## **The Underground Economist: Volume 5, Issue 2**

B-2025-01-31b

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Threat Actor

**January 31, 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 9:00 AM (EST) on January 31, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

# **Brief | The Underground Economist: Volume 5, Issue 2**

## **| Classified U.S. Department of Defense Documents Advertised on the Deep Web**

On January 25, 2025, Russian and English-speaking actor “nxe” advertised classified U.S. Department of Defense (DoD) documents for sale on the deep web forum xss. The actor claimed that the documents are highly classified and allegedly include information regarding the United States’ Nuclear Command and Control (NC2) system. The actor demanded 400,000 rubles for the confidential documents (equivalent to approximately USD 4,000) and stated they would be willing to provide a sample of the classified documents once interested buyers provide proof of funds.

- Nxe joined xss in September 2024, and this is their first post.
- While use of escrow is a mandatory requirement for sellers operating on xss (as well as on other deep web forums such as BreachForums), nxe’s willingness to provide samples is a positive indicator of the actor’s credibility.
- The actor stated that they prefer to specify all deal details in English.

Selling a classified US Department of Defense document - information about the NC2 system

nxe · Saturday at 11:12 PM · documents | government | USA

ESCROW AVAILABLE IN THIS THREAD!

[New deal](#)

 **nxe**  
floppy disk  
User  
Joined: Sep 28, 2024  
Messages: 2  
Reaction score: 0

Saturday at 11:12 PM

Price: 400,000 P  
Contacts: Session: 056cc2a3de8e4a1a3646321c3c63031cc95ec76d481720eff1177361874df37529

I am selling a highly classified US Department of Defense document containing critical information about the NC2 system.

This document is highly confidential. XSS/BF escrow is required.

The preferred language for transactions is English. Samples of the document will only be provided upon receipt of proof of funds, such as a screenshot of your cryptocurrency wallet.

[Report](#)

### Translation of the post by nxe advertising the sale of classified DoD documents

Source: xss

It is very likely that nxe acquired the NC2 system documents from an unknown intelligence information broker on BreachForums and is now attempting to sell the data on the xss forum. ZeroFox identified a December 2024 post by nxe on BreachForums wherein the actor was looking to buy classified intelligence documents—namely, classified government or military intelligence documents of any kind. The actor claimed that he was not focused on any particular country in the post.

CLASSIFIED INTELLIGENCE DOCUMENTS  
by nxe - Wednesday December 18, 2024 at 08:26 PM

 **nxe**  
Baphometさんの妻  
GOD  
Posts: 219  
Threads: 34  
Joined: Oct 2023  
Reputation: 612

12-18-2024, 08:26 PM (This post was last modified: 01-27-2025, 09:14 AM by nxe.)

Hello,

I am looking to purchase classified governmental/military intelligence documents of any kind.

I am not focused on any particular country and am open to most offers.

**ESCROW IS REQUIRED**

Price of the documents may vary depending on the country of origin, classification level, date, and other factors.

I only deal on Session: **056cc2a3de8e4a1a3646321c3c63031cc95ec76d481720eff1177361874df37529**

For more details, contact me.

nxe  
session: 056cc2a3de8e4a1a3646321c3c63031cc95ec76d481720eff1177361874df37529  
telegram: @nxe2226

PM Find

### December 2024 post by nxe seeking to buy classified intelligence documents

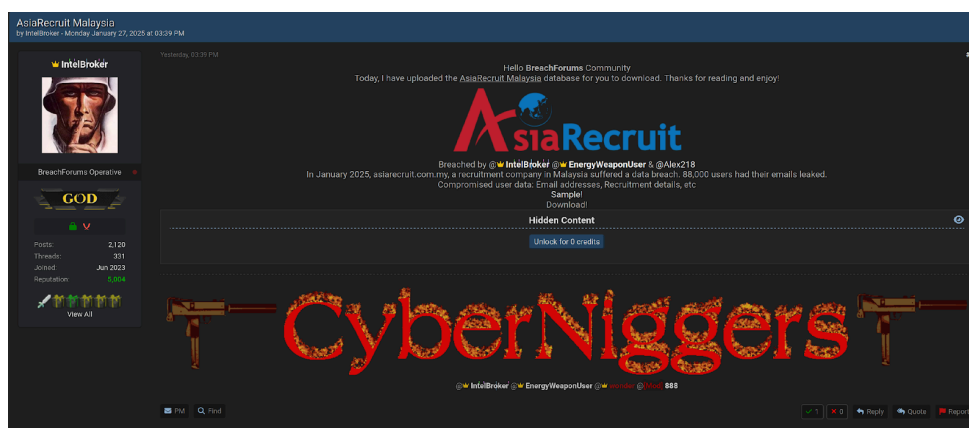
Source: BreachForums

If nxe's claims are credible, the sale of such data is likely to attract the attention of nation-state actors and governmental players, as well as other politically motivated cybercriminals. Such data is very likely to contain sensitive, proprietary information that would be of considerable value to adversarial actors and would likely represent a significant risk to national security operations.

## **| IntelBroker Renounces Ownership of BreachForums**

On January 23, 2025, "IntelBroker" announced their resignation as the owner of BreachForums, citing a lack of adequate time to manage the platform. A few hours after the announcement, the actor's status changed to "BreachForums Operative." IntelBroker further clarified that they would remain a regular member and continue posting occasionally but would no longer be part of the forum's ownership or administration.

- IntelBroker has a history of advertising data breaches, illicit network accesses, and network vulnerabilities—often targeting high-profile organizations and institutions—on BreachForums. The actor has also either removed their account or changed their "moderator" status numerous times since the forum's disruption in May 2024.
- On January 27, 2025, IntelBroker, along with their associates "EnergyWeaponUser" and "Alex218", claimed to have breached recruiting company AsiaRecruit Malaysia (asiarecruit[.]com[.]my) and posted a database allegedly belonging to the company.



**IntelBroker's BreachForums post advertising AsiaRecruit data breach**

*Source: BreachForums*

It is unclear whether IntelBroker's stated reason for renouncing a moderator or administrator role on BreachForums is comprehensive. There is a likely chance that IntelBroker intends to place more emphasis on monetizing their expertise by conducting increased, direct network breaches. There is also a roughly even chance that the actor seeks to lessen their exposure to law enforcement activity. While it will almost certainly remain a popular illicit hacking forum in the short to medium term, there is a roughly even chance that the change in ownership by IntelBroker—who was often unofficially marketed as the "face" of BreachForums—will result in less actors frequenting the forum.

## **| Actor Advertises Network Access to Multinational Pharmaceutical Company**

On January 18, 2025, actor "SmartDust101" posted in the dark web forum Onniforums, where they are newly registered. The actor claims to be an employee of an unspecified multinational pharmaceutical company with a 2024 annual revenue of USD 50 billion, and advertised the following services relating to leaking the organization's information:

- **Comprehensive database access.** SmartDust101 claims that they are able to provide comprehensive access to the organization's databases, which hold data pertaining to client information that includes both public and private pharmacies, hospitals, and clinics. The actor also claims to have access to personally identifiable information (PII), likely of buyers and patients, including payment details such as international bank account numbers (IBANs) and value-added tax (VAT) numbers.
- **Technical passive reconnaissance.** SmartDust101 offers to facilitate "technical passive reconnaissance" of the organization's systems and networks. The reconnaissance allegedly includes information about remote desktop protocols (RDPs) and security infrastructure (including endpoint detection and antivirus solutions), as well as a list of local and web-based applications in use.
- **Miscellaneous.** The actor claims that prospective buyers are able to propose specific requests for information, data, or actions that are not covered by the previous two offerings.

# Insider Pharma Company Post Reply

 **SmartDust101**  
Newbie ... 1

01-18-2025, 11:07 AM #1

I am an employee at a multinational pharmaceutical company that generated over \$50 billion in revenue last year. I have three offers available for those who may be interested.

1. I possess comprehensive access to our databases containing client information, which includes pharmacies, hospitals, and clinics, both public and private. This data encompasses:
  - Complete addresses along with phone numbers, email addresses, and contact persons.
  - Payment details such as IBAN, KBIS, and VAT numbers.
  - Historical order data.
  - Mailboxes from various departments.
2. I can facilitate technical passive reconnaissance of our computer systems and network. Please note that I will not disclose my credentials or any information that could be traced back to me, unless you are a government APT offering citizenship in your country—this is a serious stipulation, with the exception of North Korea. The reconnaissance includes:
  - RDP information.
  - Details regarding security solutions such as antivirus, endpoint detection and response, and firewall.
  - A list of applications in use, both local and web-based.
  - The default browser is set to Internet Explorer, and I receive daily emails with information from our online applications, so I can click on links and internet explorer pops up.
  - An assessment of whether applications can be executed with administrative privileges, including checks for UAC and other potential misclicks by an average employee.
  - Additional reconnaissance tasks that you may suggest, provided they are not overly obvious, such as executing your executable or DLL files.
  - Information regarding the versions of PDF readers and Outlook.
3. Miscellaneous information, data, or actions that you may propose.

I can only proceed with these offers if it is extremely difficult for the blue team or prosecutorial authorities to trace them back to me.

For any inquiries, information, proposed data exfiltration methods by me or you, or payment negotiations, please contact me privately. We will utilize an escrow service for transactions.

...

### SmartDust101's Onniforums advertisement

Source: ZeroFox Intelligence

SmartDust101 specified that any activity would only be carried out if there is a very low risk of detection and identification. However, an exception is granted for “government APTs”, which SmartDust101 suggests could facilitate citizenship in their associated country in return for the services. No prices were stated in the advertisement, which is very likely indicative of a highly diverse set of offerings that require negotiation.

There is a likely chance that the advertisement is legitimate and reflective of a genuine disgruntled employee willing to sell their organization’s data. The explicit intent to use escrow for any transactions and an apparent effort to remain anonymous are reflective of increased credibility.

- Threat actors of all motivations and capabilities would almost certainly be interested in targeting a multinational pharmaceutical organization, given the sheer diversity of customer, proprietary, and supply-chain data likely in its

possession. Such an organization is also likely to have extensive relationships with governments and critical national infrastructure such as hospitals—both of which are deemed lucrative targets across the cyber threat landscape.

If the advertised services are legitimate, then there is a very likely chance that SmartDust101 is financially motivated, with a less likely chance that the actor solely seeks to inflict punitive measures on their organization as political, ideological, or philosophical retribution. An ulterior motive of obtaining citizenship to a foreign country is also possible, though the extent to which this is a priority is unclear. This is more likely reflective of a willingness by SmartDust101 to compromise themselves for a perceived high-payoff result.

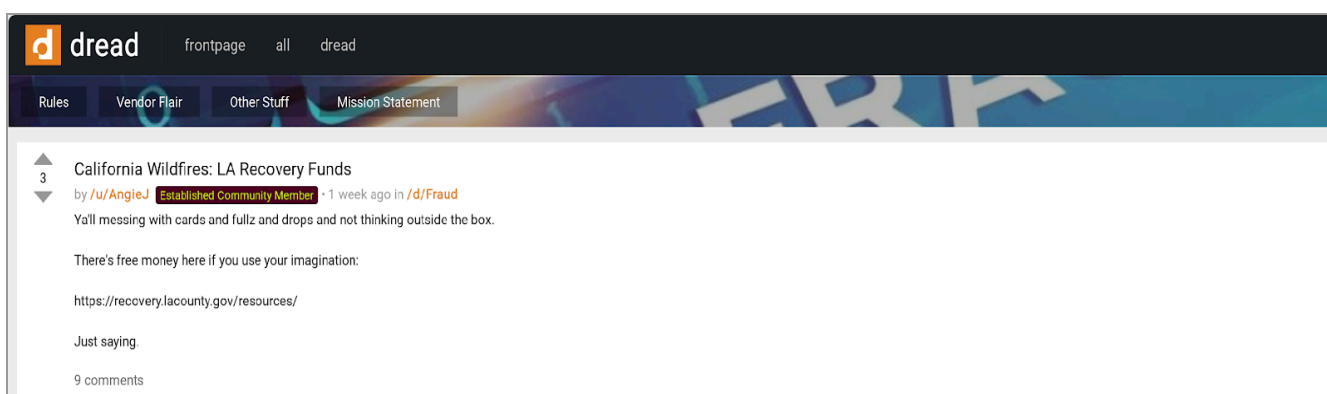
There is also a less likely chance that the advertisement represents either a scam attempt, a law enforcement operation, or a cybersecurity entity seeking to gain insight to threat actor intents and tactics, techniques, and procedures (TTPs).

Following the post, Onniforums became inaccessible for several days. As of the writing of this report, there have been no responses to or discussion surrounding SmartDust101's advertisement, although there is a likely chance that any correspondence would take place privately. If the services are being purchased and leveraged, a compromise of the target organization, a partner or supply-chain organization, or an associated government or customer base is very likely to occur.

## **| Threat Actors Seeking to Exploit California Wildfire Recovery Funds**

On January 15, 2024, an untested threat actor known as "AngieJ" initiated a topical discussion regarding the exploitation of California wildfire recovery funds on the dark web forum Dread. The actor suggested that these funds could be leveraged to fraudulently illicit payouts from government authorities. AngieJ drew attention to the website [hXXps://recovery.lacounty\[.\]gov/resources/](https://recovery.lacounty.gov/resources/), highlighting it as a potential focus for exploitation. It is very likely that some financially motivated actors perceive these funds as having inadequate verification processes, making them fertile ground for financial gain and posing very little risk to the scammers applying.

- Following the outbreak of the January 2025 wildfires across California, authorities have made Federal Emergency Management Agency (FEMA) assistance funds available for residents impacted by wildfires in Los Angeles (LA) County.
- In the thread, AngieJ criticized other members of the Dread forum for relying on outdated fraud methods, such as using financial mules and stolen payment cards.
- The post almost certainly indicates ongoing threat actor interest in exploiting these funds via financially motivated scams. Based on previous behavior and attitudes towards disaster relief funds, it is very likely that a broader array of threat actors are interested in exploiting these funds than those identified to date.



**AngieJ's original post on Dread, where actors mention LA County's wildfire recovery program as a potential target for fraud**

*Source: Dread*

AngieJ alluded to scams conducted during the COVID-19 pandemic as a blueprint for exploiting wildfire recovery funds. The actor elaborated on their initial post, stating that trillions of dollars in loans had been obtained from the U.S. government during the COVID-19 pandemic, specifically through the Paycheck Protection Program and Economic Injury Disaster Loans. AngieJ implied that some of these loans were obtained fraudulently and that similar scams could possibly be leveraged again, with potentially low risk to the threat actor.

- According to AngieJ, individuals who forged limited liability company (LLC) paperwork to secure USD 50,000 loans were often not pursued by authorities if they disappeared after receiving the funds, barring a few exceptions.

An untested actor known as "satanisyourmaster" replied to AngieJ with a lengthy post that garnered significant attention, the most relevant part of which addresses fraud related to LA wildfire recovery funds. The actor remarked, "I read the first returns through the gate have a much higher chance of being flagged for verification. So maybe wait a little. How long? Idk. But there ya go." This highlights a strategic approach for improving the success rate of applications for relief funds related to the LA wildfires, emphasizing threat actor patience to avoid early scrutiny during the verification process.

 **/u/AngieJ**  2 points 5 days ago\*

YEP!!!

You got any idea how much PPP and EIDL loan money was pumped out of the government for COVID?

TWO. TRILLION. BUCKS.

You stated you had a business with employees and loss of income and paperwork was rubber stamped with no backup and no proof and you had a wire transfer for \$100,000 in two weeks.

Those loans were forgiven and nobody even looked at amounts under a certain threshold. Sure the FBI went after people who heisted missions, and rightfully so. But if you faked LLC paperwork for a dozen \$50,000 loans, nobody is coming for you.

There aren't any "guides" to do this on here.

The best fraud is the fraud you don't read about on here.

Use your skills and imagination.

Make the money.

Then after the government gets wise to everything and faucet is tightened up, simply write up a guide and sell that for \$500 on here to the newbies who are looking for a payday. All day long.

LOLOLOL.

 **/u/satanisyourmaster** 2 points 5 days ago

I know. I missed the boat on COVID money and it burns my ass. Not this time!

And yeah, I get the newbie asking for guides from not knowing better, or even someone more experienced wanting a primer in something they have yet to dabble (something I definitely look for as needed), but I don't get people asking to basically have the work done for them.

That's literally not how \*anything\* works.

But hey, maybe there's an idea in here. FaaS: Fraud as a Service Service.

You don't need the tools or knowhow to do the job, or even what the job itself is! No more sauces or methods to buy, only to read and find out it was written in 2018. No more clicking one link at a time on the list of CARDABLE SITES, like you'll eventually click a link that takes you to a retailer that's banner reads "when paying, enter any name, address and any 16 digits for the card number! No exp! No CVV! Here at the Astroglide Discount Bakery and Nike Outlet, we cater to dipshits that spent \$12 (15-16 after you get fucked by exchange rates) on a PDF of "3,000 URLs that were definitely online retailers at some point in time!!"

Instead of that nonsense, you pay me to do fraud. And after I do fraud, I keep the money for myself and block your messages. You may not get a return on your initial investment, but you WILL certainly learn a lot. Namely, that people are more likely to help you for FREE if you seem the type to know how to help yourself and ask intelligent questions. Or even dumb questions that aren't easily searchable.

Like right now, I want a 2025 tax method. And fuck no, I am not paying a dime for one. I'll burn a few attempts at trial and error if it means I'll land on a home cooked method that won't be on the IRS radar.

I do have one free tip. This is for real and I read it regarding this tax season. Don't file the minute returns open up. File your own of course, but because people using stolen info want to beat the actual person before they file, they do so the first day/week returns are accepted. I read the first returns through the gate have a much higher chance of being flagged for verification. So maybe wait a little. How long? idk. But there ya go

### Relevant comments in the chatter for LA wildfire recovery funds fraud

Source: Dread

Although ZeroFox has identified no evidence that threat actors are actively—and successfully—leveraging wildfire recovery funds in financial scams, the thread indicates threat actor interest in exploiting such relief funds for this purpose. If such scams are successful, not only could they result in financial and reputational damage for state or local government authorities, they would also very likely reduce the availability of relief funds for those legitimately affected by the wildfires—as well as perpetuate the idea that these kind of schemes are a viable attack vector for bad actors.

## **| 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 multi-factor authentication (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 deep and dark web forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated TTPs.

## | Appendix A: Traffic Light Protocol for Information Dissemination

### WHEN SHOULD IT BE USED?

#### 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.

#### 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.

### HOW MAY IT BE SHARED?

##### Recipients may NOT share

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

##### 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?

##### 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.

#### 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.

### HOW MAY IT BE SHARED?

##### Recipients may share

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

##### 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%         |