



| Brief |

The Underground Economist: Volume 5, Issue 6

B-2025-03-28a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Threat Actor

March 28, 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 (EDT) on March 28, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 5, Issue 6

| Access to Law Enforcement CarFax Accounts Advertised on DDW

On March 24, 2025, threat actor "DataSec" posted in the hacking forum BreachForums, advertising a new access-as-a-service. According to DataSec, buyers are able to request reports from automobile organization CarFax, obtainable through access to an alleged U.S. and Canadian law enforcement (LE) account. The service is priced at USD 175 "per account", but it is not clear exactly what buyers of the service receive for this price.

The threat actor claims the service enables unlimited searches on a database that contains up to 34 billion vehicle history records, which include crash reports, ownership changes with address updates, driving habits, and vulnerabilities (among other details) that can be used for "stalking victims or rivals."

- CarFax, a part of S&P Global, provides detailed vehicle history information that helps people make informed decisions when buying, selling, servicing, or shopping for cars. Its comprehensive reports include key information on accidents, ownership, service history, and more.
- The actor urges potential buyers to make contact via the encrypted messaging channel Session. At the time of writing, some interest had been generated in the thread, though it is unclear if and how payments are taking place.

(US & CA) CarFax Law Enforcement (Police) Plate search Account Access
by DataSec - Monday March 24, 2025 at 09:14 AM

Yesterday, 09:14 AM (This post was last modified: Yesterday, 09:17 AM by DataSec.)



DataSec

BreachForums Patriot

GOD

\$

Posts: 208
Threads: 9
Joined: Feb 2025
Reputation: 191



DataSec Presents

CarFax Law Enforcement (Police) Plate Search Account Access

Track Targets with Precision
[*]Tap into 34 billion vehicle history records to stalk victims or rivals. Service logs, crash reports, and ownership changes give you addresses, habits, and vulnerabilities

Exploit Government Access Loopholes
Government access and police access in carfax make it so that a \$44+ report is free, unlimited free searches.

Weaponize Real-Time Data
Driver Exchange and VIN scans hand you live updates—stolen cars, fraud flags, or exact locations, run full searches on anyone in real time.

Hunt with Fragments
Partial License Plate Search turns scraps of info into full leads. Three digits, or more, become a partial search seller on telegram or forums.

Create Reports
Create crash reports or VIN alerts for payment.

Monitor Your Fleet
Set VIN alerts on your stolen or burner cars—know instantly if cops flag them. Stay ahead and track any plate or VIN, (CSINT)

\$175 Per Account
Contact on session

[*]Session ID: 050b6fe5345a72f3015bd989abbf86f1e93552dc24b07226506b0938c9dads5652

DataSec advertisement in BreachForums

Source: ZeroFox Intelligence

DataSec is a newly registered, positively trending threat actor that first appeared in BreachForums in February 2025. The actor, who has a “God Tier” status in the forum, has previously been observed advertising forged subpoena templates (a pre-designed, fillable template) and EDRs (Emergency Data Requests) as a service.

- According to their bio, DataSec specializes in selling access to sensitive government emails, leaking confidential information, and facilitating illicit data requests from various platforms.

There is a very likely chance that the services offered by DataSec are legitimate and as advertised. Given that DataSec also advertises the sale of EDRs, access to a U.S. and Canadian LE CarFax account was most likely achieved via the compromised credentials of an LE member. There is also a less likely chance that DataSec represents an LE insider with access to platforms associated with EDRs.

Some of the information allegedly obtainable is very likely to appeal to a variety of threat actors. Financially motivated actors may seek to re-sell this information in deep and dark

web (DDW) forums or on instant-messaging platforms, as well as acquire personally identifiable information (PII) for purposes of conducting targeted social engineering activity. The ability to link vehicle registration numbers (VRNs) to names and locations may also appeal to criminals interested in engaging in auto theft.

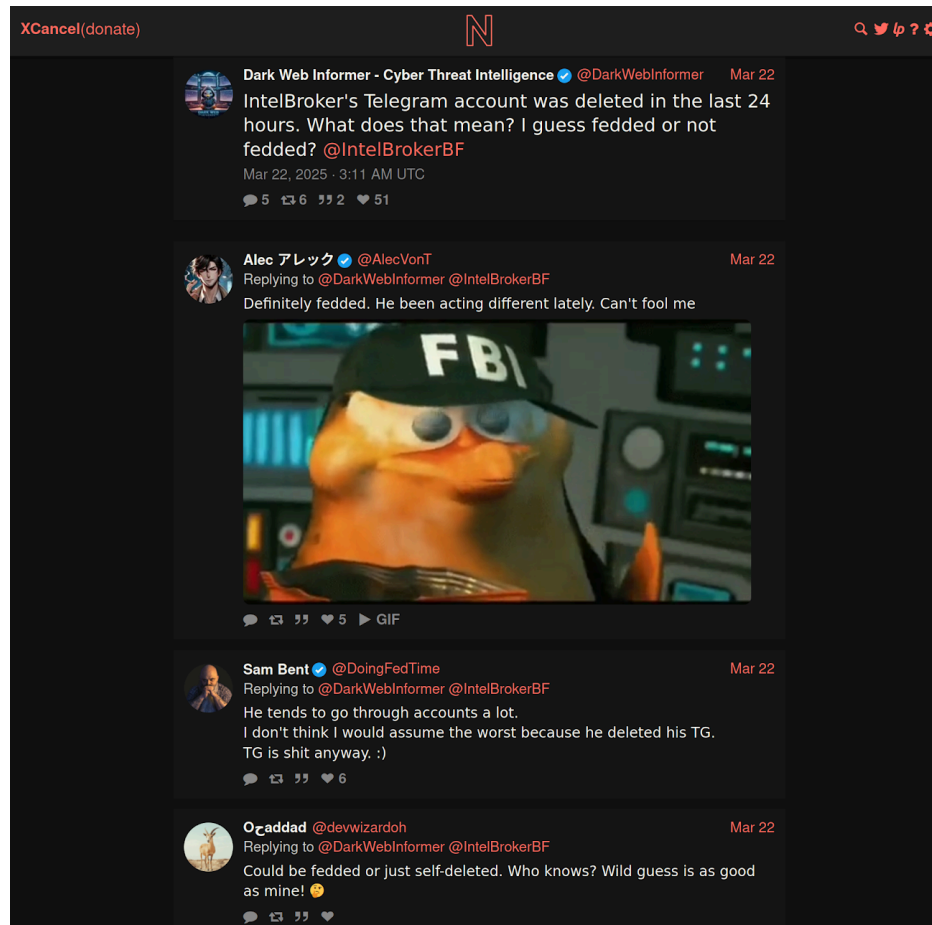
While DataSec's advertisement specifies the alleged ability to obtain official, government, and LE documentation such as crash reports and driver exchange forms, it is not clear the extent to which these can be leveraged in fraudulent claims; this will likely differ significantly between cases.

| IntelBroker's Atypical Activity Causes Suspicion Within Dark Web Forums

On March 22, 2025, the user "mzkz" started a discussion on the deep web forum BreachForums regarding rumors surrounding the threat actor "IntelBroker". According to the thread, IntelBroker has allegedly either been apprehended or recruited by the U.S. Federal Bureau of Investigations (FBI).

- IntelBroker is a notorious threat actor known for conducting a wide array of malicious cyber activity against diverse targets. IntelBroker is also thought to have fulfilled an administrative role within BreachForums and has also very likely operated under different pseudonyms.

One of the conversations likely referenced by mzkz was initiated by user "Dark Web Informer", who posted an article in the Xcancel community claiming that IntelBroker's Telegram account had been deleted. Other users within the discussion thread claimed that IntelBroker has been "acting different lately."



mzkz's original post on BreachForums

Source: ZeroFox Intelligence

As of the writing of this report, there is an unlikely chance that IntelBroker is operating in conjunction with the FBI. This is primarily due to the substantial lack of corroborating information. Such speculation surrounding IntelBroker has long occurred, beginning with the May 2024 LE seizure of BreachForums and continuing through a period of moderator changes. ZeroFox notes that the lack of any observable activity from IntelBroker during the past 45 days is highly unusual; however, the actor has stated on numerous occasions that they do not operate a Telegram account.

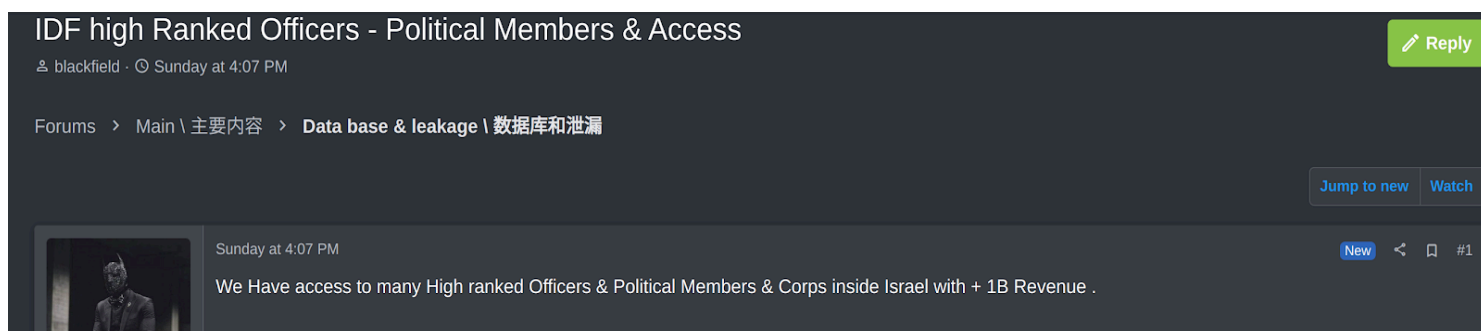
| Pro-Palestinian Hacktivist Group Targets Israel

On March 15, 2025, threat actor “blackfield” announced on the dark web forum RAMP that they had gained access to sensitive documents associated with high-ranking Israeli Defense Forces (IDF) officers, Israeli political figures, and an Israel-based healthcare organization with an annual revenue of USD 1 billion.

- Blackfield is part of the pro-Palestinian, anti-Israel hacktivist group Shadow, a collective responsible for numerous cyberattacks exclusively targeting Israeli infrastructure.
- The actor joined RAMP on February 5, 2023, where they have a “well-known member” reputation status.

No price for the full data set was observed; instead, prospective buyers were urged to make contact. Blackfield did specify, however, that prices would correlate to the “name + rank”—almost certainly alluding to that of the victim.

The advertisement included samples of the data allegedly stolen, very likely as an attempt to demonstrate legitimacy and encourage prospective buyers. These included 11 separate links leading to downloadable archives.



blackfield's original post on the RAMP forum

Source: Zerofox Intelligence

The nature of the data related to the IDF and Israeli political figures is not specified in the advertisement, though there is a very likely chance that it comprises primarily PII such as names, addresses, and contact information rather than classified government information.

Blackfield specified that information related to an Israel-based healthcare organization is associated with employees that have ties to the IDF and includes “personal information.” Unspecified information related to “hundreds of Israeli settlers” is also allegedly available.

Spoiler: Links

https://limewire.com/d/7fd7741e-5c6...f#0DLvAioudL24RhJgTdyrm_xbuBfbTNkHkKJkhqW4Dx-8
<https://c.mail.com/@1476496372009018175/KVxDUUE6mkzXXgM7hIRUJg>
<https://c.mail.com/@1476496372009018175/cpdv6cv8HIKGF17MnyqBsw>
<https://c.mail.com/@1476496372009018175/WKdcoRaHqEvuTuEj31MPHg>
<https://c.mail.com/@1476496372009018175/hWch-6yUn8PGDv6XXal46Q>
<https://c.mail.com/@1476496372009018175/qHv0nnwJ8Q9sNjlhccD8MA>
<https://c.mail.com/@1476496372009018175/Q3CoHVVY0Jg9SDtL4ygm8Uw>
<https://c.mail.com/@1476496372009018175/WBmOOACyHKLAExb0IUecOQ>
<https://c.mail.com/@1476496372009018175/ZQfdu6cDzgU-ULWho1bLyg>
<https://c.mail.com/@1476496372009018175/QhdZtmEOvbOtlNcQJhktXQ>
https://c.mail.com/@1476496372009018175/3t4paj-aFqmGwj_DHrkQw

For Sale : We still have access to Politcal Members "OutSide & Inside IL+ IDF ranked officers , The price will be related to the Name + Rank

Links to data samples available within blackfield's advertisement

Source: Zerofox Intelligence

On March 17 and 18, 2025, blackfield made subsequent posts proclaiming themselves a cyber espionage collective that targets only high-profile victims, unlike other collectives that target “women’s haircut stores and car washes.” A separate post warned that upcoming attacks would target U.S.-based entities and would appear to have been conducted by China, Iran, or North Korea.

Like other pro-Palestinian hacktivist groups, blackfield displays an overt hostility towards Israel and Israeli-based entities, which almost certainly extends to allies such as the United States, European nations, the European Union (EU), the North Atlantic Treaty Organization (NATO), and the West in general. Future activity from blackfield is very likely to target those perceived as misaligned with the interests of Palestine and Iran. Despite the clear ideological motivation, blackfield very likely also seeks to simultaneously financially profit from their attacks.

Information such as that advertised by blackfield almost certainly appeals primarily to other ideologically and politically motivated threat actors that would seek to leverage PII in further disruptive cyberattacks or in the planning of physical targeting.

| 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%