



**| Flash |**

# **New Malicious Tool Advertises Comprehensive Personal Information**

**F-2024-06-18a**

**Classification: TLP:CLEAR**

**Criticality: Medium**

**Intelligence Requirements: Deep and Dark Web, Personally Identifiable  
Information, Data Breach**

**June 18, 2024**

**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 June 18, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

# **| Flash | New Malicious Tool Advertises Comprehensive Personal Information**

## **> Key Findings**

- On June 16, 2024, a positive-reputation actor known as “spam\_assistant” announced a new tool called Data Fusion in the dark web forum Exploit. According to the advertisement, Data Fusion is capable of providing buyers with a significant amount of both personally identifiable information (PII) pertaining to individuals and organizational tax data.
- Unlike similar deep and dark web (DDW) services offering the sale of PII, Data Fusion is allegedly capable of creating bespoke background reports that summarize the requested data.
- PII such as that advertised by spam\_assistant is an integral aspect of many forms of cyberattack. Personal details are used to inform and enhance sophisticated social engineering attacks, such as spear phishing and business email compromise, or to enable fraudulent activity like identity theft and tax-related scams.
- Given the high and continuous demand for sensitive data such as PII, threat actors are almost certain to continue pursuing innovative, automated tools able to draw from an increasingly expansive repository of both publicly available information and illicit data leaks.

## Details

On June 16, 2024, a positive-reputation actor known as spam\_assistant announced a new tool called Data Fusion in the dark web forum Exploit. According to the advertisement, Data Fusion is capable of providing buyers with a significant amount of both PII pertaining to individuals and organizational tax data. The service is currently available via spam\_assistant's Telegram channel.

- PII is easily monetized in DDW marketplaces due to a consistent demand from threat actors with various motivations. It is usually sold either in the form of a complete data breach or via automated tools able to offer the buyer specific information.

Spam\_assistant alleged that they are in possession of data entries numbering in the billions pertaining to "all people in the world." Three hundred fifty million of these records are purported to be U.S.-based, and the actor claims to have various tax data for "more than half" of all U.S. organizations. Data Fusion can allegedly provide buyers with data such as:

- Social Security numbers (SSNs)
- Addresses, ZIP codes, and dates of birth (DOBs)
- Driver's license numbers
- Taxpayer Identification Numbers (TINs) and Employer Identification Numbers (EINs)

spam\_assistant

kilobyte



Paid registration

3

31 posts

Joined

07/10/20 (ID: 106192)

Activity

cnam / spam

Posted 34 minutes ago

We are happy to announce that we are launch Data Fusion! We created Automatized huge storebot marketplace fof all.

We have billions of data - all people in the world. (In different countries)

We have a base of more than 100m SSN data, and we can also find any SSN/DL, even that we do not have - and all this for our lovely customers.

We have a database of almost 350m US and we create own BG. Data Fusion Reports.

We have ALL EINs/TINs more than half US companies.

WE HAVE API FOR RESELLERS! and we can create duplicate our bot in few minutes for each reseller!

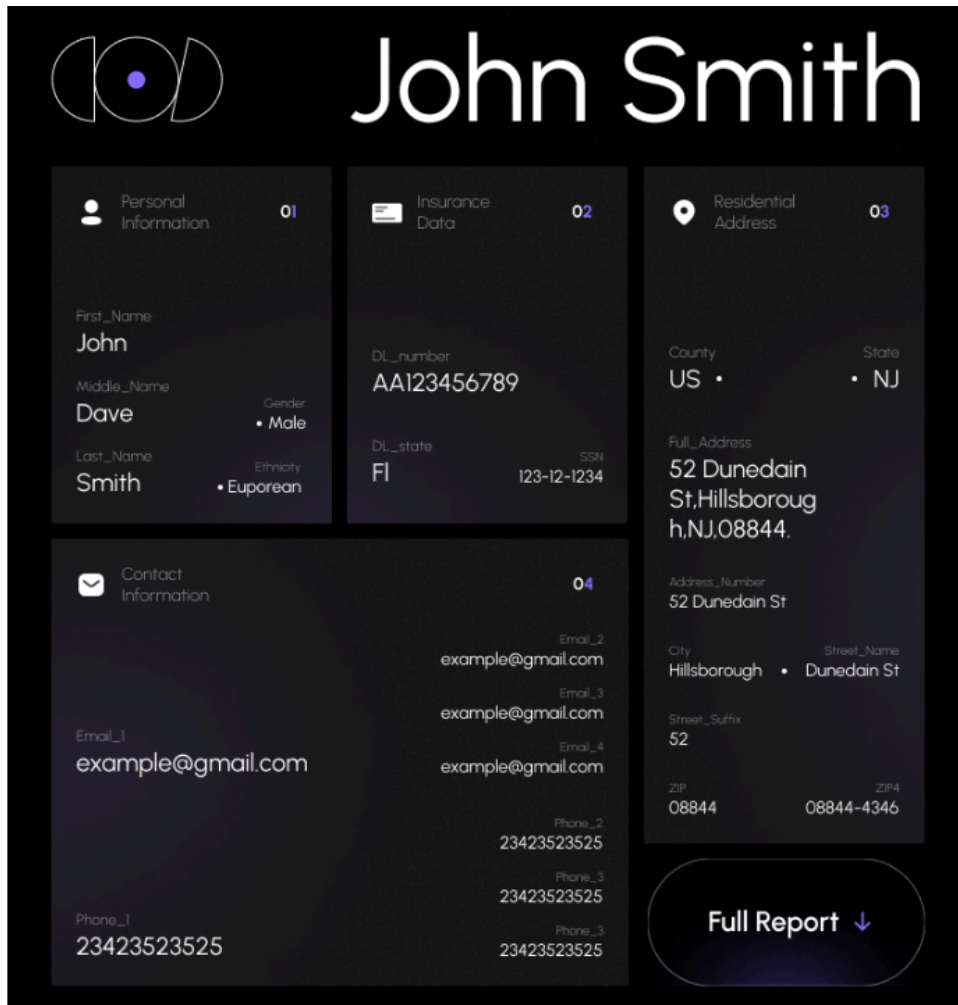
**DataFusion - We find All info about everyone to anyone!**

### Exploit post advertising the the launch of Data Fusion

Source: ZeroFox Intelligence

Unlike similar DDW services offering the sale of PII, Data Fusion is allegedly capable of creating bespoke background reports that summarize the requested data. The price of these reports varies depending upon the type of information requested, and—though discounts are available for bulk sales—no subscription-based model is available. As a result, Data Fusion is almost certainly more expensive than other methods of purchasing PII, many of which offer partial results for free.

- Data Fusion also allows resellers to access its Application Programming Interface, where they can advertise the platform's information. This is almost certainly intended to increase the service's market reach.



The image shows a dark-themed user interface for a report titled "John Smith". At the top left is a logo consisting of three overlapping circles with a purple dot in the center. The report is organized into four numbered sections:

- 01 Personal Information:** Displays First\_Name (John), Middle\_Name (Dave), Last\_Name (Smith), Gender (Male), and Ethnicity (European).
- 02 Insurance Data:** Displays DL\_number (AA123456789), DL\_state (FL), and SSN (123-12-1234).
- 03 Residential Address:** Displays County (US), State (NJ), Full\_Address (52 Dunedain St, Hillsborough, NJ, 08844), Address\_Number (52 Dunedain St), City (Hillsborough), Street\_Name (Dunedain St), Street\_Suffix (52), ZIP (08844), and ZIP4 (08844-4346).
- 04 Contact Information:** Displays multiple email addresses (example@gmail.com) and phone numbers (23423523525).

A "Full Report" button with a downward arrow is located at the bottom right of the report.

## Example of custom Data Fusion report

Source: ZeroFox Intelligence

The extent of information offered by Data Fusion is almost certainly exaggerated. Spam\_assistant very likely leverages a large and diverse number of data sources, including those that are publicly available (such as various government resources and historic data breaches, many of which very likely contain incorrect or extant information) and contemporary data breaches (many of which carry a price tag). It is unlikely that comprehensive and accurate information can be provided at the advertised breadth.

- While spam\_assistant claims that Data Fusion is an automated service, this is likely only partially true. The tool almost certainly requires a human element able to search for, compile, and supply the requested data.

PII such as that advertised by spam\_assistant is an integral aspect of many forms of cyberattack. Personal details are used to inform and enhance sophisticated social engineering attacks, such as spear phishing and business email compromise, or to enable fraudulent activity like identity theft and tax-related scams. PII is also regularly resold in other DDW forums, though—given the comparatively high price of Data Fusion—this is less likely.

Given the high and continuous demand for sensitive data such as PII, threat actors are almost certain to continue pursuing innovative, automated tools able to draw from an increasingly expansive repository of both publicly available information and illicit data leaks.

## **Recommendations**

- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Implement secure password policies with phishing-resistant multi-factor authentication (MFA), complex passwords, and unique credentials.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).
- 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.
- Develop a comprehensive incident response strategy.
- Configure email servers to block emails with malicious indicators and deploy authentication protocols to prevent spoofed emails.
- Deploy a holistic patch management process and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Proactively monitor for compromised accounts being brokered in DDW forums.
- Configure ongoing monitoring for Compromised Account Credentials.

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

|                                | <b>Red</b>                                                                                                                                                                                             | <b>Amber</b>                                                                                                                                                                                                                                                                                                                 |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>WHEN SHOULD IT BE USED?</b> | <b>Sources may use</b><br><b>TLP:RED</b> 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. | <b>Sources may use</b><br><b>TLP:AMBER</b> when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.                                                                                                           |
| <b>HOW MAY IT BE SHARED?</b>   | <b>Recipients may NOT share</b><br><b>TLP:RED</b> with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.                                     | <b>Recipients may ONLY share</b><br><b>TLP:AMBER</b> 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.<br><b>Note that</b><br><b>TLP:AMBER+STRICT</b> restricts sharing to the organization only. |
|                                | <b>Green</b>                                                                                                                                                                                           | <b>Clear</b>                                                                                                                                                                                                                                                                                                                 |
| <b>WHEN SHOULD IT BE USED?</b> | <b>Sources may use</b><br><b>TLP:GREEN</b> when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.              | <b>Sources may use</b><br><b>TLP:CLEAR</b> when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.                                                                                                                                                      |
| <b>HOW MAY IT BE SHARED?</b>   | <b>Recipients may share</b><br><b>TLP:GREEN</b> information with peers and partner organizations within their sector or community but not via publicly accessible channels.                            | <b>Recipients may share</b><br><b>TLP:CLEAR</b> 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%         |