



# | Flash |

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

F-2025-05-30a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Deep and Dark Web, Social Engineering

**May 30, 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 May 30, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

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

## **| Key Findings**

- 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.
- Sentap claimed 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.
- Sentap also claims that the data encompasses “strategic” regions of Illinois, Indiana, Wisconsin, Minnesota, Iowa, Colorado, and Kansas but offers no further context.
- If the data is as-advertised, its diverse nature would almost certainly appeal to a wide array of mostly financially motivated threat actors seeking to exploit personally identifiable information (PII).

## **| Details**

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, ownership history, 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 PII could be obtained from such documents:

- Names
- Addresses
- Dates of Birth
- Social Security numbers
- Phone numbers
- Email addresses
- Mortgage details
- Property description 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.

## **Recommendations**

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege, and implement network segmentation to separate resources by sensitivity and/or function.
- Implement phishing-resistant multi factor authentication (MFA), secure and complex password policies, and ensure the use of unique and non-repeated credentials.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud-based servers at least once per year—and ideally more frequently.
- 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 (DDW) forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).
- Utilize ZeroFox Intelligence and our proprietary platform to understand potential exposure in stealer logs.

## Appendix A: Traffic Light Protocol for Information Dissemination

|                         | Red                                                                                                                                                                                                    | Amber                                                                                                                                                                                                                                                                                                                        |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WHEN SHOULD IT BE USED? | <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.                                                                                                           |
| HOW MAY IT BE SHARED?   | <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. |
|                         | Green                                                                                                                                                                                                  | Clear                                                                                                                                                                                                                                                                                                                        |
| WHEN SHOULD IT BE USED? | <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.                                                                                                                                                      |
| HOW MAY IT BE SHARED?   | <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%         |