ZEROFOX INTELLIGENCE

Flash

ZeroBytes Targets French Agencies

F-2026-08-25a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Threat Actor, Ransomware, Data Leak

August 25, 2026

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 10:00 AM (EDT) on August 25, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | ZeroBytes Targets French Agencies

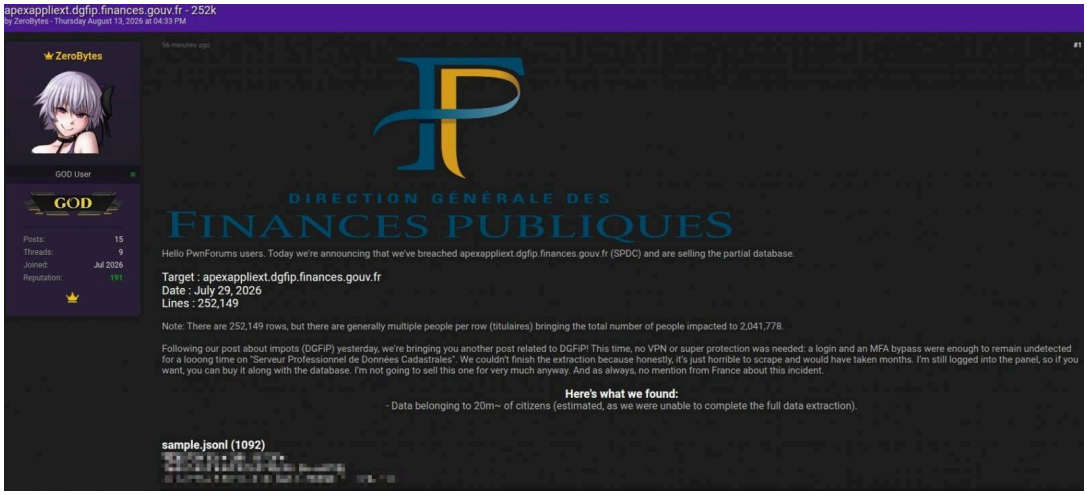
| Key Findings

- On August 13, 2026, threat actor "ZeroBytes" posted on the dark web forum PwnForums claiming to have breached France's Ministry of National Education; several days later, the group reposted the claim on its public X profile.
- The Ministry of National Education disclosed a breach on July 25, 2026, but claims that no student information, bank details, or passwords were stolen in the breach.
- This is the largest breach claimed by ZeroBytes and the second French central-government-body victim the group has claimed in under two months.
- There is a roughly even chance the threat actor maintains access to the data. If ZeroBytes' claim is legitimate, the group will almost certainly sell that access in addition to the exfiltrated data.
- ZeroBytes is almost certain to continue targeting French government agencies, and there is a roughly even chance the group will continue using social engineering and credential stuffing to gain ever-increasing levels of access to more secure data.

Details

On August 13, 2026, threat actor ZeroBytes posted on the dark web forum PwnForums claiming to have breached France's Ministry of National Education; several days later, the group reposted the claim on its public X profile. The actor claimed to have been detected by the ministry but not cut off and to have exfiltrated 43GB of data, including student records, teaching-staff identifiers, and a directory dump containing hashed passwords.[1]

- The Ministry of National Education disclosed a breach on July 25, 2026, but claims that no student information, bank details, or passwords were stolen.[2]
- This is the largest breach claimed by ZeroBytes and the second French central-government-body victim the group has claimed in under two months.[3]



ZeroBytes' PwnForums post (August 13, 2026)
Source: ZeroFox Intelligence

[1] hXXps://www.cyberdaily[.]au/security/14056-france-suffers-from-unprecedented-cyber-attack-wave-with-one-hacker-supposedly-behind-it-all
[2] hXXps://www.education.gouv[.]fr/incident-de-securite-affectant-les-donnees-de-personnels-de-l-education-nationale-505407
[3] hXXps://www.agenzianova[.]com/en/news/francia-hacker-di-zerobytes-rivendicano-attacchi-a-fisco-e-ministero-dellistruzione-colpito-ente-di-previdenza/

ZeroBytes' X post (August 17, 2026)
Source: hXXps:///x[.]com/ZeroBytesG/status/2089459694251233321

The discrepancy between government disclosure and threat actor claim is very likely a result of persistent access to databases. ZeroBytes claimed to maintain access to the Ministry of National Education's database, stating they are in possession of several rows of information for each person but did not extract the full dataset because scraping was taking too long.[4] There is a roughly even chance the threat actor maintains access to the data; if their claim is legitimate, ZeroBytes will almost certainly sell that access in addition to the exfiltrated data.

The French government confirmed the intrusions originated from legitimate accounts; in one instance, credentials were usurped between authorized parties over a virtual private network (VPN)[5] and in another the threat actor hijacked a professional account.[6] This indicates ZeroBytes very likely gained initial access via social engineering and phishing to acquire legitimate credentials.

ZeroBytes does not operate on an extortion model; the group runs no leak site and negotiates with no one. It lists stolen data for sale to third-party buyers who set their own

[4] hXXps://www.cyberdaily[.]au/security/14056-france-suffers-from-unprecedented-cyber-attack-wave-with-one-hacker-supposedly-behind-it-all
[5] hXXps://presse.economie.gouv[.]fr/acces-illegitime-au-systeme-dinformation-de-la-direction-generale-des-finances-publiques/
[6] hXXps://www.education.gouv[.]fr/incident-de-securite-affectant-les-donnees-de-personnels-de-l-education-nationale-505407

price and disclaims responsibility for what those buyers do next. The group is almost certain to continue targeting French government agencies.

It is unclear at this point if ZeroBytes has a larger goal beyond selling data. However, there is a roughly even chance the group will continue using social engineering and credential stuffing to gain ever-increasing levels of access to more secure data—and ZeroBytes is very likely to continue to focus on French targets.

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**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.	**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	Clear
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.	**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%