



| Flash |

NATO Data Leak Shared on Deep Web Forum

F-2024-05-24a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Data Leak

May 24, 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 17:00 AM (EDT) on May 23, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Flash | NATO Data Leak Shared on Deep Web Forum

› Key Findings

- On May 19, 2024, threat actor “Sumo” announced a data leak pertaining to a NATO school’s e-learning platform on the Russian-speaking deep web forum Cronos.
- It is likely that the data breach originated from an SQL injection vulnerability that was privately advertised for sale on Telegram in January 2024. The vulnerability allegedly implicated an unknown NATO entity.
- It is very likely that the intended use of this data is social engineering and other fraudulent activity, with a likely chance it has already been leveraged in attacks by financially-motivated threat actors.

Details

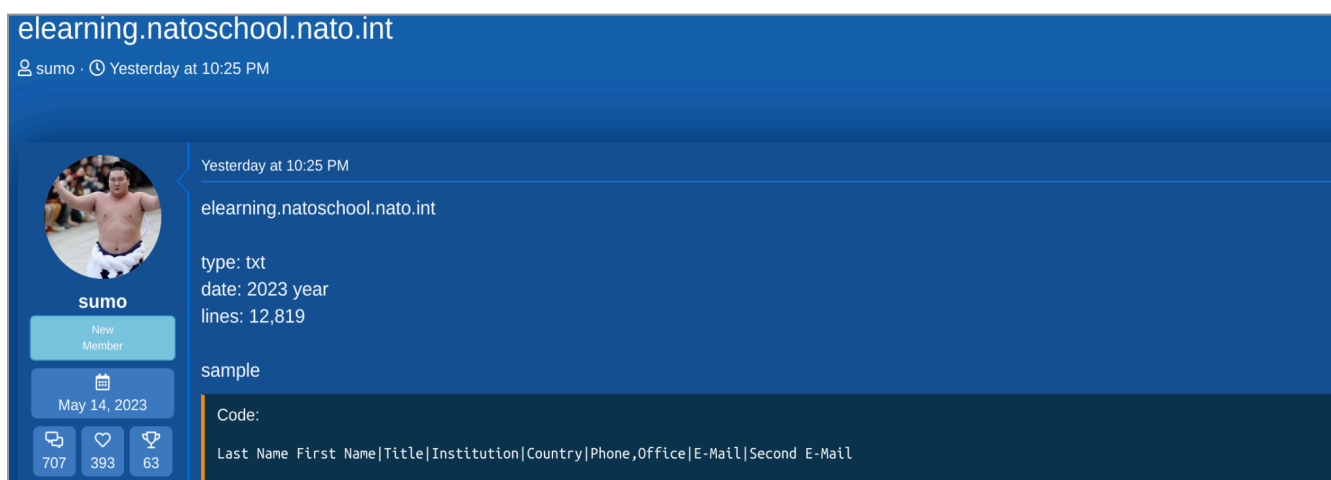
On May 19, 2024, threat actor Sumo announced a data leak pertaining to a NATO school’s e-learning platform on the Russian-speaking deep web forum Cronos. The data is available to all Cronos forum members that have paid for account privileges and could very likely be leveraged in various types of malicious social engineering activity.

- Sumo is a well-regarded, prolific distributor of data leaks in DDW forums, posting information stolen from both Western and Russian victims.

- The stolen data is primarily personally identifiable information (PII) such as names, titles, military ranks, institutions, countries, and contact information, likely pertaining to both military and civilian staff and e-learning students.

Cronos was created in 2022 and is focused on data breaches and hosting unique leaks, as well as republishing those from other forums. There is a roughly even chance that Cronos will increase its traffic and popularity following the recent closure of BreachForums.

- On May 15, 2024, English-language DDW forum BreachForums was seized in an operation coordinated by multiple international law enforcement agencies.
- Since mid-2023, BreachForums has been one of the most popular DDW marketplaces, hosting discussion surrounding the trading of illicitly-obtained goods.



Sumo's post on the forum Cronos

Source: ZeroFox Intelligence

It is likely that the data breach originated from an SQL injection vulnerability that was privately advertised for sale on Telegram in January 2024. The vulnerability allegedly implicated an unknown NATO entity.

- An SQL injection is a code injection technique used to attack data-driven applications that use SQL databases. It exploits security vulnerabilities in web applications that construct SQL statements from user input without properly sanitizing or validating that input.

It is very likely that the intended use of this data is social engineering and other fraudulent activity, with a likely chance it has already been leveraged in attacks by financially-motivated threat actors. There is also a smaller possibility that the information can be leveraged in geopolitically or ideologically-motivated espionage activity by state-associated actors.

| Recommendations

- Do not divulge personal details unless the sender of communications can be verified. The majority of legitimate organizations will not ask for such information via email.
- Ensure an organization-level system is in place that enables employees to report suspicious communications in order to bring awareness to ongoing campaigns and protect other users.
- Implement strong password policies and phishing-resistant multi-factor authentication (MFA).
- Implement a password policy mandating that passwords are at least 12 characters long and consist of upper and lowercase letters, numbers, and special characters. Passwords should be regularly changed and never reused.
- Maintain a principle of least trust by ensuring access is continuously scrutinized and adjusted and implementing identity and access management (IAM) solutions, along with network segmentation.
- Safeguard classified, sensitive, or business-critical assets using secure, off-site backup methods, compartmentalization, and authentication mechanisms.
- Organizations should implement training for employees focusing on awareness of contemporary threats, phishing vigilance, social engineering resilience, and basic cybersecurity hygiene.

| 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%