



| Flash |

Dark Web Actors Promoting Maritime Data

F-2024-01-17d

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Geopolitical, Supply Chains

January 17, 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 10:00 AM (EST) on January 17, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash |

Dark Web Actors Promoting Maritime Data

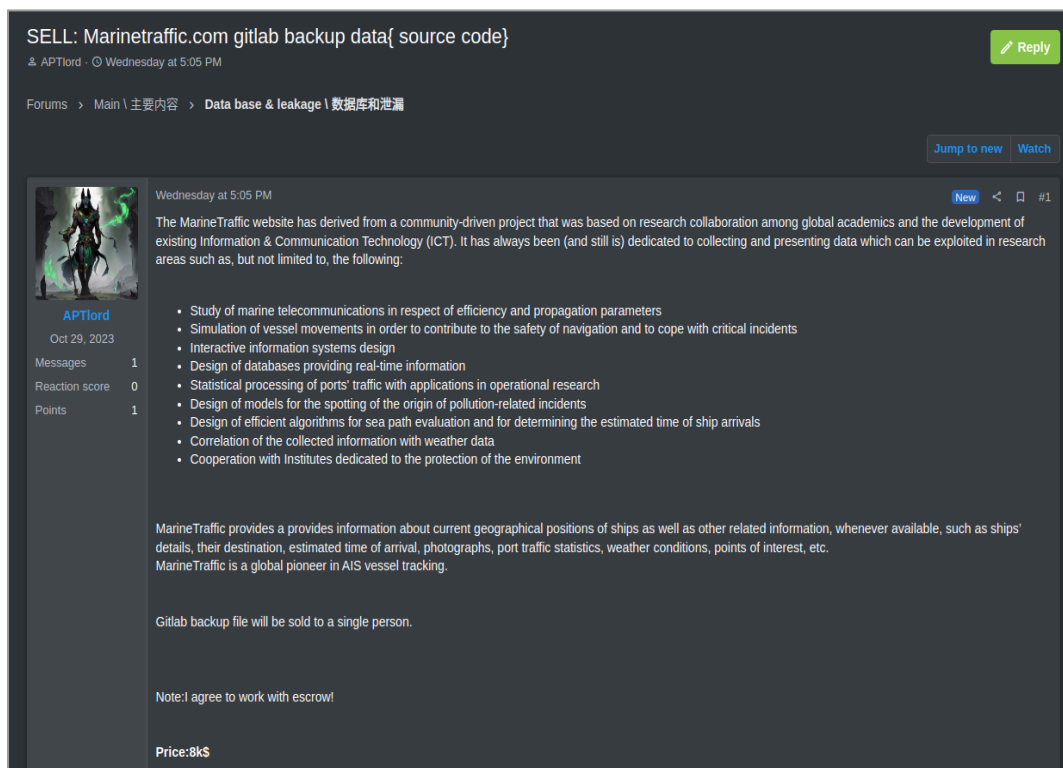
› Key Findings

- ZeroFox has identified at least two instances in which threat actors are selling data that provides real-time information on maritime vessels, including the geographic positions of vessels, vessel details, journey details, and data on maritime infrastructure.
- The leaked data has little monetary value for the buyer or seller and may demonstrate that politically-motivated actors will forgo profit to achieve their ideological aims, and there will likely be continued convergence between geopolitical issues and cybersecurity threats.
- Houthi attacks targeting commercial vessels transiting the Red Sea have resulted in significant political gains for the group and have caused major disruptions to global supply chains.
- There are other important shipping lanes across the globe, and threat actors may view obtaining similar datasets as helpful to achieving their political aims or harming their political adversaries.

Details

On December 27, 2023, threat actor “APTlord” announced on dark web forum RAMP that they were selling source code and other information owned by marinetraffic[.]com, which was allegedly obtained by the theft of backup data from web-based Git repository GitLab. Marinetraffic[.]com is an open-source analytics platform that provides real-time information on maritime vessels and activity around the globe. Some of the information available includes:

- The geographic positions of vessels (accuracy and update frequencies vary between vessels)
- Vessel details (such as photographs, country of operation, speed, design, and other physical attributes)
- Journey details (such as originating locations, destinations, and expected arrival times)
- Information relating to maritime infrastructure (such as port locations, capacity, traffic statistics, and weather conditions)



SELL: Marinetraffic.com gitlab backup data{ source code}
▲ APTlord · Wednesday at 5:05 PM

Forums > Main \ 主要内容 > Data base & leakage \ 数据库和泄露

Jump to new Watch

Wednesday at 5:05 PM

APTlord
Oct 29, 2023
Messages 1
Reaction score 0
Points 1

The MarineTraffic website has derived from a community-driven project that was based on research collaboration among global academics and the development of existing Information & Communication Technology (ICT). It has always been (and still is) dedicated to collecting and presenting data which can be exploited in research areas such as, but not limited to, the following:

- Study of marine telecommunications in respect of efficiency and propagation parameters
- Simulation of vessel movements in order to contribute to the safety of navigation and to cope with critical incidents
- Interactive information systems design
- Design of databases providing real-time information
- Statistical processing of ports' traffic with applications in operational research
- Design of models for the spotting of the origin of pollution-related incidents
- Design of efficient algorithms for sea path evaluation and for determining the estimated time of ship arrivals
- Correlation of the collected information with weather data
- Cooperation with Institutes dedicated to the protection of the environment

MarineTraffic provides a provides information about current geographical positions of ships as well as other related information, whenever available, such as ships' details, their destination, estimated time of arrival, photographs, port traffic statistics, weather conditions, points of interest, etc. MarineTraffic is a global pioneer in AIS vessel tracking.

Gitlab backup file will be sold to a single person.

Note: I agree to work with escrow!

Price: 8k\$

RAMP post advertising the sale of source code owned by marinetraffic[.]com

Source: ZeroFox Intelligence

Then, on January 13, 2024, threat actor “Drechsler” announced on the same RAMP forum that they had dumped the source code of Maritime Situation Inconsistency Analysis (ANAIS), a software used for the analysis of maritime space by the French Navy. ANAIS aims to aggregate and process maritime data more efficiently, especially in regards to suspicious or dangerous vessel behavior, in order to facilitate intervention decisions. ANAIS also allegedly features innovations in maritime research and intelligence pertaining to the development of maritime AI, among other things.

Problematic

The ANAIS project (for “Maritime Situation Inconsistency Analysis”) aims to better aggregate maritime data to process it more efficiently. The objective is to better monitor the multiple activities at sea, and in particular detect suspicious or dangerous vessel behavior in order to decide more quickly and intervene more effectively. The idea is to start by working on the global flow of ship positions coming from the European Maritime Safety Agency, in collaboration with the Maritime Affairs Directorate. This basic data will be enriched throughout the project by other data sources and analyzed in greater detail.

Goals

Keep the agile team as close as possible to operational users Regularly secure developments to deploy more widely Make a lighter version of ANAIS available to the academic world to deepen the algorithm

Results

Concrete and recognized operational contribution
Testing of an innovative method and tool by the Navy.
Issues of digital sovereignty and development of maritime AI
ANAIS is accessible by invitation link

About the source code :

- Git history included, so you can see history
- about 50 MB of content (compressed)
- Estimated cost of creation of this software, for french military services, according to data leaked, is \$800/day for 2 developers since late 2018 = At least \$1m (lowest estimation)
- Software deployed to french aircraft carrier, according to another leak

anais.infrastructure/
commits count: 66
Latest commit dumped: 2020-11-25
anais.kubernetes/
commits count: 5
Latest commit dumped: 2020-09-15
anais.loader/
commits count: 700
Latest commit dumped: 2021-03-10
anais.map-proxy/
commits count: 15
Latest commit dumped: 2021-02-09
anais.ports/
commits count: 3
Latest commit dumped: 2020-11-12
anais.scripts/
commits count: 14
Latest commit dumped: 2020-11-16
anais.server/
commits count: 117
Latest commit dumped: 2019-10-09
h3clock.rust/
commits count: 28
Latest commit dumped: 2021-05-06

RAMP post advertising the sale of source code for ANAIS software

Source: ZeroFox Intelligence

On the same day, Drechsler also published another French military-related leak of management software “Les alpps,” which is used by the 27th Mountain Infantry Brigade. The software aims to facilitate mountain training operations and improve reaction time in the event of an accident during such operations.

[Free][Army related][France] Software that manage internship for 27th Mountain Infantry Brigade

& Drechsler · Saturday at 3:27 PM

Forums > Main \ 主要内容 > Data base & leakage \ 数据库和泄漏

Jump to new Watch

D

Drechsler

Nov 21, 2023

Messages 2

Reaction score 0

Points 1

Saturday at 3:27 PM

As we want to proof our claim about accessing french military code bases, we're releasing here the source code of "Les alpps" for free, because estimated value is low.

Archive password : rampio

<https://ufile.io/kzn7qkuq>

mirror <https://file.io/gSaALP18ZEHg>

About the software, translated from french via deepl

Reply

Making mountain outings safer for militaries

Context

The EMHM (Ecole Militaire de Haute Montagne), part of the 27th Mountain Infantry Brigade, employs military and civilian mountain instructors, all experts in their field. These instructors focus primarily on two crucial activities: Training and assessing trainees. Mountain training, in both summer and winter, to ensure they remain seasoned in this dangerous and demanding environment. As part of these activities, not only instructors, but also all qualified people who need to train, must prepare their itinerary when they go into the mountains, and submit it to their corps leader for validation. This procedure, known as FACM (Fiche d'Activité à Caractère Montagne), enables them to be covered in the event of an accident, but also to inform their comrades of their itinerary and timetable, so as to facilitate the activation and intervention of emergency services in case of need.

Issues

The FACM application and validation procedure is based on a paper form requiring the approval and signature of several parties. This inflexible process can be laborious, and sometimes leads to people leaving without a FACM. The assessment of trainees, the planning of training courses and the processing of their results is also a lengthy process involving multiple players. To avoid a multiplication of tools, EMHM wanted a single tool on which its staff could manage their two main activities.

Objectives

- Simplify the creation and processing of FACMs to optimize the responsiveness of sights and signatories, and reduce processing times.
- Maximize FACM coverage for mountain outings
- Manage courses and evaluate trainees according to given skill criteria
- Have an application accessible via Millistore

RAMP post advertising the sale of French Army training software “Les alpps”

Source: ZeroFox Intelligence

Analyst Commentary

In the first hack on December 13, 2023, APTlord asserts that some of the website's research areas—such as interactive information systems design, design of databases providing real-time information, and correlation of the collected information with weather data—can be exploited. However, the price requested for the data is USD 8,000,

and the threat actor claims that the information will only be sold to a single buyer. This is at odds with most disclosures on the deep and dark web (DDW), where profit-seeking is the primary motive.

In the two attacks on January 13, Drechsler does not mention a price but claims the ANAIS software itself is worth USD 1 million. However, ZeroFox assesses that the value of the leaked source code in terms of the ability of the purchaser to profit is close to zero. Rather, the value of these leaks may be ideological, and threat actors selling or purchasing the data may be inspired by other attacks on maritime targets.

It is unclear how this information could be directly leveraged to facilitate attacks against maritime targets—especially given the abundance of maritime data already publicly available. However, Houthi rebel attacks in the Red Sea region since mid-November have had significant impacts on international trade and demonstrate the vulnerability of international shipping.

- There have been approximately 30 Houthi-sponsored attacks since mid-November.¹ While no vessel targeted has failed to complete its journey—and the sophistication of the Houthi munitions is limited compared to the U.S.-led multinational task force patrolling the area—the attacks have still had significant impacts.
- Houthi rebels originally stated they were targeting ships linked to Israel. They then expanded that to the United States and United Kingdom (UK) after those countries launched direct attacks on Houthi positions in Yemen in mid-January.²
- About half the vessels that normally transit the Red Sea have decided to take a longer and more expensive journey around southern Africa instead, adding 10 days to the journey and millions in additional costs.
- Shipping companies are charging ships still traversing the area a 1 percent risk cover of the ship's value, up from one tenth of a percent before the attacks.³ With this increase, a ship carrying USD 100 million worth of cargo would now need to pay USD 1 million to get insurance.

¹ [hXXps://edition.cnn\[.\]com/2024/01/15/politics/houthi-missile-strikes-us-owned-ship/index.html](https://edition.cnn.com/2024/01/15/politics/houthi-missile-strikes-us-owned-ship/index.html)

² [hXXps://abcnews.go\[.\]com/Politics/us-carries-new-airstrike-houthis-yemen/story](https://abcnews.go.com/Politics/us-carries-new-airstrike-houthis-yemen/story)

³

[hXXps://www.bloomberg\[.\]com/news/articles/2024-01-16/insurers-look-to-exclude-us-uk-ships-from-red-sea-cover](https://www.bloomberg.com/news/articles/2024-01-16/insurers-look-to-exclude-us-uk-ships-from-red-sea-cover)

- Insurance companies are inserting clauses that their coverage does not apply to ships with U.S., Israeli, or UK interests.
- The cost to ship from Asia to Northern Europe has increased by 176 percent in one week ending January 11.⁴ The cost of the Asia-to-U.S. East Coast route, which also traverses the Red Sea, has increased 50 percent in a week.
- There have also been cost increases on routes that avoid the area. The Asia-U.S. West Coast route has seen a 50 percent jump in costs due to more companies using it as an alternative supply chain.⁵ There are also the added costs of delivering goods by truck or rail from the U.S. West Coast to their intended destination on the East Coast.

Threat actors may view the success the Houthis have had at disrupting global trade along a key supply chain that handles 12–15 percent of global trade⁶ and attempt to apply it elsewhere. Possible targets include the Malacca Strait between Indonesia and Malaysia, which handles 28 percent of global trade; the South China Sea, responsible for 30 percent; and the East China Sea, which handles 21 percent.⁷

Pro-Chinese or North Korea threat actors could be inspired by events in the Red Sea to target ships and thus harm the economies of Taiwan, Japan, and South Korea. These countries are all major technology exporters that import most of their energy by sea. Were these passageways to become impassable, there would be major cost increases and delivery issues for consumer electronics like laptops, smartphones, semiconductor chips, and oil and gas.

Conclusion

Recent data leaks on the RAMP forum do not align with the typical profit-making schemes on the DDW. However, geopolitically-engaged threat actors may nevertheless see value in such leaks if they can be used to achieve their goals or harm their

⁴ <https://www.freightos.com/january-10-2024-update/>

⁵

<https://www.supplychaindive.com/news/ocean-freight-rates-continue-climb-red-sea-crisis-Suez-Canal/704386/>

⁶ <https://www.bbc.com/news/business-67980256>

⁷

<https://www.bloomberg.com/opinion/articles/2024-01-14/supply-chains-canal-aren-t-the-biggest-shipping-chokepoints>

adversaries. The increasing regularity of these sorts of leaks could be tied to the growing convergence of geopolitical tensions and cyber threats.

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%