ZEROFOX INTELLIGENCE

Flash

0APT Syndicate Lacking Credibility

F-2026-02-19a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Malware, Threat Actor, Ransomware

February 19, 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 8:00 AM (EST) on February 19, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | 0APT Syndicate Lacking Credibility

| Key Findings

- ZeroFox assesses that newly founded and self-proclaimed ransomware-as-a-service (RaaS) collective 0APT Syndicate (0APT) is very likely a scam or hoax group. As of this writing, the group has not published any legitimate data from its list of 200 alleged victim companies; further, the purported data samples on its leak site cannot be downloaded and appear to be entirely fabricated.

- While little is known about the group at this time, the operators have explicitly stated that they are politically neutral and motivated solely by financial gain. Although the ransomware 0APT purports to be using is fully functional, it was first created in 2011 and most recently updated in 2023—making it unlikely the group is actually conducting data breaches, as operational ransomware groups typically update their executables more frequently.

- All available evidence suggests that 0APT is almost certainly a scam and not a legitimate threat at this time.

Details

ZeroFox assesses that newly founded and self-proclaimed RaaS collective 0APT is likely a scam or hoax group; as of this writing, their leak site has been offline since sometime after February 10. From its founding on January 28, 2026, to the present, it is very likely that 0APT has not published any legitimate data from its list of 200 alleged victim companies.[1] The data samples it has released appear to be entirely fabricated, and there is a roughly even chance they were compiled using unsophisticated artificial intelligence tools.

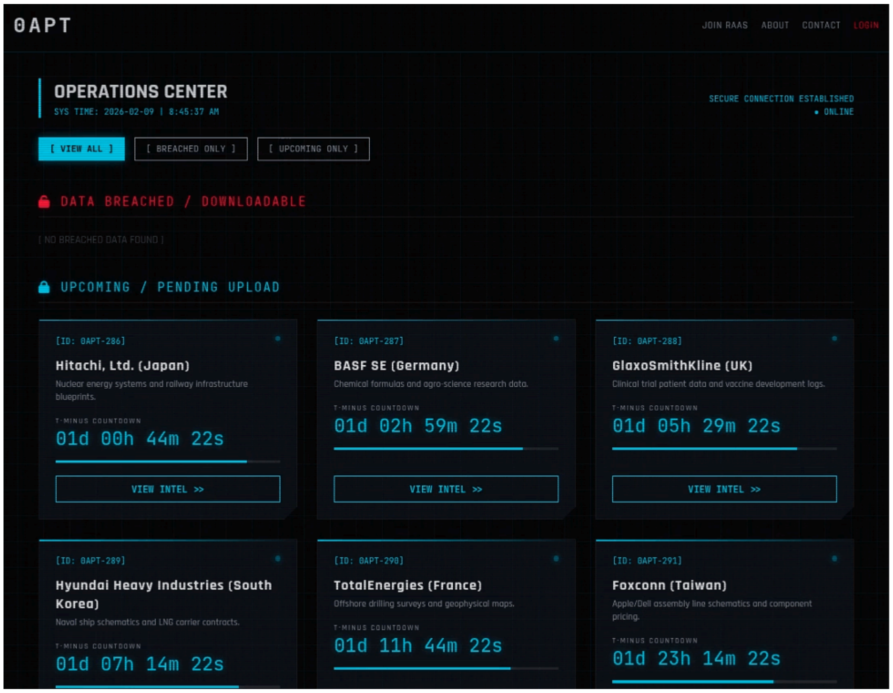
0APT's data leak site was abruptly taken offline on February 8, 2026, following several reports questioning its number of purported victim companies. When the site came back online the following day, the number of published victims had been reduced to 54. The site was subsequently taken down again sometime after February 10—likely by 0APT itself—and remains offline.

- Reports from security researchers indicate that at least two of the listed victim companies have not experienced a breach.
- Notably, 0APT's data leak site resembles a site previously used by the well-established ransomware group ShinyHunters, where data from a January 2026 breach was posted.

Although little is known about the group, the design of its data leak site has the look and feel of a legitimate RaaS platform, offering a locker, chat support, and negotiation services; additionally, the operators explicitly stated that they are politically neutral and motivated solely by financial gain. The ransomware 0APT claims to be using for data extraction is fully functional but was first created in 2011 and most recently updated in 2023, making it unlikely the group is actually conducting data breaches; operational ransomware groups typically update their executables more frequently. Additionally, 0APT appears to be overloading target systems with data, creating the illusion that a 20GB file is being extracted.

[1] hXXps://hackread[.]com/cybercrime-group-0apt-faking-breach-claims/

- ZeroFox observed that attempts to download sample data from 0APT's leak site are throttled to the point that it would take an estimated 7,000 days to complete the download. This is almost certainly because the data is not there, and the supposedly available samples are only posted to make the site look legitimate.



OPERATIONS CENTER
SYS TIME: 2026-02-09 | 8:45:37 AM

SECURE CONNECTION ESTABLISHED
● ONLINE

DATA BREACHED / DOWNLOADABLE

[NO BREACHED DATA FOUND]

UPCOMING / PENDING UPLOAD

[ID: 0APT-286]
Hitachi, Ltd. (Japan)
Nuclear energy systems and railway infrastructure blueprints.
T-MINUS COUNTDOWN
01d 00h 44m 22s

[ID: 0APT-287]
BASF SE (Germany)
Chemical formulas and agro-science research data.
T-MINUS COUNTDOWN
01d 02h 59m 22s

[ID: 0APT-288]
GlaxoSmithKline (UK)
Clinical trial patient data and vaccine development logs.
T-MINUS COUNTDOWN
01d 05h 29m 22s

[ID: 0APT-289]
Hyundai Heavy Industries (South Korea)
Naval ship schematics and LNG carrier contracts.
T-MINUS COUNTDOWN
01d 07h 14m 22s

[ID: 0APT-290]
TotalEnergies (France)
Offshore drilling surveys and geophysical maps.
T-MINUS COUNTDOWN
01d 11h 44m 22s

[ID: 0APT-291]
Foxconn (Taiwan)
Apple/Dell assembly line schematics and component pricing.
T-MINUS COUNTDOWN
01d 23h 14m 22s

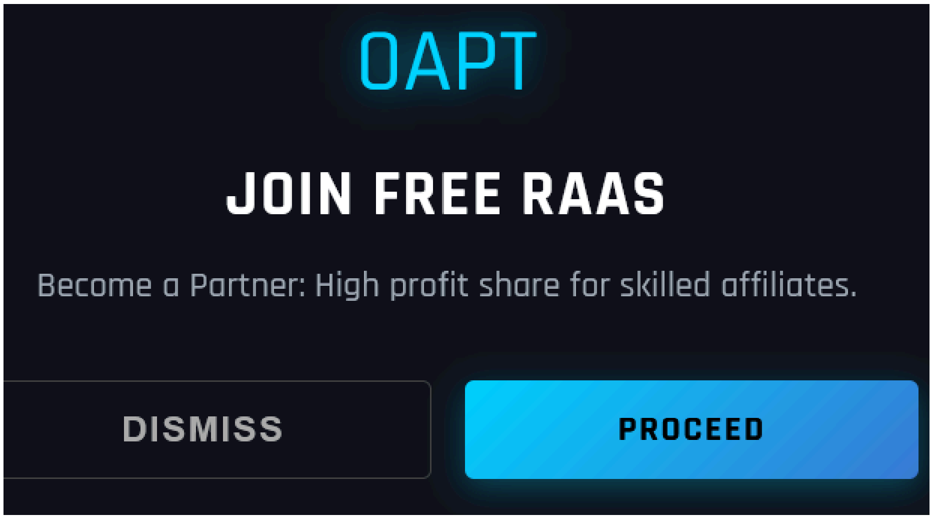
0APT's data leak site

Source: ZeroFox Intelligence

0APT's tactics suggest this is highly likely a scam campaign with two objectives. The first is likely to collect a ransom from the organizations 0APT claims to have attacked. This almost certainly has a low likelihood of success, as the targeted organizations' internal cybersecurity and analysis has not revealed that any breaches have occurred.[2] A second, very likely to be more successful objective is to target potential affiliates with 0APT's advertised RaaS program. Although the group's affiliate message calls it a "free Raas," 0APT is asking for a 1 Bitcoin assessment fee (approximately USD 67,000 at the time of writing) to join its affiliate program.[3] Given the nature of 0APT's observed operation, ZeroFox assesses it is highly unlikely that the affiliate program exists.

[2] hXXps://www.bankinfosecurity[.]com/fake-out-0apt-data-leak-ransomware-group-branded-scam-a-30726
[3] *Ibid.*

- A threat actor known as “Mogilevich” conducted a similar operation in early 2024. In that case, the actor eventually came forward and admitted the fraud, claiming to have gained USD 85,000 as a result of the scam.



JOIN FREE RAAS

Become a Partner: High profit share for skilled affiliates.

0APT affiliate program message

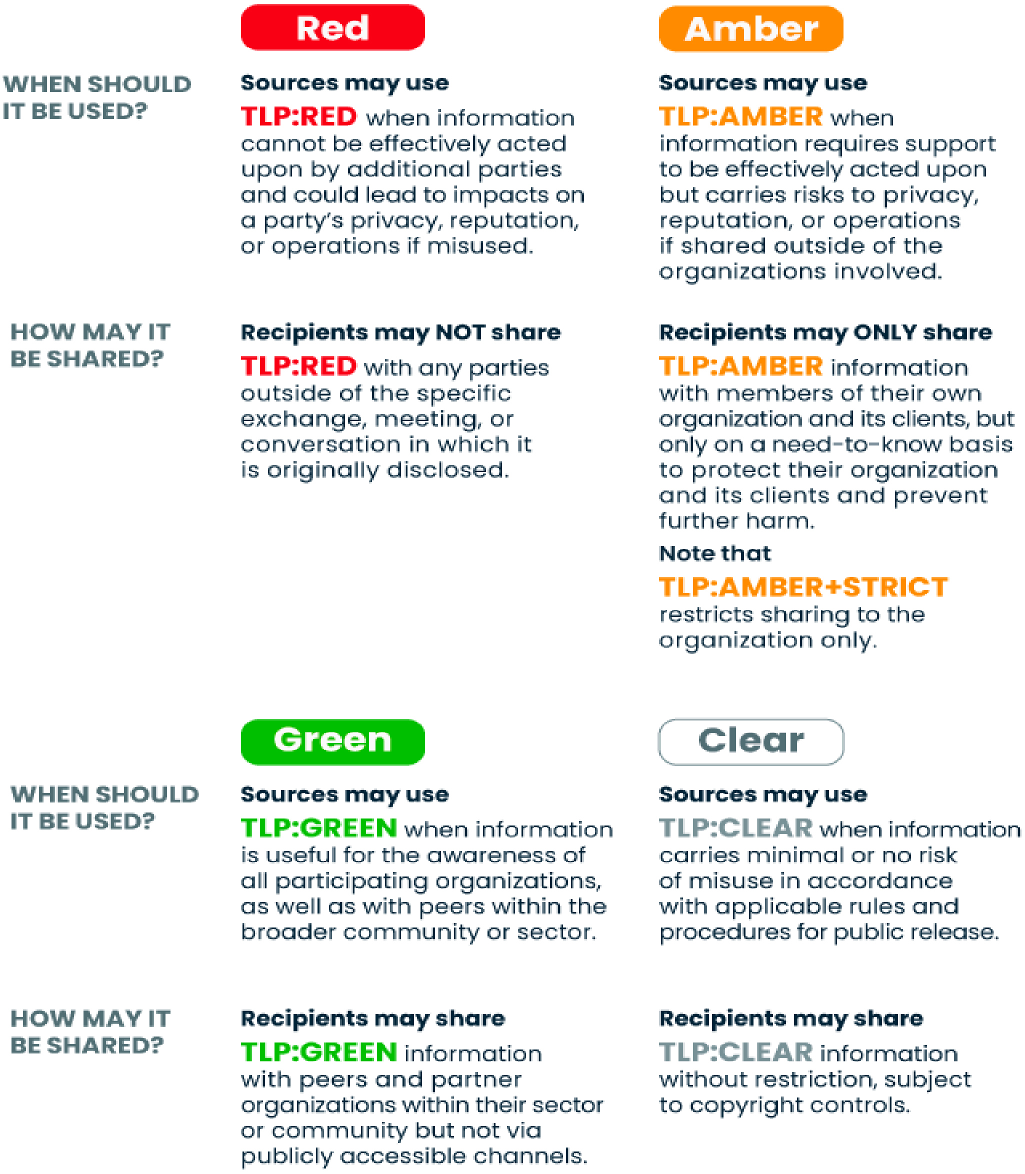
Source: ZeroFox Intelligence

All available evidence suggests that 0APT is almost certainly a scam and not a legitimate threat at this time. In the future, if the group were to start using an updated ransomware panel or demonstrating actual data extraction from targets, that would indicate it had likely developed into a more serious threat. Currently, 0APT is almost certainly operating a scam primarily targeting other cybercriminals.

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- 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.
- Implement secure password policies, phishing-resistant multi-factor authentication (MFA), and unique credentials.
- 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).

Appendix A: Traffic Light Protocol for Information Dissemination

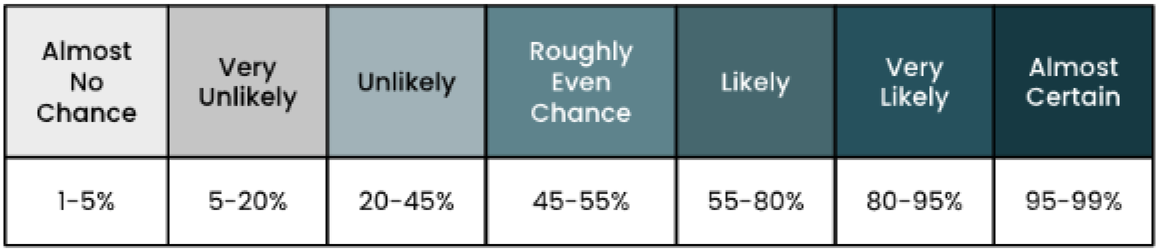


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** **TLP:AMBER** when information requires support to be effectively 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%