



| Brief |

The Underground Economist: Volume 5, Issue 1

B-2025-01-17a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Threat Actor

January 17, 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 January 17, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 5, Issue 1

| Actor Offers Access to Law Enforcement Portals

On January 12, 2025, actor “vadimblyaa” posted on BreachForums advertising alleged access to over 100 government and law enforcement (LE) email accounts across Europe, Asia, South America, and Africa. According to vadimblyaa, the accounts can be leveraged to access LE portals associated with organizations such as PayPal, TikTok, Instagram, and Google.

- LE portals are used by government entities to facilitate Emergency Data Requests (EDRs) and Law Enforcement Requests (LERs). These requests for information are issued by LE entities in order to gain access to personal information held by private organizations in the event of suspected criminal activity.
- Requested personal information can include names, addresses, contact details, IP addresses, passwords, geolocation data, and details surrounding financial transactions. Typically, a LE entity may only request information regarding a citizen within their jurisdiction.

Yesterday, 03:10 PM. (This post was last modified: Yesterday, 03:13 PM by vadimblyaa.)

Selling Access to **Law Enforcement + Government** email accounts.

We have access to **over 100 Emails** from countries across continents such as **Europe, Asia**, South America, and Africa.

With these mails, you can access **Law Enforcement Panels** for companies such as **Paypal, Tiktok, Instagram, Google**, etc. And you can request emergency data for anyone you want.

Escrow / Middleman is **ALWAYS** accepted.

Contact:

Telegram - vadimblyaa

Signal - vadimblyaa.77

qTox - E745132EE07E3721131BB5E52805B6EEDBF00A0465A29B0C4357BAC33AD2C15894D07FC8DD7D

Session - 05d65ce6c54c926ff5e3d11dd0e33881297f45458cbe4c333bdf4419368f26736d

(If you contacted me on any platform other than Telegram, please leave a comment to let me know.)

BreachForums post by vadimblyaa advertising email accounts

Source: ZeroFox Intelligence

The majority of vadimblyaa's previous activity in the forum relates to various compromises of LE and government departments from multiple countries. In 2024 the actor advertised databases allegedly belonging to police departments based in South American nations, as well as a nine-gigabyte data breach allegedly stolen from the California Secretary of State in the United States.

- ZeroFox observed speculation amongst other forum users that vadimblyaa's compromises have been achieved through the leveraging of Username:Password:URL (ULP) data extracted from botnet logs.

Search Results	
Thread / Author	
SELLING Access To Government + Law Enforcement Mails.	★ vadimblyaa
COLLECTION 12340 policia.rionegro.gov.ar personnel	★ vadimblyaa
USA California Secretary of State + documents. 9gb (1 2)	★ vadimblyaa
2600 rosey.ch emails + full names.	★ vadimblyaa
800 Puerto Rico Police Personell.	★ vadimblyaa

BreachForums post by vadimblyaa advertising email accounts

Source: ZeroFox Intelligence

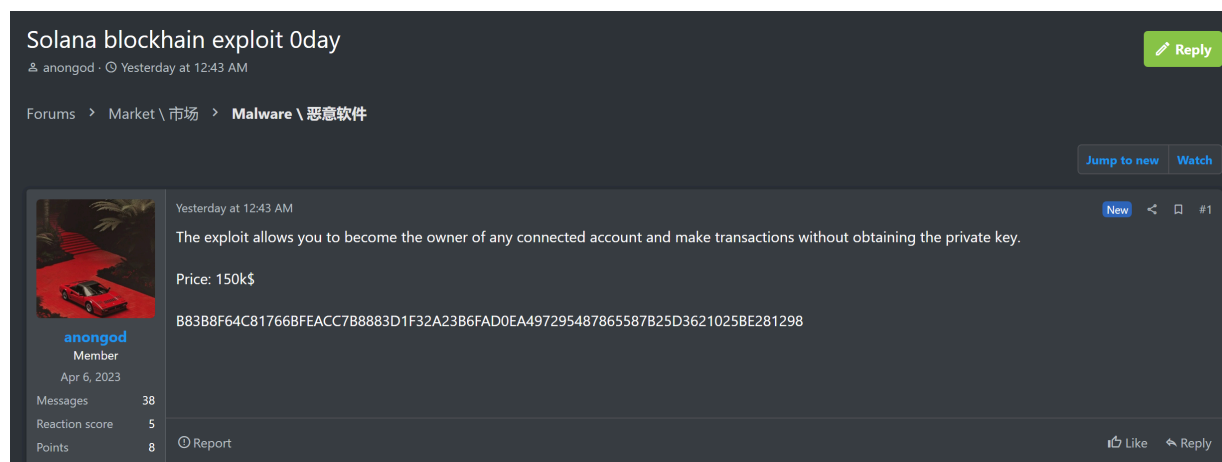
Unauthorized access to LE panels enable a malicious actor to submit fraudulent data requests to organizations, some of which hold vast quantities of personally identifiable information (PII) and personal financial information (PFI) relating to customers and end users. As LE panels vary by use case, the ease of which such requests could be made and successfully fulfilled is not clear. However, accounts associated with LE panels have often already obtained specific clearances and met any outlined requirements, very likely leading to lessened scrutiny upon data requests.

If successfully exploited, threat actors will likely seek to obtain the data of specific individuals—such as government officials, company executives, celebrities, or other high-profile entities—with the intent of conducting subsequent malicious activities of a cyber or physical nature.

| Blockchain Zero-Day Vulnerability Advertised for Sale

On January 5, 2025, English-speaking threat actor “anongod” posted in the popular deep web hacking forum RAMP advertising a zero-day vulnerability that allegedly targets the Solana Blockchain platform. The listed price for the vulnerability was USD 150,000.

- Solana is a decentralized blockchain that was launched in 2020. The platform gained popularity due to low transaction fees, scalability, a fast-growing ecosystem supporting decentralized finance (DeFi), non-fungible tokens (NFTs), and Web3 applications, as well as its unique implementation of Proof of History (PoH) and Proof of Stake (PoS) consensus mechanisms.
- Anongod joined RAMP in 2023 and has a mixed reputation on the forum. The actor has previously advertised alleged zero-day vulnerabilities targeting web applications and operating systems and has also sought to acquire stolen data relating to Blockchain networks.

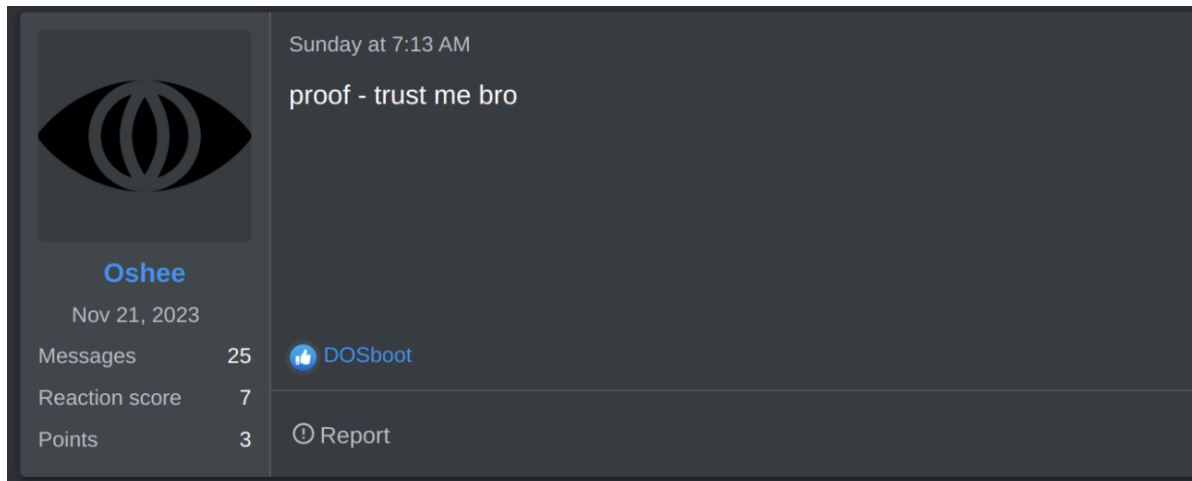


RAMP post by anongod advertising alleged zero-day vulnerability

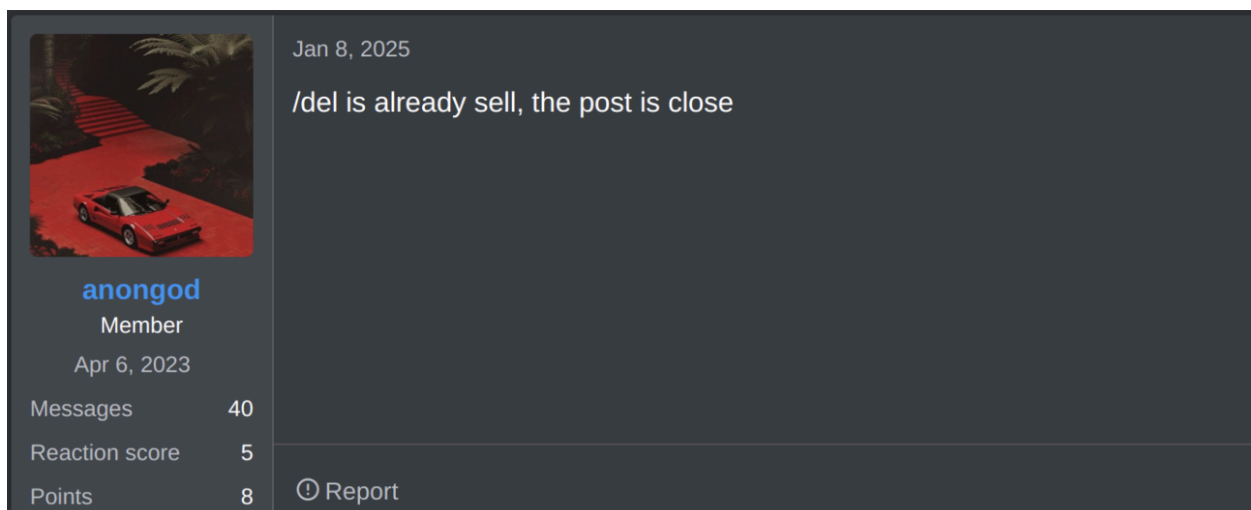
Source: ZeroFox Intelligence

According to anongod, successful exploitation of the vulnerability enables an attacker to “become the owner” of a connected account and conduct transactions without obtaining a private key. No further detail is provided to specify how the vulnerability is exploited, the private keys are bypassed, or how other security features such as multi-signatures and multi-factor authentication (MFA) are circumvented.

The advertisement elicited a skeptical response from forum users, who questioned why anongod was offering to sell such a potentially lucrative vulnerability rather than exploiting it themselves to generate significantly more revenue. Forum user “Oshee” alluded to insufficient credibility; responses from anongod suggested that other threat actors selling comparable products are taking similar courses of action.

**Oshee RAMP post alluding to insufficient credibility of the alleged vulnerability***Source: ZeroFox Intelligence*

Anongod updated the post on January 8, 2025, stating that the vulnerability had been sold and the thread closed. No further information surrounding the sale price, the buyer, or the platform was offered.

**RAMP post by anongod alleging the sale of the vulnerability***Source: ZeroFox Intelligence*

Given the relatively low asking price, the omission of escrow services, anongod's mixed reputation in the forum, and the lack of any demonstration, proof of concept (PoC), or offer to provide more detail to interested parties, there is a very likely chance that the

alleged zero-day vulnerability does not exist or has been greatly exaggerated. If this is the case, anongod's likely intent was to draw attention to their other services. It is unlikely that the actor would attempt to conduct a scam in a generally restricted and "professionalized" forum such as RAMP.

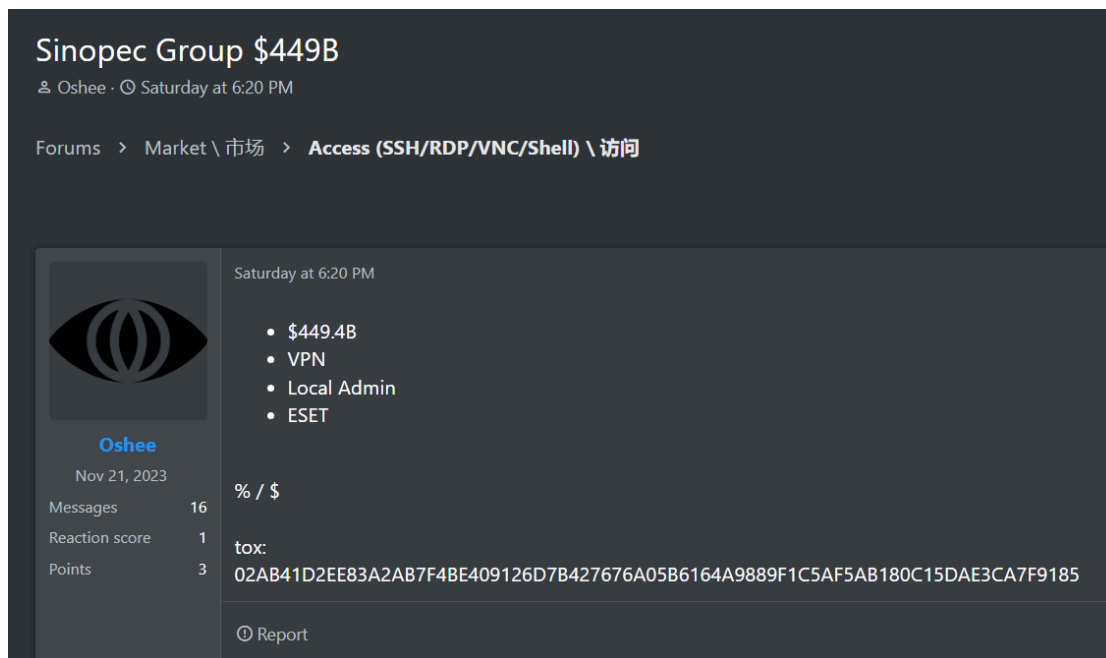
If the alleged zero-day vulnerability is legitimate to some extent, it is likely that anongod either lacks the technical expertise to conduct the necessary exploitive activities themselves or deems a sale a lower-risk option that is still capable of generating significant revenue. Any legitimate vulnerability as advertised would almost certainly attract the attention of a vast range of primarily financially motivated actors interested in diverting digital assets to their own cryptocurrency wallets, stealing PII and PFI, or conducting digital extortion activities.

| Access to Chinese Corporation Advertised in Dark Web Forum

On December 28, 2024, actor Oshee, posted on the dark web platform RAMP advertising alleged virtual private network (VPN) access with local administrative privileges to the corporate networks of Sinopec Group, a China-based energy, utilities, and waste management company. In line with Oshee's previous posts, the asking price was not specified. This is almost certainly indicative of intent to attract maximum interest before selling to the highest bidder.

- Oshee, who has a relatively positive reputation in the forum, has been a member of the RAMP community since approximately November 2023 and engages solely in the brokerage of illicit initial access sales.

Despite listing alleged network access to high-profile organizations, Oshee's observable activity history is very limited. The majority of the actor's sales very likely take place in private channels with established customers, such as digital extortion collectives. It is not clear whether Oshee is directly involved in obtaining illicit network accesses or if they are sold on behalf of a broader collective. The former is more likely, however, as Oshee has previously shared posts related to Metasploit, which is software widely used in penetration testing.

**Oshee RAMP post advertising alleged network access**

Source: ZeroFox Intelligence

Based upon Oshee's previous activity, there is a likely chance that the advertised network access is legitimate. However, given Oshee's lack of detail surrounding sale procedures, use of an escrow, and reputation within the forum, there is also an unlikely chance that the access either does not exist or has been exaggerated.

If the access is legitimate and has the potential to function as advertised, it would almost certainly demand a high sale price. Given the stature of the alleged victim (one of China's largest corporate entities) and the extent and quantity of their potentially lucrative information, the network access is almost certain to appeal to a broad array of threat actors.

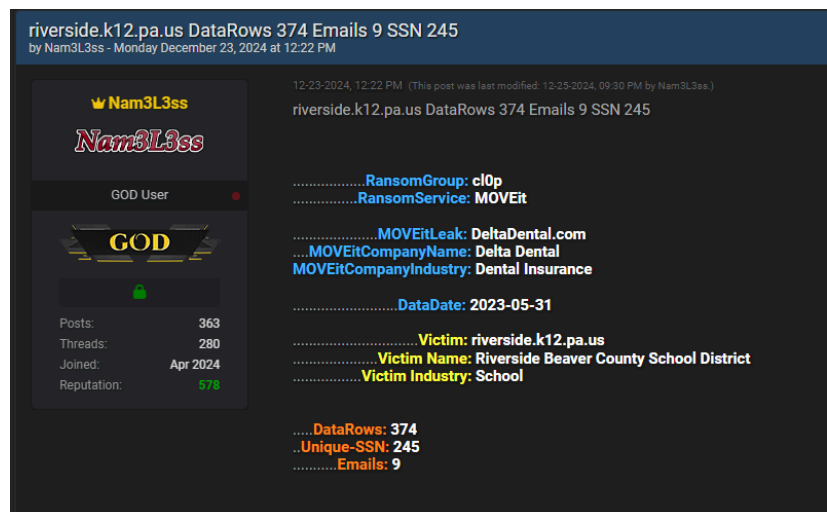
- Financially motivated digital extortion collectives often leverage illicitly obtained network access to deploy ransomware, leading to potential business downtime and both reputational and financial damage. Competitor organizations—both domestically and internationally—also likely view proprietary information and intellectual property as financially lucrative.

- As a state-owned enterprise, Sinopec is very likely an attractive target for both ideologically and politically motivated actors, such as hackers seeking to cause disruption and state intelligence agencies seeking to engage in espionage.

| Leaked Data Allegedly Obtained from C10p Victims Published in Forum

On December 23, 2024, well-regarded actor “Nam3l3ss” disclosed over 200 separate data sets in the deep web hacking forum BreachForums. Nam3l3ss began publishing these to the forum in approximately November 2024, though always in a significantly lower quantity than the most recent incident. According to Nam3l3ss, the affected organizations are victims of the 2023 digital extortion campaign against managed file transfer (MFT) platform MOVEit that was conducted by the threat collective C10p.

- C10p is a ransomware collective that has been associated with numerous high-profile data breaches in recent years. In Q2 2023, the collective leveraged a critical zero-day vulnerability tracked as CVE-2023-34362 to exploit a MOVEit web application. Hundreds of organizations around the globe were subsequently targeted, resulting in one of the most high-profile digital extortion campaigns ever observed.
- Most recently, in December 2024, C10p claimed responsibility for a recent spate of data theft attacks that targeted organizations using Cleo MFT software solutions. Over the following weeks, more than 60 alleged victim organizations were added to the collective’s victim leak site. As of the writing of this report, the full extent of the initial compromise is unclear.

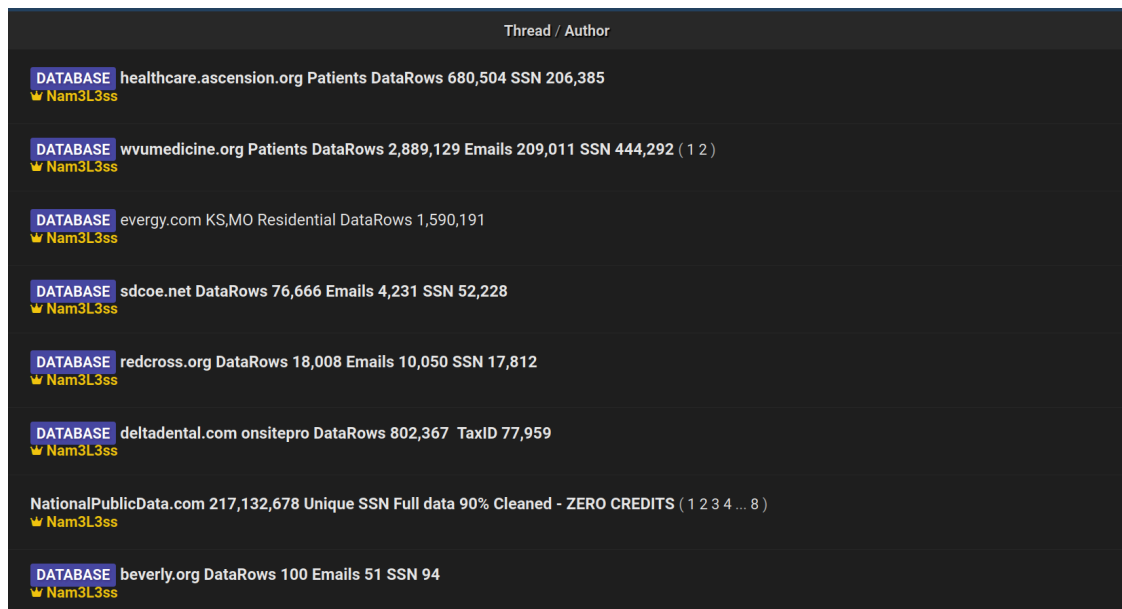
**Most recent databases shared by Nam3L3ss in BreachForums***Source: ZeroFox Intelligence*

Some of the organizations listed by Nam3L3ss have previously been listed on Cl0p's victim leaksite, indicating a very likely chance that they were compromised by the Cl0p collective during the 2023 MOVEit extortion. However, other organizations do not appear to be direct victims of Cl0p's campaign, in which case they are likely either victims of subsequent targeting by other threat collectives (enabled by data stolen from MOVEit) or of unrelated data breaches. It is unlikely Name3L3ss obtained the data from Cl0p's non-public-facing digital infrastructure without Cl0p's consent. When questioned by forum members, Nam3L3ss denied any affiliation with Cl0p.

Nam3L3ss achieved their "GOD" tier status in BreachForums primarily through the republishing of information previously stolen from organizations by ransomware collectives. In the majority of cases, information samples are provided for free, with the full data set being obtainable via credits (BreachForums' internal currency). Such activities are very likely ideologically motivated and intended to boost reputation and enhance collaboration opportunities rather than obtain significant funds.

- In a 2024 interview, Nam3L3ss self-described as an "information watchdog and activist." Outlining their motives, they specified "advocating for proactive measures that can prevent them (data breaches) from occurring in the first

place”, and “empowering them (victims) to demand better protections from those who handle their data).”¹



Most recent databases shared by Nam3L3ss in BreachForums

Source: ZeroFox Intelligence

In the case that the listed organizations are subsequent, indirect victims of CIOp’s 2023 MOVEit compromise, Nam3L3ss’ activities highlight the extent to which associated organizations within supply chains and other partnerships can remain subjected to an enduring threat long after a significant data breach. In the very unlikely case that the published data emanated from non-public-facing CIOp digital infrastructure, there is a roughly even chance that victims of CIOp’s 2023 MOVEit compromise—who successfully met ransom demands—are having their stolen data published nonetheless.

Given its availability and minimal cost, the published data is almost certain to appeal to a wide range of primarily financially motivated actors. While the exact content of the data sets is unclear, they almost certainly contain various types of PII and PFI that can be leveraged to conduct further data breaches, digital extortion, or cyberfraud. The data could also be further parsed and resold.

¹ [hXXps://databreaches\[.\]net/2024/12/23/conversation-with-a-nam3l3ss-watchdog-part-1-background/](https://databreaches[.]net/2024/12/23/conversation-with-a-nam3l3ss-watchdog-part-1-background/)

| 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 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 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%