



| Brief |

The Underground Economist: Volume 4, Issue 5

B-2024-02-29a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Vulnerability Exploitation, Deep and Dark Web,
Ransomware, Social Media

February 29, 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 9:00 AM (EST) on February 29, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 4, Issue 5

LockBit Attempts to Maintain Operations and Credibility

As of February 29, 2024, LockBit administrators remain committed to projecting the appearance of a fully-functioning and resilient ransomware and digital extortion (R&DE) operation. Following Operation Cronos—a coordinated effort by multiple law enforcement (LE) agencies to seize aspects of LockBit's infrastructure—much of LockBit's immediate operational capability was disrupted and its reputation severely damaged in deep and dark web (DDW) communities. Since then, LockBit has taken steps to downplay the disruption and outwardly appear as if it is recovering.

- On February 24, 2024, LockBit posted a lengthy response to the Federal Bureau of Investigation (FBI), pledging to focus more of their attacks against government entities.
- LockBit claimed that the decryption keys seized by LE were that of a small, “unprotected variety”, used mostly by low-level affiliates that make ransom demands of USD 2,000 and below.
- A new .onion address was announced as a data leak site, which lists 10 separate victims as of the writing of this report. It is very likely that at least some of these are associated with attacks that took place prior to February 19, 2024, with others possibly consisting of reposted, old data breaches.



Seizure message displayed on LockBit's leak site following LE disruption

Source: ZeroFox Intelligence

The threat actor alleged that the FBI was able to breach two of their servers, though this was due to “becoming lazy” and not correctly updating them.

- Even if this statement has some element of accuracy, it is almost certainly a part of LockBit's attempt to preserve credibility and ensure that operations can continue despite LE scrutiny.

LockBit announced that, while they will continue to conduct extortion activity, the group will only work with “vetted” affiliates. This condition includes a deposit payment made by affiliates to LockBit, of BTC 2 (approximately USD 62,500).

- This demand is very likely a result of LockBit's damaged stature and credibility, as well as deteriorated mutual trust between ransomware-as-a-service operators and affiliates following several months of heightened LE activity within dark web communities.
- Given the ongoing FBI scrutiny of LockBit and the considerable vetting price, the group is likely to struggle retaining affiliates in the short term.

LockBit very likely remains severely degraded. Attempts to continue operations despite crippling LE activity are not uncommon amongst R&DE collectives and often ultimately result in the cessation of activities. The discord surrounding and within LockBit's operations is likely to incentivize other collectives to expand their operations and compete for former LockBit resources, including affiliates, pentesters, and brokers.

- Currently, LockBit's primary focus appears to be on maintaining credibility and status above all else.
- Claims of a LockBit revival or resumption in operations are likely premature, despite the high chance that alleged new victims will be added to the operation's leak site in the coming weeks.
- While it is likely that LockBit will attempt new attacks in the short term, the threat actor is very unlikely to be able to restore its reputation and the scale of its previous operations.

| Zero-Day Vulnerability in Golang Announced for Sale

On February 16, 2024, well-regarded threat actor "skid_raper" announced in the English-speaking dark web community Omnicore that they are selling a zero-day vulnerability that affects the Go Programming Language's (Golang) networking stack module.

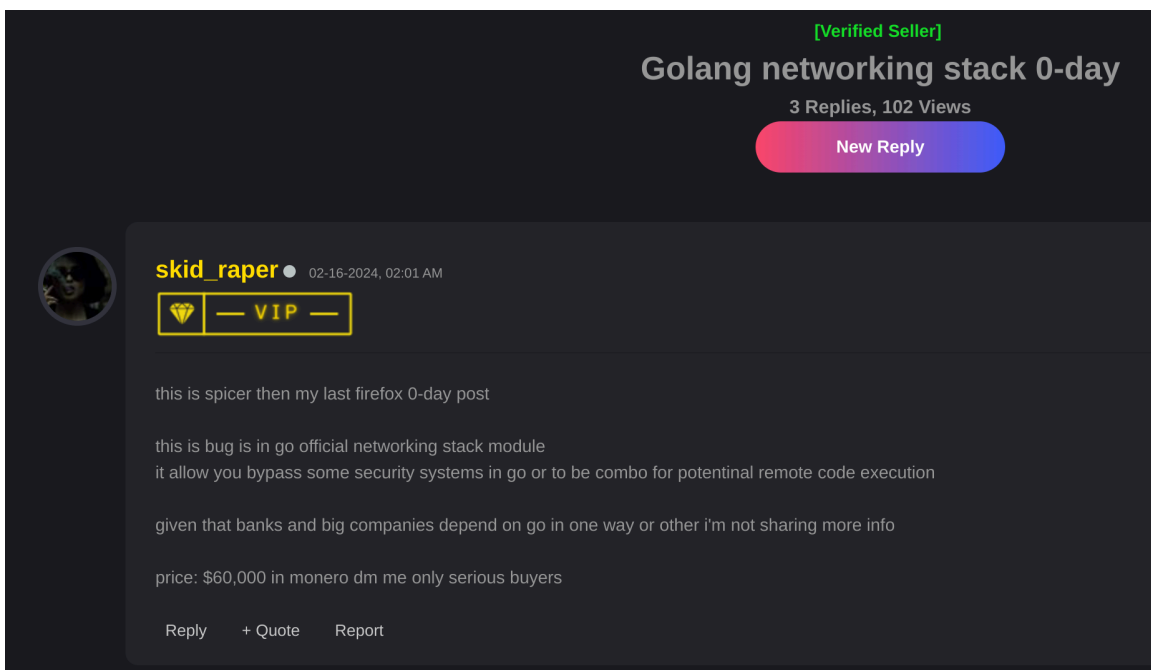
- Golang is an open source programming language that is popular in DevOps and the building of cloud and server-side applications, namely due to its fast execution speed and ease of use.
- The vulnerability is alleged to enable threat actors to bypass security implementations in order to perform remote code execution (RCE) attacks.

Skid_raper claims that "banks" and "big companies" deploy Golang but refused to give additional information so as to not compromise the exploit.

- As one of the most widely-used programming languages, Golang is almost certainly present within the networks of organizations of all sizes in multiple industries across the globe.

The threat actor requested USD 60,000 in XMR (Monero) for the vulnerability, indicating a likely chance that they are situated in the United States or Europe and are conscious of their privacy.

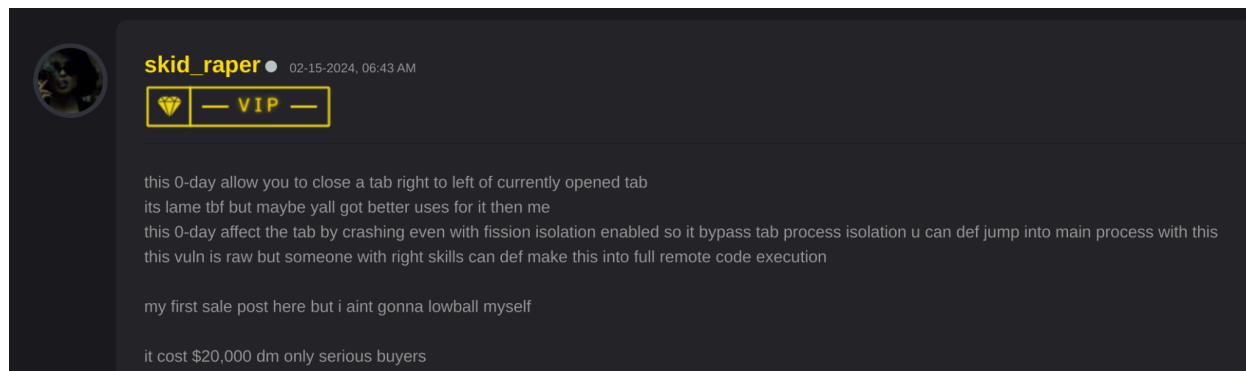
- XMR is growing in popularity amongst threat actors trading illicit services in DDW forums, primarily due to its high fungibility and anonymity.



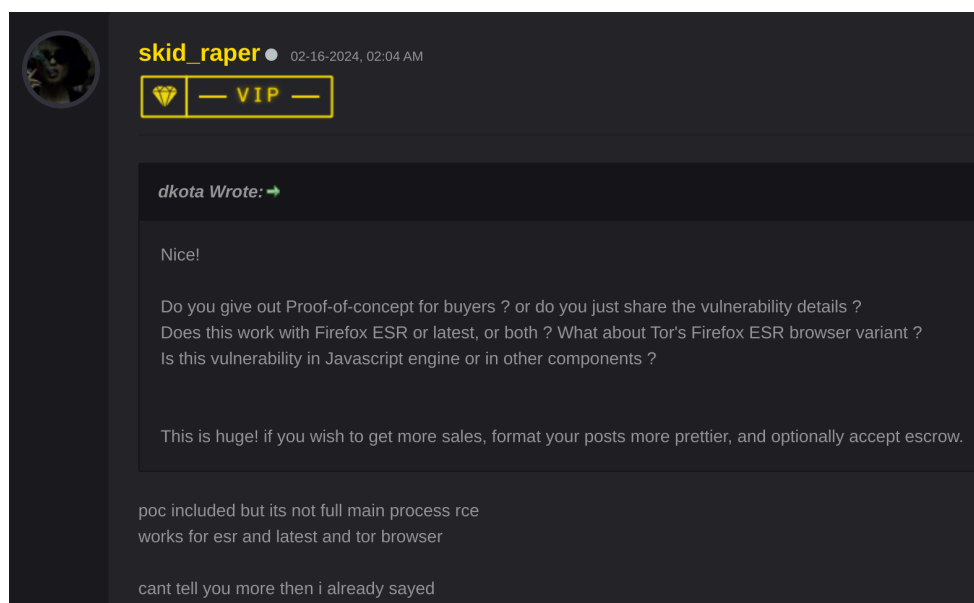
DDW post advertising Golang zero-day vulnerability

Source: ZeroFox Intelligence

One day earlier, on February 15, 2024, skid_raper also posted another alleged zero-day exploit for sale that they claimed would allow the attacker to close tabs from within the victim's FireFox web browser. The threat actor suggests that although "lame", this could be developed into a full remote code execution by a buyer with more technical competency. The asking price for this vulnerability was USD 20,000, also payable in XMR.

**DDW post advertising second Golang zero-day vulnerability***Source: ZeroFox Intelligence*

This post was met with praise from the community admin representative, known as “dkota.” This feedback suggests that even unclear, potentially inapplicable, and technically unfinished exploits are perceived in DDW forums as highly desirable and are able to command high prices.

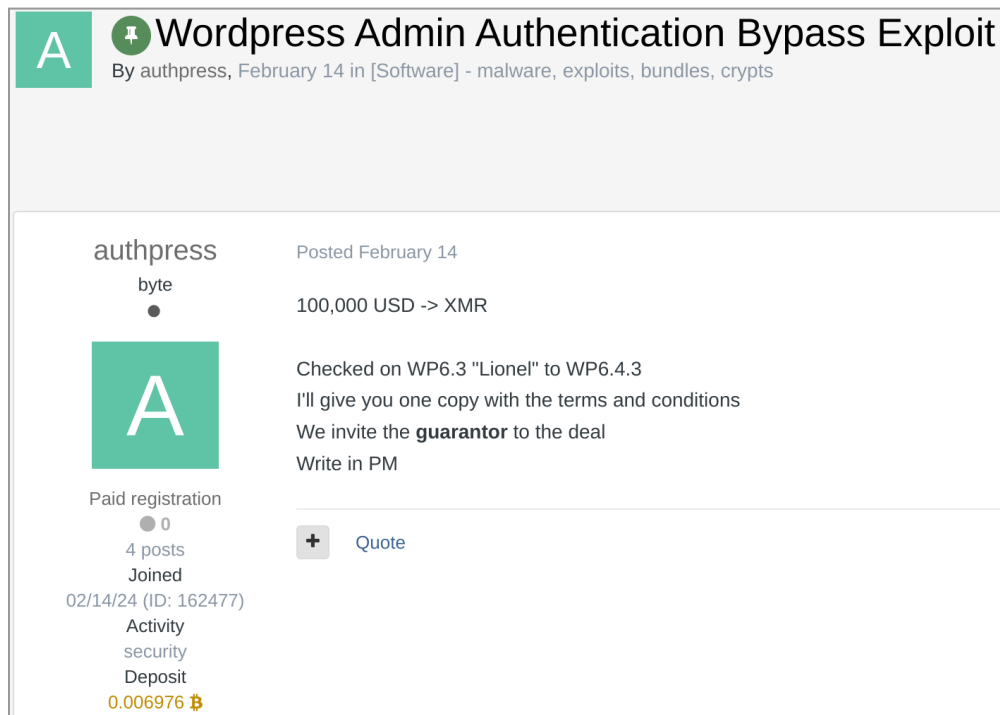
**DDW post highlighting praise from the community admin***Source: ZeroFox Intelligence*

As of the writing of this report, ZeroFox Intelligence cannot confirm whether either of these vulnerabilities have been purchased or leveraged in cyberattacks.

| WordPress Zero-Day Exploit Sold on the Dark Web

On February 14, 2024, untested English-speaking threat actor “authpress” announced the sale of a WordPress administrator authentication bypass zero-day exploit on the predominantly Russian-language dark web forum exploit[.]in. Despite many corporate websites having been built leveraging the tool, WordPress vulnerabilities are very commonly disclosed in open sources, with it widely regarded as one of the more vulnerable website building services.

- Authpress alleged that the exploit would grant buyers access to the administrator panel of WordPress websites.
- The exploit was allegedly tested—and effective—on WordPress versions 6.3 to 6.4.3, although ZeroFox notes the possibility that other versions may be impacted.
- The asking price for the exploit was set at USD 100,000, to be paid in XMR (Monero).



The screenshot shows a forum post on a dark web platform. The post title is "Wordpress Admin Authentication Bypass Exploit". The user "authpress" posted it on February 14. The post content includes the price "100,000 USD -> XMR", the versions "Checked on WP6.3 'Lionel' to WP6.4.3", and the terms "I'll give you one copy with the terms and conditions". It also mentions "We invite the guarantor to the deal" and "Write in PM". The user profile for "authpress" is visible on the left, showing a green avatar with a white 'A', 4 posts, and a balance of 0.006976 XMR.

Wordpress Admin Authentication Bypass Exploit
By authpress, February 14 in [Software] - malware, exploits, bundles, crypts

authpress
byte
●
100,000 USD -> XMR

Posted February 14

Checked on WP6.3 "Lionel" to WP6.4.3
I'll give you one copy with the terms and conditions
We invite the **guarantor** to the deal
Write in PM

Paid registration
● 0
4 posts
Joined
02/14/24 (ID: 162477)
Activity
security
Deposit
0.006976 

+ Quote

Authpress' post selling the WordPress zero-day exploit vulnerability

Source: ZeroFox Intelligence

ZeroFox has moderate confidence in the credibility of the exploit sale. Despite the fact that the actor is untested—and likely registered on exploit[.]in for the single purpose of selling the specific exploit—authpress stated they were open to using escrow and made a Bitcoin deposit, adding further credibility.

- On February 27, 2024, authpress announced that the deal was no longer public and that an escrow account had been created. The deal was likely completed shortly after.
- ZeroFox can neither confirm nor deny the actual price agreed with the buyer, but it is unlikely to be much lower than the original asking price.

| Increased Demand for X Accounts in Dark Web Forum

A public shop that began trading under the name fireaccs[.]biz on the dark web forum xss on January 4, 2024, is gaining momentum amongst threat actors and has exceptionally high numbers of social media accounts associated with various different platforms for sale. The thread is operated by untested threat actor “fireaccs”, who updates the shop on a daily basis to meet customer demands. As a public shop, customers are able to buy goods without negotiating with the vendor.

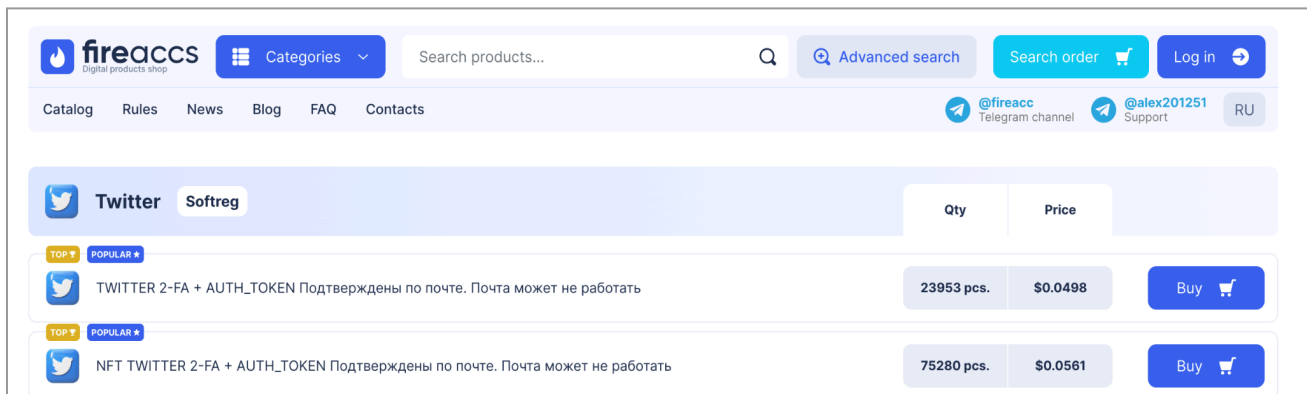
- While such shops are not uncommon in DDW marketplaces, fireaccs is notable primarily for the sale of hundreds of thousands of X accounts (formerly Twitter) in just several weeks—a rate that remains at a steady pace.
- The shop offers the sale of both new “bot” accounts and “aged” accounts, some of which are advertised with followers. Though the latter is more expensive, the former are selling in much higher numbers.

On the store, X accounts are significantly more numerous and in demand compared to other social media. This is very likely indicative of their favor amongst a wide array of threat actors, given the perceived benefits of operating on X versus other platforms. X accounts are almost certainly being increasingly implicated in various types of cybercrime that target individuals and organizations. This is enabled, to some extent, by:

- The allegedly lower levels of active internal regulation of accounts by X in comparison to its predecessor, Twitter. This results in fewer instances of accounts

being suspended or banned for conveying controversial speech or otherwise violating the platform's user guidelines.

- The ability of threat actors to leverage legit as-a-service tools to bypass Know Your Customer (KYC) protocols, which are often associated with the creation of social media accounts. This aids the automated registration of large numbers of accounts for a small price and in a short period of time—accounts which are then used to conduct various nefarious activities without fear of reprisal.
- The inherent anonymity often associated with X in comparison to other social media platforms, where users expect profiles to contain overt links to other legitimate profiles as a display of authenticity. This enables and encourages antisocial behavior.
- The ability for users to engage with audiences far beyond their immediate following. This increases the opportunity available for malicious messages or services to be publicized.
- The payments from the platform to users that are part of the Creator Ads Revenue Sharing Program and receive at least 5 million organic impressions on a post. This encourages the posting of contentious or inflammatory language that may be more likely to be widely shared.



The screenshot shows the Fireaccs website, a digital products shop. The header includes the Fireaccs logo, a search bar, and navigation links. The main content area displays a list of products under the 'Twitter' category. The products are listed in a table with columns for 'Qty' and 'Price'. Each product entry includes a Twitter icon, a 'TOP' badge, and a 'POPULAR' badge. The products are 'TWITTER 2-FA + AUTH_TOKEN' and 'NFT TWITTER 2-FA + AUTH_TOKEN', both described as 'Подтверждены по почте. Почта может не работать'. The prices are \$0.0498 and \$0.0561 respectively. Each entry has a 'Buy' button with a shopping cart icon.

	Qty	Price	
 Twitter Softreg			
 TOP POPULAR TWITTER 2-FA + AUTH_TOKEN Подтверждены по почте. Почта может не работать	23953 pcs.	\$0.0498	Buy 
 TOP POPULAR NFT TWITTER 2-FA + AUTH_TOKEN Подтверждены по почте. Почта может не работать	75280 pcs.	\$0.0561	Buy 

Fireaccs advertising of X accounts

Source: ZeroFox Intelligence

Twitter Aged		Qty	Price	
TOP	POPULAR			
	TWITTER 2010-2023 2-FA + AUTH_TOKEN. Подтверждены по SMS. Подтверждены по почте(почта не работает). Профиль частично заполнен.	2526 pcs.	\$0.6312	Buy 
TOP	POPULAR			
	TWITTER 2022 +AUTH_TOKEN. Подтверждены по почте. Почта в комплекте. Профиль частично заполнен. Токен может не работать.	1746 pcs.	\$0.6312	Buy 
TOP				
	TWITTER 2022 2-FA +AUTH_TOKEN. Подтверждены по почте. Почта в комплекте. Профиль частично заполнен.	9343 pcs.	\$0.6312	Buy 

Fireaccs advertising of “aged” X accounts

Source: ZeroFox Intelligence

Fireaccs sells accounts in both the Russian and English language, indicating a broad marketplace of customers who are almost certainly procuring accounts to conduct a diverse array of malicious activities known to take place on X. These are very likely to include:

- Non-fungible token (NFT) scams, which can include rug-pulling, the use of social engineering techniques to access users’ NFT account details, bidding scams, and the spreading of misinformation intended to artificially inflate NFT prices. Many X accounts sold on fireaccs claim to be optimized toward the use of NFTs and blockchain accounts.
- Crypto scams, which are very likely on an upward trajectory in 2024. Threat actors use bot accounts to manipulate the prices of cryptocurrencies and deliver crypto wallet-draining malware using phishing techniques, such as displaying malicious, redirecting ads to users.
- Verification scams, whereby threat actors masquerading as X staff offer users the platform’s popular blue checkmark in exchange for personal details, money, or both. Only users who have purchased X Premium are eligible to receive the blue tick on their profiles, as well as some notable public figures still associated with the now-legacy Twitter verification program.¹

¹ [hXXps://help.twitter\[.\]com/en/managing-your-account/about-x-verified-accounts](https://help.twitter.com/en/managing-your-account/about-x-verified-accounts)

| Recommendations

- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Implement secure password policies with phishing-resistant multi-factor authentication (MFA), complex passwords, and unique credentials.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).
- 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.
- Develop a comprehensive incident response strategy.
- Configure email servers to block emails with malicious indicators and deploy authentication protocols to prevent spoofed emails.
- Deploy a holistic patch management process and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Proactively monitor for compromised accounts being brokered in deep and dark web forums.
- Configure ongoing monitoring for Compromised Account Credentials.

| 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%