



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

November 11, 2024

Scope Note

ZeroFox's Weekly Intelligence Briefing highlights the major developments and trends across the threat landscape, including digital, cyber, and physical threats. 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 12:00 PM (EST) on November 8, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Weekly Intelligence Brief |

 Cyber and Dark Web Intelligence Key Findings	3
Pro-Palestine Hacktivist Groups Targeting Turkey	3
North Korean Hackers Target macOS Users	4
Custom "Pygmy Goat" Malware Used in Firewall Hack on Government Network	5
 Exploit and Vulnerability Intelligence Key Findings	7
CVE-2024-10443	8
CVE-2024-51567	8
 Ransomware and Breach Intelligence Key Findings	11
This Week's Ransomware Round-Up	11
Seven Days, Multiple Data Breaches: The Growing Threat to Personal and Corporate Data	12
 Physical and Geopolitical Intelligence Key Findings	15
Physical Security Intelligence: Global	15
Physical Security Intelligence: United States	16
 Appendix A: Traffic Light Protocol for Information Dissemination	17
 Appendix B: ZeroFox Intelligence Probability Scale	18

| **Cyber and Dark Web Intelligence** |

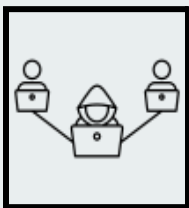
| Cyber and Dark Web Intelligence Key Findings



Pro-Palestine Hacktivist Groups Targeting Turkey

What happened: On November 3 and 4, 2024, ZeroFox observed several pro-Palestine hacktivist groups coordinating cyberattacks targeting Turkish entities. Groups like LulzSec Black, 1915 Team, and Anonymous Syria defaced a Turkish online store, linking their actions to Turkish military operations in Kurdish regions. Another group, Sylhet Gang, targeted the Turkish Armed Forces Foundation website as part of a campaign labeled #op_turkey. Additionally, the groups EvilByte Algeria, Anonymous Syria, PARADOX 17, and LulzSec Muslims pledged to unite with other pro-Arab hacktivist actors. Moroccan Soldiers claimed they breached some databases of a Turkish furniture company, and the Moroccan Black Cyber Army reportedly launched attacks on Turkish media, hospitals, and health centers.

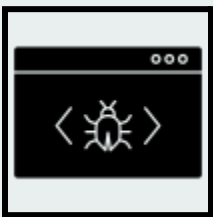
- > **What this means:** A coordinated campaign against Turkish entities by pro-Palestine hacktivist groups is a likely indication of escalation in cyber tactics used in geopolitical conflicts. The Israel-Hamas conflict is cited as an active motivation for politically aligned hacktivists to launch coordinated operations in response to real-world military actions. The explicit targeting of entities in sectors ranging from defense to healthcare to media indicates a willingness among hacktivists to disrupt not only symbolic or government-affiliated websites but also critical infrastructure that affects civilians. Even though most hacktivist attacks do not have long-lasting tangible effects, persistent attacks can cause disruptions in crucial services and networks. Several actors aim to gain global attention and draw traction to their political “rationale.” Additionally, the collaboration between diverse hacktivist factions suggests an evolving strategy wherein cross-border alliances are solidifying, potentially complicating digital defense strategies for nations involved in international conflicts. Such trends in hacktivism suggest that nation-states may increasingly face cyber threats from ideologically driven non-state actors, pushing Turkey and potentially other countries to rethink their cybersecurity strategies across public and private sectors.



North Korean Hackers Target macOS Users

What happened: A recent cyberattack campaign led by the North Korean hacking group BlueNoroff has been targeting macOS users, particularly those in the cryptocurrency and decentralized finance (DeFi) sectors. The attackers are using phishing emails with fraudulent news headlines or stories about cryptocurrency trends to lure victims into downloading malicious applications. These applications, disguised as links to PDF documents on topics like Bitcoin price surges or the future of stablecoins, are designed to infect macOS systems with malware. The campaign, dubbed “Hidden Risk,” relies on these deceptive emails to gain initial access, which is followed by the execution of malicious code on the victim’s device.

- > **What this means:** The significance of this attack lies in its sophisticated tactics and the targeted nature of the phishing campaign. Cryptocurrency businesses and DeFi platforms are prime targets for cybercriminals due to the high value of digital assets and the potential for financial gain. The BlueNoroff group’s ability to use new techniques to bypass macOS security is a reminder of the evolving nature of cyber threats and the importance of staying vigilant against increasingly sophisticated attack strategies. What makes this attack particularly concerning is its ability to evade macOS Ventura’s built-in security features. To maintain persistence on infected systems, the malware abuses the system’s “zshenv” configuration file—a method that allows it to run in the background without triggering the usual notifications that would alert users to suspicious changes in system processes. By bypassing these security measures, the malware remains active and undetected for longer periods, which increases the likelihood of a successful attack and the theft of sensitive data. For macOS users in the cryptocurrency space, this incident highlights the need for heightened awareness and improved security practices to protect against such targeted campaigns.



Custom "Pygmy Goat" Malware Used in Firewall Hack on Government Network

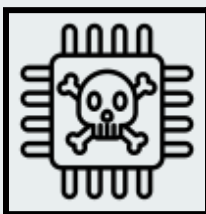
What happened: The UK National Cyber Security Centre (NCSC) has released a [report](#) on a Linux malware strain called Pygmy Goat that is targeting specific network firewall devices via a sophisticated backdoor. The malware, likely linked to a Chinese threat actor, uses deceptive techniques to blend into systems and access devices remotely. Featuring advanced persistence and evasion methods, Pygmy Goat compromises devices by exploiting CVE-2022-1040 and is often deployed on high-level government and technology partner networks. The malware's structure mirrors known nation-state tactics, leveraging complex execution paths to avoid detection and maintain long-term access.

- > **What this means:** The Pygmy Goat malware employs advanced cyber espionage tactics targeting critical infrastructure. By backdooring certain firewall devices, the malware poses a direct threat to organizations relying on network firewall devices for security. Pygmy Goat's use of rootkit techniques, which mimic legitimate file structures, enables it to bypass detection, making it difficult for security teams to identify and remove the infection. The malware's persistence mechanisms allow it to survive system reboots, ensuring continued unauthorized access—a tactic that can lead to prolonged data collection and surveillance. Additionally, Pygmy Goat employs tactics, techniques, and procedures (TTPs) similar to other sophisticated malware attributed to Chinese threat actors, indicating it may be part of a broader espionage campaign focused on gathering intelligence from high-value targets, including government networks. Given its advanced capabilities, this malware strain represents an escalation in the targeting of network devices—crucial points of defense—demonstrating the need for organizations to reinforce their security measures and monitor for suspicious activity within trusted hardware.

| **Exploit and Vulnerability Intelligence** |

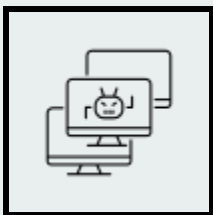
| Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox has observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in technology, software development, industrial control systems (ICS), and government services. [SteelFox](#), a new malicious package, abuses the WinRing0.sys driver vulnerable to [CVE-2020-14979](#) and [CVE-2021-41285](#). Abusing these vulnerabilities allows any threat actor to gain NT AUTHORITY\SYSTEM privileges. Such privileges give the actor unrestricted access to any resource and process. Cybersecurity researchers have discovered six flaws in the Ollama artificial intelligence (AI) framework that actors could exploit for denial-of-service (DoS) attacks, model poisoning, and model theft. Among these, [CVE-2024-39720](#) is an out-of-bounds read [vulnerability](#) in the /api/create endpoint that lets attackers send two HTTP requests with a malformed GGUF file, triggering a segmentation fault and causing a DoS crash. For [CVE-2024-8957](#), PTZOptics PT30X-SDI/NDI before firmware 6.3.40 is vulnerable to an OS command injection issue. The camera does not sufficiently validate the ntp_addr configuration value, which may lead to arbitrary command execution when ntp_client is started. When chained with [CVE-2024-8956](#), a remote and unauthenticated attacker can execute arbitrary OS commands on affected devices. Cybersecurity and Infrastructure Security Agency (CISA) has added these vulnerabilities to its Known Exploits Vulnerabilities (KEV) Catalog based on evidence of active exploitation. [CVE-2024-45240](#) addresses a flaw in the TikTok application before 34.5.5 for Android, which allows the takeover of Lynxview JavaScript interfaces via deeplink traversal (in the application's exposed WebView). On Android 12 and later, this is only exploitable by third-party applications. [CVE-2024-43093](#) can allow threat actors to escalate privileges in the Android Framework component, likely leading to unauthorized access to "Android/data," "Android/obb," and "Android/sandbox" directories and their subdirectories. Google's [Android Security Bulletin](#) addresses several severe vulnerabilities that could lead to local escalation of privilege with no additional execution privileges needed. CVE-2024-43093 and CVE-2024-43047 are two vulnerabilities that may be under limited and targeted exploitation.

**CRITICAL****CVE-2024-10443**

What happened: Synology, a Taiwanese company known for its network attached storage (NAS) devices, recently addressed two critical zero-day vulnerabilities. Discovered by a security researcher, these flaws—collectively tracked as CVE-2024-10443 and named **RISK:STATION**—affect Synology Photos and the BeePhotos feature of Synology's BeeStation software. The vulnerabilities allow remote attackers to execute arbitrary code with root privileges on vulnerable NAS appliances that are exposed to the internet, without needing any user interaction (zero-click).

- **What this means:** The attackers could potentially gain full control of affected devices remotely, which poses a serious security risk to organizations using vulnerable Synology NAS systems—especially those with exposed internet-facing services. Once compromised, attackers could steal sensitive data, deploy ransomware, alter system configurations, or use the device as a foothold for further attacks on internal networks. Immediate patching is critical to prevent potential exploitation.
- **Affected products:**
 - Synology Photos 1.7 for DSM 7.2
 - Synology Photos 1.6 for DSM 7.2
 - BeePhotos for BeeStation OS 1.1
 - BeePhotos for BeeStation OS 1.0

**Critical****CVE-2024-51567**

What happened: A critical vulnerability in CyberPanel with a CVSS score of 10 enables unauthenticated remote attackers to execute root-level commands. Attackers exploited this flaw in October 2024 by bypassing security controls in `/dataBases/upgrademysqlstatus`.

- **What this means:** With CyberPanel widely used for server management, the ability to execute arbitrary commands with this level of access exposes data, disrupts services, and

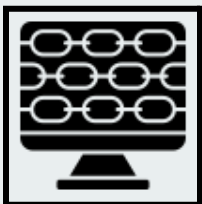
could allow attackers to pivot across interconnected systems. Adding it to CISA's KEV Catalog means that the vulnerability is actively leveraged in the wild.

➤ **Affected products:**

- CyberPanel versions up to 2.3.6
- CyberPanel unpatched version 2.3.7

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

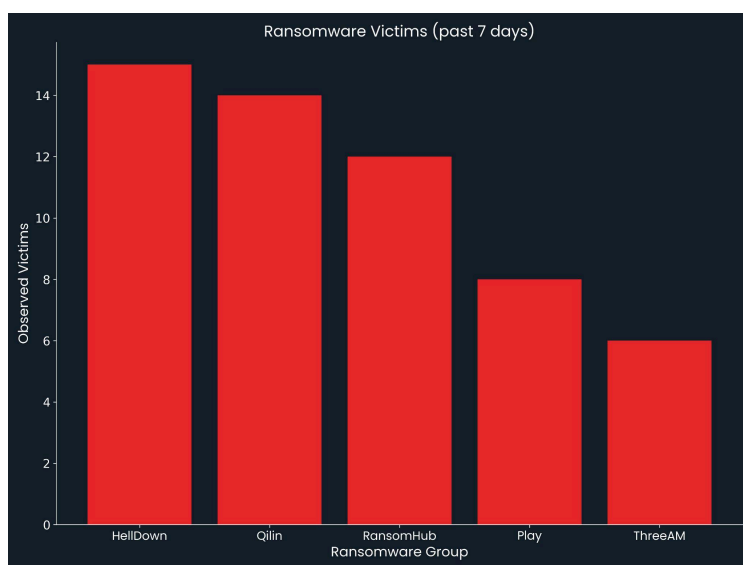


This Week's Ransomware Round-Up

What happened: In the past week, ZeroFox observed more than 100 ransomware attacks, most of which were detected in North America. The most affected sector was manufacturing, while the most active group was the HellDown ransomware group. A July ransomware attack on database systems of the city of Columbus, Ohio, [exposed](#) the personal data of 500,000 individuals. Approximately 3 TB of sensitive information was leaked, including records from the prosecutor's office and crime databases dating back to 2015.

Meanwhile, a new ransomware group, Interlock, has [emerged](#) that is targeting FreeBSD servers globally, including a significant breach in Wayne County, Michigan. Schneider Electric [suffered](#) a cyberattack involving unauthorized access to its project tracking platform in an isolated environment. The attacker, linked to the new Hellcat ransomware variant, listed Schneider on its leak site, demanding USD 150,000 in Monero. It claims to possess over 40GB of data, potentially containing sensitive project and user information. In other news, ransomware attacks have [disrupted](#) multiple U.S. healthcare providers. Memorial Hospital and Manor in Georgia reported a ransomware attack disabling its electronic health records, leading to patient care delays.

- **What this means:** The Columbus data breach puts half a million people at risk of identity theft, financial fraud, and even physical danger. Sensitive details such as home addresses and bank information could be exploited by criminals, exposing crime victims, minors, police officers, and domestic violence survivors to extortion or harassment. For Wayne County and other Interlock targets, the decision to attack FreeBSD servers is especially concerning. FreeBSD is often used in critical infrastructure, meaning these attacks could disrupt essential services or lead to severe operational and financial fallout. The Schneider



Source: ZeroFox Internal Collections

breach could expose sensitive operational data, including project plans and potentially proprietary methodologies, making Schneider Electric vulnerable to intellectual property theft or espionage by competitors. Furthermore, threat actors shifting to Monero is a likely indication of the increasing use of privacy-focused cryptocurrencies in ransomware schemes, challenging tracing and accountability in cybersecurity responses. The ransomware attack on Memorial Hospital and Manor in Georgia forced a shift to paper records, delaying care and increasing the risk of medical errors. For smaller hospitals, such disruptions strain resources and impact patient access, highlighting weaknesses in community healthcare systems.



Seven Days, Multiple Data Breaches: The Growing Threat to Personal and Corporate Data

What happened: A series of cyberattacks have been observed involving large-scale data breaches and targeted operations. The global criminal group EmeraldWhale [exploited](#) misconfigured AWS S3 buckets and Git repositories to steal over 15,000 credentials, cloning more than 10,000 private repositories and using phishing to gather additional access details that were then sold on the dark web. Additionally, a leaked database from a popular football app [containing](#) over 6 million user records, including passwords, is allegedly being sold for USD 9,000, posing a significant risk to its user base—especially in Spain. Meanwhile, Singapore Telecommunications (SingTel) [reported](#) a breach by Chinese state-sponsored hackers (believed to be Volt Typhoon), though no data was compromised and no operations were affected. Another major leak [involved](#) ORBCOMM, a leader in Internet of Things (IoT) and machine-to-machine (M2M) solutions, with over 70TB of sensitive data from its database being offered for sale. The hacker claimed to have accessed all of ORBCOMM's data, including sensitive information and violations. Other incidents include the [leak](#) of 110,000 user records from Sri Lanka's Abans Group on BreachForums and the [exposure](#) of over 2 million student records from Buenos Aires, revealing personal details of students across the region.

- **What this means:** The string of cyberattacks reflects an alarming rise in both the scale and sophistication of cybercrime, with a diverse range of TTPs. The breach of EmeraldWhale shows how attackers can exploit basic misconfigurations, such as exposed AWS S3 buckets and insecure Git repositories, to steal vast amounts of credentials, which are then sold on the dark web. The exposure of such a large volume of user data highlights vulnerabilities in app security, especially in platforms with high user engagement. Users of the app are advised to change their passwords immediately and monitor their accounts

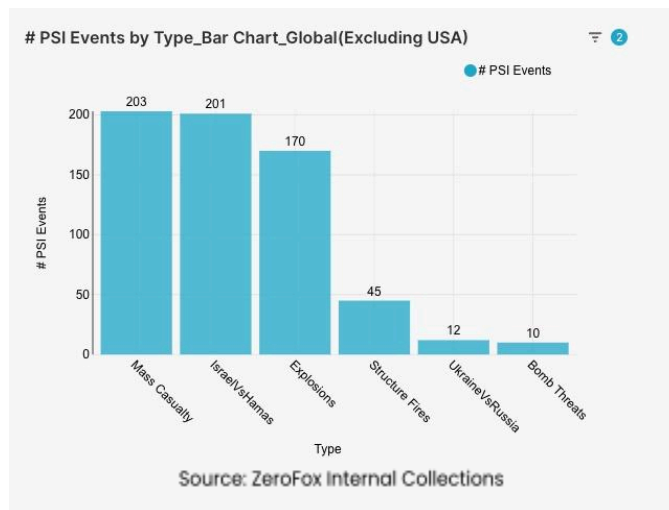
for any unusual activity. The breach at SingTel, despite the lack of negative impacts at the time of writing, demonstrates the ongoing threat of state-sponsored hacking groups targeting critical telecommunications infrastructure. It is likely that the attackers were testing their capabilities for future, more successful attacks against telecommunication entities. The 70TB ORBCOMM data leak signals the growing risk to IoT and M2M operations, which often handle sensitive information at scale. The fact that the stolen data, which reportedly includes sensitive information and evidence of violations, is being offered for sale at USD 30,000 (with a removal price negotiable up to USD 100,000) demonstrates the severe financial and reputational risks associated with such breaches, as well as the potential for further exploitation if the data is not secured. The leak of 110,000 user records from Abans[.]com, which includes a wide range of personal and sensitive information, poses serious risks to the affected individuals. This breach could lead to identity theft, fraud, and targeted phishing attacks, as criminals now have access to highly detailed user profiles. The availability of such a comprehensive data set on the dark web further escalates the potential for abuse and exploitation. Similarly, the Buenos Aires student data leak emphasizes how personal and private data can be easily compromised and exploited, affecting both businesses and individuals. The leak of over 2 million student records exposes sensitive personal information and puts individuals at risk of identity theft, harassment, and targeted scams. These incidents collectively underscore the critical need for organizations to adopt stronger cybersecurity practices, improve data protection, and remain vigilant against increasingly sophisticated threats.

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

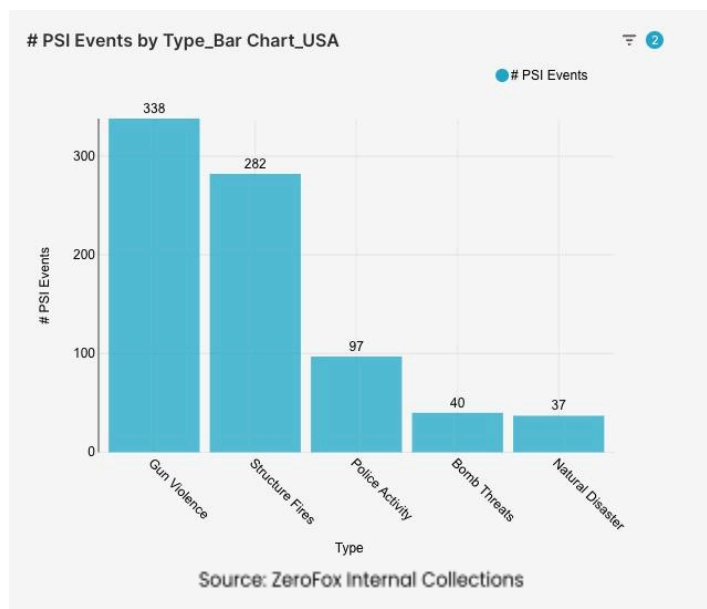
What happened: Excluding the United States, there was an 11.3 percent decrease in the Mass Casualty incidents perpetrated by elements across the globe, with Palestine, Lebanon, and Israel contributing the highest alerts in the category; approximately 65 percent of the alerts were Explosions. General Alerts pertaining to the Israel-Hamas war (including protest, raids, and involvements in the neighboring countries) decreased by 7 percent. Notably, Israel and Palestine accounted for 42 percent of all Explosions. Additionally, events related to the ongoing Russia-Ukraine war decreased by 8 percent. The top three most alerted sub-type were Explosions, Structure Fires, and Gun Violence. This week, Explosions and Gun Violence decreased by 10 percent and 14 percent, respectively, while Structure Fires increased by 87 percent. Global Protest-related incidents declined by 9 percent.



- What this means:** The war between Israel and Hamas continues, as multiple locations around the war zone continue to experience bombings. Eighty-four people were killed in Gaza as a result of Israel bombing a residential structure there. At least [52 people were](#) killed in an attack by Israel in the Baalbek Hermel region of Lebanon. This week, despite the fall in the number of alerts, the number of casualties were higher compared to the previous several weeks. This week also saw a huge [protest](#) spread across Israel against the removal of Defense Minister Yoav Gallant. The ongoing war across Russia and Ukraine saw a decrease in the number of incidents this week. However, cross-border shellings continued, one of which killed [six](#) and injured 16 in Zaporizhzhia. Similarly a police station was targeted in Kharkiv, killing one and injuring [46 others](#). Structure Fires almost doubled this week, with most of the alerts from South American countries.

Physical Security Intelligence: United States

What happened: This past week, the most alerted sub-types were Gun Violence, Structure Fires, and Police Activity. Illinois and Ohio recorded the highest number of incidents in the Gun Violence category with 47 and 26 alerts, respectively, contributing 22 percent of the total alerts this week. Police Activity alerts decreased by 10 percent this week, and Structure Fires decreased by 20 percent. Similar to the Police Activity, School Threats also saw a decrease of 7 percent compared to the previous week. The Shots Fired subtype showed a decrease of 15 percent this week as well. Forty Bomb Threats incidents were reported this week in the United States, which is an increase of 340 percent compared to the nine alerts of the previous week.



- **What this means:** After months of campaigning and primary elections, the U.S. election season is over and Donald Trump will succeed Joe Biden as the 47th President of the United States. On Election Day, a large number of disruptive actors targeted the polling stations with Bomb Threats in multiple states, leading to a halt in the voting process in polling booths. Among the states with Bomb Threats made, Georgia stood apart with the highest number of alerts, leading to polling hours being extended there; most of the alerts were hoaxes, and no incidents of Mass Casualty were reported. These calls of Bomb Threat to the polling stations resulted in a 344 percent increase in the number of alerts compared to last week. In [Pittsburgh](#), Pennsylvania, three people attempted to physically stop voters from casting their ballots, creating a hindrance to the polling process. Furthermore, Gun Violence showed a 15 percent increase in the number of alerts, with Illinois and Ohio being the top two contributors. In [Illinois](#), two people were killed and 16 others were injured in shooting-related incidents over the weekend. Natural Disasters showed an increase of 164 percent in the number of alerts this week, with many localized Tornadoes and Wildfires contributing to the category. The rest of the subtypes showed a decrease this week, including School Threats, which reduced by 7 percent from 113 to 105 alerts.

| 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%