



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

January 13, 2025

Scope Note

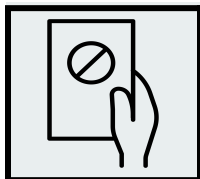
ZeroFox's Weekly Intelligence Briefing highlights the major developments and trends across the threat landscape, including digital, cyber, and physical threats. ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary 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 January 10, 2025**; 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
U.S. Sanctions Chinese Cybersecurity Firm Associated with State-Sponsored Hacks	3
"U.S. Cyber Trust Mark" Label to Certify Cybersecurity of Internet-Connected Devices	3
Marketer Fined for False Claims About Making Websites Adhering to Accessibility Guidelines	4
 Exploit and Vulnerability Intelligence Key Findings	7
CVE-2024-6209	7
CVE-2025-0282	8
 Ransomware and Breach Intelligence Key Findings	10
Ransomware in the Past Week: Attacks, Victims, and Security Moves	10
Breaches and Misconfigured Systems Expose Sensitive 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



U.S. Sanctions Chinese Cybersecurity Firm Associated with State-Sponsored Hacks

What happened: The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned Integrity Technology Group, a Beijing-based cybersecurity firm, for its involvement in cyberattacks against U.S. targets. From the summer of 2022 to fall 2023, the Chinese hacking group Flax Typhoon used Integrity Tech's infrastructure to launch cyber intrusions that compromised U.S. organizations, especially those within critical infrastructure sectors. This partnership allowed Flax Typhoon to send and receive stolen data through Integrity Tech's systems, facilitating its cyber espionage activities.

- **What this means:** The sanctioning of Integrity Tech signals the U.S. government's effort to counteract Chinese cyber operations against U.S. targets, especially those aimed at critical infrastructure. By cutting off the company from the U.S. financial system and imposing penalties, OFAC is seeking to disrupt Flax Typhoon's operational capabilities and deter future cyber intrusions. Flax Typhoon, along with other Chinese state-sponsored actors like Volt Typhoon and Salt Typhoon, has been consistently targeting sensitive data and critical infrastructure, posing a risk to U.S. national security. Through such state-sponsored campaigns, adversarial states are likely to obtain confidential intelligence to gain a strategic upper hand over the targeted country. On September 18, 2024, the Federal Bureau of Investigation (FBI), in collaboration with the Cyber National Mission Force (CNMF), National Security Agency (NSA), and Five Eyes partners, released a joint cybersecurity [advisory](#) detailing the tactics, techniques, and procedures (TTPs) of Flax Typhoon. The advisory also highlighted the involvement of Integrity Tech.



"U.S. Cyber Trust Mark" Label to Certify Cybersecurity of Internet-Connected Devices

What happened: The voluntary cybersecurity labeling program for wireless interconnected smart products administered by the Federal Communications Commission (FCC) will help Americans make more informed decisions about the cybersecurity of products they bring into their homes—from baby monitors to security systems. In December 2024, several major electronics,

appliance and consumer product manufacturers, retailers, and trade associations made voluntary commitments to increase cybersecurity for the products they sell.

- **What this means:** With home security systems being a growing target for cyberattacks, ensuring these products meet stringent cybersecurity standards likely reduces the risk of breaches, unauthorized access, and privacy violations. Threat actors are increasingly targeting home security systems to unlock doors or to tap into insecure home cameras to illicitly record conversations. The U.S. Cyber Trust Mark label program allows electric appliances makers to test products against established cybersecurity criteria from the U.S. National Institute of Standards and Technology via compliance testing by accredited labs and earn the Cyber Trust Mark label. American consumers can also use the label to assess the cybersecurity of products they choose to bring into their homes. By signifying a product's security rating through use of a standardized label, this initiative helps to protect consumers and their data from privacy threats.



Marketer Fined for False Claims About Making Websites Adhering to Accessibility Guidelines

What happened: The Federal Trade Commission (FTC) has ordered a software provider to pay USD 1 million to settle allegations that it misrepresented the ability of its AI-powered web accessibility tool to make any website compliant with the Web Content Accessibility Guidelines (WCAG) for people with disabilities. New York-based accessiBe Inc. and accessiBe Ltd. (accessiBe) market and sell a web accessibility software plug-in called accessWidget that the company has stated can make any website compliant with WCAG, a comprehensive set of technical criteria used to assess website accessibility. The company made the claims on its website, social media, and in articles on third-party websites formatted to look like impartial and objective reviews.

- **What this means:** According to the complaint, accessWidget did not make all user websites WCAG compliant, making accessiBe's claims false, misleading, or unsubstantiated, in violation of the FTC Act. In a number of instances, websites running the accessWidget software contain or have contained barriers that would make it difficult or impossible for persons with disabilities to use the web content for its intended purpose. In addition, the complaint alleges that accessiBe deceptively formatted third-party articles and reviews and failed to disclose its material connections to the supposedly objective reviewers. AccessiBe engaged in a campaign to place these third-party articles that appeared to be reviews from impartial and unbiased authors when, in fact, accessiBe paid

for those reviews and, in some instances, reviewed or edited their content before the reviews were published.

| **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, and government services. [Ivanti](#) released security updates to address vulnerabilities (CVE-2025-0282 and CVE-2025-0283) in Ivanti Connect Secure, Policy Secure, and ZTA Gateways. A cyber threat actor could exploit CVE-2025-0282 to take control of an affected system, while CVE-2025-0283 could allow a local authenticated attacker to escalate privileges. The Cybersecurity and Infrastructure Security Agency ([CISA](#)) has added CVE-2025-0282 to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation. A [vulnerability](#) in the NuPoint Unified Messaging (NPM) component of Mitel MiCollab versions up to 9.8 SP1 FP2 (9.8.1.201) could allow an unauthenticated attacker to perform a path traversal attack due to inadequate input validation. CISA has added this vulnerability to its KEV catalog as well. A cross-site scripting (XSS) vulnerability ([CVE-2025-21616](#)) has been identified in Plane, an open-source project management tool, in versions prior to 0.23. The vulnerability allows authenticated users to upload SVG files containing malicious JavaScript code as profile images, which gets executed in victims' browsers when viewing the profile image. A high-severity [vulnerability](#) has been revealed in ProjectDiscovery's Nuclei, a popular open-source vulnerability scanner. If exploited, this flaw could enable attackers to bypass signature checks and execute malicious code.



CRITICAL

CVE-2024-6209

What happened: In certain versions of WEB Server in ASPECT, this bug enables unauthorized actors to access files on vulnerable systems. It has been assigned the highest CVSS score of 10.0/10.0. CISA has released an [ICS advisory](#) to address this bug, along with multiple other bugs affecting ABB ASPECT-Enterprise, NEXUS, and MATRIX series products.

- **What this means:** The vulnerabilities are caused by configuration issues that allow the attacker to take various unauthorized actions on the target device. If this vulnerability is successfully exploited, it could allow the attacker to take control of the system node. Furthermore, it allows the attacker to insert and run arbitrary code.
- **Affected products:**
 - WEB Server in ASPECT versions 3.08.01 and earlier

**CRITICAL****CVE-2025-0282**

What happened: A stack-based buffer overflow vulnerability has been identified in several Ivanti products, including Ivanti Connect Secure (prior to version 22.7R2.5), Ivanti Policy Secure (prior to version 22.7R1.2), and Ivanti Neurons for ZTA gateways (prior to version 22.7R2.3). This vulnerability occurs when more data than expected is written to a memory buffer, causing the overflow to overwrite adjacent memory. As a result, a remote, unauthenticated attacker can exploit this flaw from anywhere, without needing to be authenticated or inside the network. By carefully crafting input to trigger the overflow, the attacker could potentially execute arbitrary code. CISA has added CVE-2025-0282 to the KEV Catalog.

- **What this means:** This remote code execution (RCE) capability could allow attackers to gain full control over affected systems. If successfully exploited, the attacker could execute malicious code on the vulnerable device, compromising the system's integrity and potentially gaining access to sensitive data or internal networks. Organizations using the affected Ivanti products are at significant risk of compromise. To protect against this vulnerability, Ivanti users are advised to upgrade to the fixed versions of the software to prevent potential attacks.
- **Affected products:**
 - Ivanti Connect Secure prior to version 22.7R2.5
 - Ivanti Policy Secure prior to version 22.7R1.2
 - Ivanti Neurons for ZTA gateways prior to version 22.7R2.3

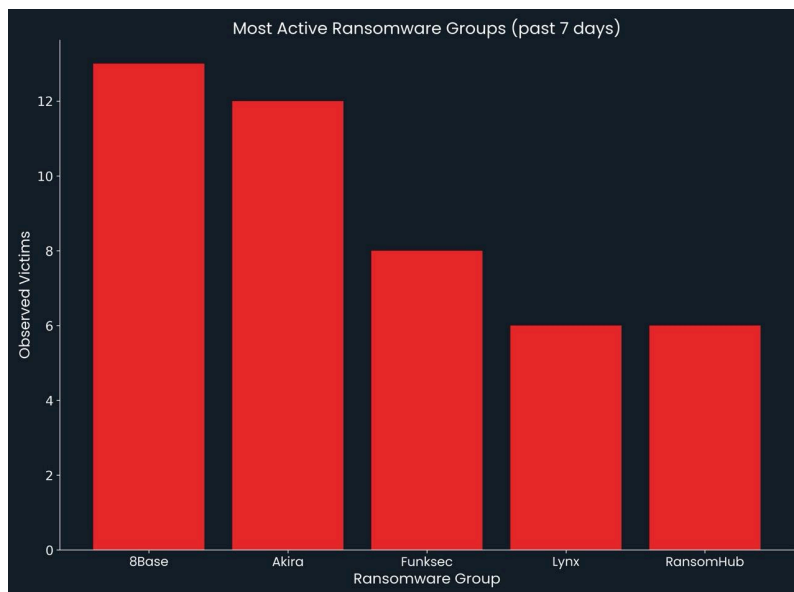
Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings



Ransomware in the Past Week: Attacks, Victims, and Security Moves

What happened: In the past week, ZeroFox observed close to 75 ransomware attacks, most of which were detected in North America. The most affected sectors were manufacturing and professional services, while the most active group was the 8Base ransomware group. In October 2024, Casio, a well-known Japanese electronics manufacturer, was the victim of a [ransomware](#) attack. The attack took place on October 5, 2024, when hackers used phishing tactics to gain access to Casio's network, leading to a significant IT systems outage. On October 10, 2024, the Underground ransomware group claimed responsibility for the attack. The group also threatened to release sensitive internal documents, financial records, project files, and employee personal data unless a ransom was paid. Casio recently confirmed that the personal information of around 8,500 individuals was exposed, including employees, business partners, and a small number of customers. Meanwhile, on December 30, 2024, ZeroFox observed an update on the Space Bears ransomware group's leak site claiming that it had [successfully breached](#) Atos, a company that provides secure communication services to military and intelligence agencies. The ransomware group alleged that they had accessed one of Atos' internal databases and stolen sensitive information. However, Atos recently [denied these claims](#), stating that the breach did not occur within its own systems. Instead, the company clarified that the attack was directed at "external third-party infrastructure" which, although it contained data mentioning Atos, was neither managed nor secured by the company itself. Conceptions Reproductive Associates of Colorado, a fertility clinic, recently confirmed that it had fallen victim to a [ransomware attack](#). The breach, which occurred in mid-April 2024, resulted in unauthorized access to the clinic's network and the theft of personal data affecting up to 80,000



Source: ZeroFox Internal Collections

current and former patients, as well as their partners. The attack was initially detected when disruptions occurred in some of the clinic's legacy computer systems. The investigation revealed that the ransomware group had infiltrated older systems and exfiltrated sensitive patient data. Richmond University Medical Center in Staten Island, New York, has been investigating a [ransomware attack](#) that took place in May 2023. The attack caused significant disruptions to hospital operations, leading to several weeks of service outages. Initially, forensic investigations indicated that the hospital's electronic health record (EHR) systems were not compromised. However, further analysis later revealed that other files within the network were accessed or exfiltrated by the attackers. On December 1, 2024, it was confirmed that at least one of the exposed files contained sensitive personal information (including Social Security numbers, driver's license numbers, dates of birth, financial details, medical records, and health insurance data), potentially affecting more than 670,000 people.

- **What this means:** Phishing, a common entry point for these attacks, was once again exploited to infiltrate Casio's network, underlining the importance of strong cybersecurity measures and employee training to prevent such incidents. The attack also reveals how ransomware groups are increasingly targeting personal and business data, threatening not only operational disruption but also the release of sensitive information. The exposed data, affecting approximately 8,500 individuals, puts both the company and those whose information was compromised at risk of further security breaches or identity theft. While Casio has not specified the full scope of customer data exposed, the presence of such information in the breach raises concerns about customer privacy. While Atos was not directly breached, the attack on external infrastructure shows how organizations can still be vulnerable to data exposure if their third-party partners do not maintain adequate security measures. It also points to the growing trend of threat actors targeting less-secure systems outside the primary target organization to gain access to valuable data. For Conceptions Reproductive Associates, the breach reveals the risks associated with outdated infrastructure, as the attackers were able to exploit weaknesses in older systems to steal valuable personal data and raises concerns about the potential misuse of the stolen data. The exposure of personal and health-related information of up to 80,000 individuals can lead to significant privacy concerns, particularly given the sensitive nature of fertility and reproductive health data. Affected patients and their partners may face increased risks of identity theft or fraud. Although Richmond University Medical Center's EHR systems were initially deemed secure, the exfiltration of other files shows the broader risks posed by cyberattacks that target multiple types of data across an organization's network. With more than 670,000 individuals potentially impacted, the compromised data can lead to increased risks of identity theft, financial fraud, and medical identity theft, especially given the sensitive nature of the information involved.



Breaches and Misconfigured Systems Expose Sensitive Data

What happened: Medusind, a billing provider for healthcare organizations, has sent out notifications to thousands of its customers whose [personal and medical information](#) was impacted in a 2023 breach. A hacker on the dark web forum xss claimed to have stolen data from U.S. [location tracking firm](#) Gravy Analytics. Education technology company PowerSchool experienced a “cybersecurity incident” in which hackers compromised the personal data of [students and teachers](#) in K-12 school districts across the United States. The [Green Bay Packers](#), an American football team, sent out notifications to impacted individuals about a September 2024 data breach targeting its online store. An online gift card store, MyGiftCardSupply, exposed over [600,000](#) ID documents and 200,000 selfies due to an unsecured cloud server with no password. Chinese-state sponsored hackers (APT 41) breached the [Philippine government](#) in 2023–2024, stealing sensitive military data related to the South China Sea. Hacker “Natohub” claims to have stolen 42,000 sensitive files from the United Nations’ aviation agency, the International Civil Aviation Organization ([ICAO](#)). The hacker alleges the data includes sensitive personal information. In Nashville, Tennessee, a flaw in an automated license plate recognition (ALPR) system exposed live vehicle data as part of a broader issue affecting 150 systems and exposing the live streams of [1,000 vehicles](#). Ukrainian hackers disrupted [Russian ISP](#) Nodex, stealing data and wiping servers.

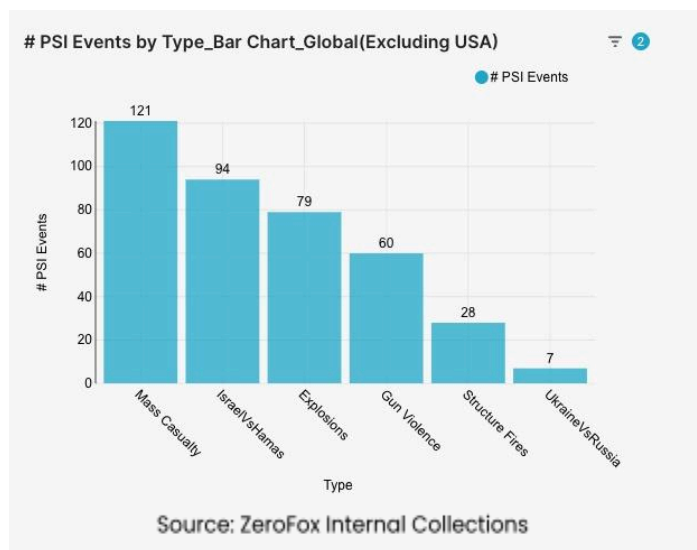
- **What this means:** The data breaches affecting Medusind, Gravy Analytics, and PowerSchool exposed sensitive personal information to threat actors. Impacted individuals will likely face heightened risks of targeted malicious attacks, including spearphishing, blackmail, financial extortion, identity fraud, and even physical security threats. Besides having similar implications, the Green Bay Packers data breach is also likely to attract threat actors looking to take advantage of the public interest in the upcoming Super Bowl 2025 scheduled to begin on February 9. These actors will likely use the exposed details to target affected individuals in scams and phishing attacks. U.S. anti-money laundering laws require companies like MyGiftCardSupply to conduct Know Your Customer checks and collect sensitive documents in order to verify identity. The data breach occurred because of a lack of server security, and the breached data exposed impacted individuals to identity theft, fraud, and account misuse. APT 41 hackers targeted agencies, hospitals, and military-related data about the South China Sea, using stolen credentials to deploy malware and evade detection. As for the ICAO breach, exposed aviation system data is likely to enable identity theft, phishing, and breaches and threaten public safety,

intellectual property, and air travel. Meanwhile, misconfigured ALPR systems exposed personal data like locations and vehicles, risking stalking or impersonation. The Ukrainian Cyber Alliance has been targeting Russia's [critical infrastructure](#), including the Ministry of Defense, the Donetsk People's Republic's Ministry of Coal and Energy, and the Commonwealth of Independent States Institute. Given Russia's large physical size, which likely makes combat efforts difficult, cyber strategies—especially those focused on targeting the country's critical infrastructure—are likely alternatives to destabilize Russia from within and fast-track efforts to end the war.

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

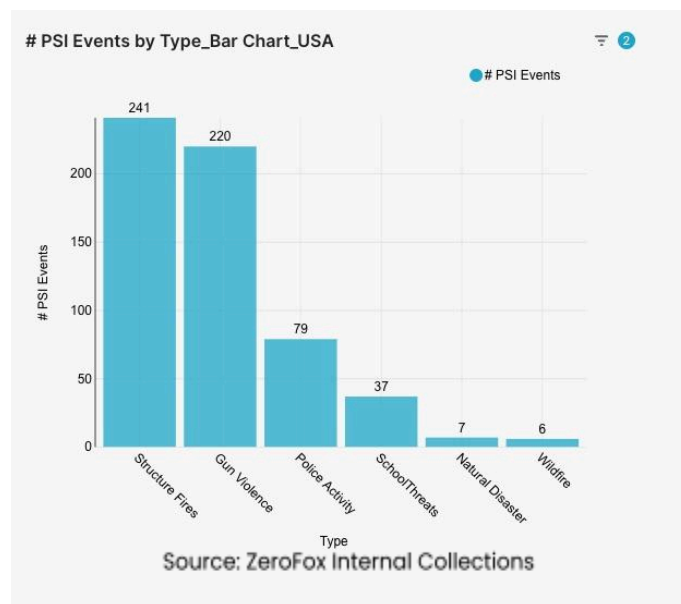


What happened: Excluding the United States, there was a 15 percent increase in mass casualty events this week from the previous week, with the top contributing countries being Palestine, India, and Syria (in that order). Approximately 65 percent of these events were explosions, and the three aforementioned countries accounted for about 45 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict (including protests, raids, and involvement in neighboring countries) increased by 59 percent from the

previous week. Events related to the Russian-Ukraine war increased by 40 percent. The top three most-alerted subtypes were explosions, which saw a 2 percent decrease from the previous week; gun violence, which increased by 18 percent; and structure fires, which decreased by 33 percent. Global protest activity increased by 45 percent, with the United Kingdom reporting the highest number of alerts.

- > **What this means:** Alerts related to the Israel-Hamas conflict saw a significant increase this week, and Palestine had the highest number of mass casualty alerts due to Israel continuing to target various areas of the West Bank. On January 8, 2025, Israeli airstrikes across [Gaza](#) killed 46 people; mediators are pushing forward with efforts to broker an agreement between Israel and Hamas that would see a ceasefire and exchange of Israeli captives held in Gaza for Palestinian prisoners held in Israeli jails, but a conclusion has not been reached yet. In India, which had the second highest number of mass casualty alerts, there were once again several hoax bomb threats at schools; at least 16 schools in [Delhi](#) received bomb threats via emails on Wednesday morning. Mexico had the highest number of gun violence alerts, which did see an increase this week as well. On January 5, 2025, a shooting at a bar in southeastern [Mexico](#) left seven people dead and five wounded, which is the latest in a series of similar attacks in the country.

Physical Security Intelligence: United States



What happened: In the past week, the most-alerted subtypes were structure fires, gun violence, and police activity. Gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim, police activity involves law enforcement presence for generalized threats or for unknown reasons, and structure fires are fires that affect man-made buildings. The top three states that had the most gun violence alerts were California, New York, and Georgia, which together made up 33 percent of this week's nationwide total. Gun violence across the United States overall decreased

by 15 percent from the week prior. Police activity alerts increased by 65 percent, and the top contributing states were California and Texas, as well as the District of Columbia. Structure fires decreased by 5 percent, and the top two states for this subtype were California and New York. Notably, alerts with the SchoolThreats qualifier tag increased from 4 to 37 incidents, which is an 825 percent increase.

- **What this means:** California had the highest number of fires this week, as wildfires are burning out of control in the greater [Los Angeles](#) area and have killed at least five people and forced nearly 180,000 from their homes. At least five fires covering more than 45 square miles are burning, sparked by dry conditions and powerful winds. Police activity increased quite drastically due to both the anniversary of the January 6th riots and the [funeral](#) of the late President Jimmy Carter. Both of these events may explain why the District of Columbia contributed greatly to the overall number of police activity alerts, as several law enforcement agencies and organizations ramped up their security measures over the last several days. Finally, school-related threats saw the largest increase this week, as the holiday season has come to an end and students have returned to their classes. However, [Winter Storm Blair](#), as well as this week's upcoming snowfall across the country, will likely cause many school cancellations and other physical security concerns.

| 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%