ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

November 1, 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 6:00 AM (EDT) on October 30, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Weekly Intelligence Brief

This Week's ZeroFox Intelligence Reports

Monthly Geopolitical Assessment November 2025

The United States is very likely reducing its military footprint in Europe, while it increases troops in Latin America. Military strikes inside Venezuela are very likely for the remainder of 2025. The strikes will very likely be focused on alleged government-sponsored drug-trafficking targets. Given the government's supposed role in drug trafficking, there is a roughly even chance the strikes will be perceived as aiming to topple the Venezuelan government. U.S.-China relations are likely to remain negative despite the relatively peaceful settlement reached in South Korea in late October, with both sides restricting each other's access to advanced technology and critical minerals over the coming years. Full compliance with the Israel-Hamas ceasefire remains unlikely due to opposition to the creation of a Palestinian state and Hamas disarmament.

.

ZEROFOX

Weekly Intelligence Brief

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

Major Telecom Supplier Customer Files Allegedly Accessed by Nation-State Actor

What we know:

- A major U.S. telecom supplier, Ribbon Communications, has disclosed a cyber incident that resulted in unauthorized access to its IT network.
- The company added that the threat actors are reportedly associated with a nation-state actor.
- The intruders reportedly remained hidden for nine months before the company became aware of the breach in early September 2025.

Background:

- The threat actors appear to have accessed customer documents saved outside the main network on two laptops, with three companies reportedly being affected.
- The company also mentioned that there is currently no evidence that the threat actors accessed "material information."
- The company is known for providing software and networking gear to various organizations, including departments in the U.S. government.

What is next:

- The involvement of a nation-state actor likely indicates reconnaissance to map telecom networks of high-value targets.
- Downstream entities related to Ribbon Communications are likely at risk of undetected intrusions.
- The incident highlights ongoing risks to the software supply chain and the need to ensure cybersecurity measures at all stages.

Researchers Find Over 4TB of EY's SQL Database Exposed

What we know:

- An SQL Server backup file with more than 4TB of data from accounting and consulting firm EY was reportedly exposed online, leaking sensitive corporate data.

Background:

- According to researchers, the BAK file contained API keys, authentication and session tokens, service account passwords, and user credentials. The file was exposed via a classic cloud bucket misconfiguration. Responding to the incident, EY said the issue was immediately remediated.

Analyst note:

- The data exposed is unlikely to be of use to threat actors because of the remediation. Without such mitigation efforts, exposure similar to this is likely to enable threat actors to access sensitive data and delete or encrypt the data.

North Korean Hackers Use Fake Job Offers to Steal Sensitive Drone and Aerospace Intelligence

What we know:

- North Korean state hackers, tied to the Lazarus Group, have been impersonating defense recruiters to lure European engineers with fake job opportunities and deploy malware to steal sensitive drone and aerospace intelligence.

Background:

- The campaign, active since March 2025 and tracked as Operation Dream Job, uses trojanized PDF readers and Dynamic Link Library (DLL) sideloading to deploy tools such as ScoringMathTea and MISTPEN. It specifically targets companies in the European defense supply chain involved in unmanned aerial vehicle (UAV) and metal-engineering projects.

Analyst note:

- The intelligence gathered in the operation is likely to be utilized in North Korea's domestic drone production to enhance reconnaissance and strike capabilities. If successful, it could also inspire copycat recruitment-based espionage by other state actors, expanding the threat to global aerospace and defense sectors.

Exploit and Vulnerability Intelligence

Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in technology, software development, and critical infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA) added four vulnerabilities to its known exploited vulnerabilities (KEV) catalog on October 24 and October 28. Additionally, CISA released three Industrial Control Systems (ICS) advisories on October 28. QNAP has warned users that its NetBak PC Agent is vulnerable to a ASP.NET Core flaw (CVE-2025-55315) that could enable attackers to hijack credentials or bypass security controls via HTTP request smuggling; users are urged to update or reinstall the app to ensure the latest ASP.NET Core runtime is installed and prevent potential exploitation. Microsoft has addressed an out-of-band patch for CVE-2025-59287, a critical Remote Code Execution (RCE) vulnerability in Windows Server Update Services (WSUS) that enables unauthenticated attackers to execute code as SYSTEM. Microsoft has released an out-of-band security update addressing the vulnerability. CVE-2025-41068 is a reachable assertion bug in Open5GS that enables an attacker with access to the NRF to send a crafted NF creation (invalid type) and then request its data, triggering a crash in the NRF process. The result is a denial-of-service of the discovery service, disrupting network function discovery and potentially affecting mobile core availability. SuiteCRM v7.14.1 is vulnerable to a reflected Cross-Site Scripting (XSS) flaw (CVE-2025-41384) that allows an attacker to execute arbitrary JavaScript by manipulating the HTTP Referer header. The server tries to block the malicious domain but still enables the JavaScript code to run, potentially enabling session hijacking, phishing, or other client-side attacks.

HIGH

CVE-2025-2783

What happened: This zero-day Chrome vulnerability was exploited in the Operation ForumTroll campaign to deliver spyware from the technology firm Memento Labs. The campaign targeted Russian media, universities, research centers, government, and financial organizations via personalized phishing links to the Primakov Readings forum.

- **What this means:** Exploiting the sandbox escape in Chrome has enabled attackers to execute shellcode, install a persistent loader, and deploy the LeetAgent modular spyware. This vulnerability could enable threat actors to execute arbitrary code or carry out persistent compromise of the host.
- **Affected products:**
  - Mojo in Google Chrome

CRITICAL

CVE-2025-24893

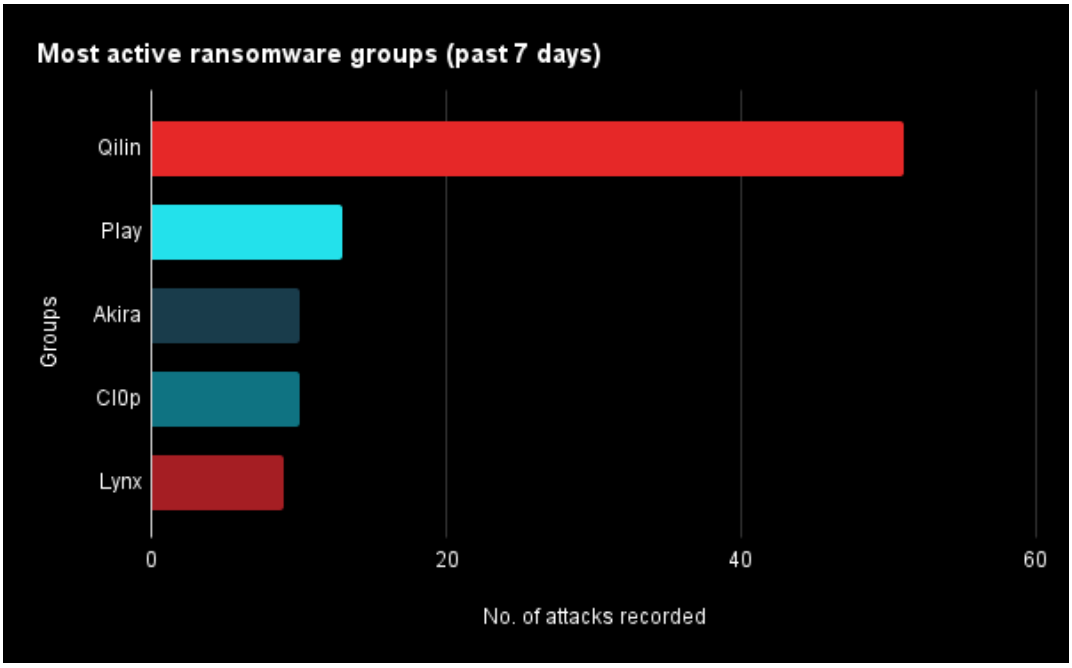
What happened: This RCE vulnerability in the XWiki platform has been exploited in the wild to deploy cryptocurrency miners on vulnerable servers. The flaw arises from improper input sanitization, enabling unauthenticated attackers to execute arbitrary commands with web server privileges.

- **What this means:** Exploitation reportedly occurs in a two-stage workflow. First, a downloader is staged on the server, then the malicious payload is executed after a short delay. Threat actors running commands with web server privileges could access and exfiltrate sensitive information stored on affected systems.
- **Affected products:**
  - XWiki platform

Ransomware and Breach Intelligence

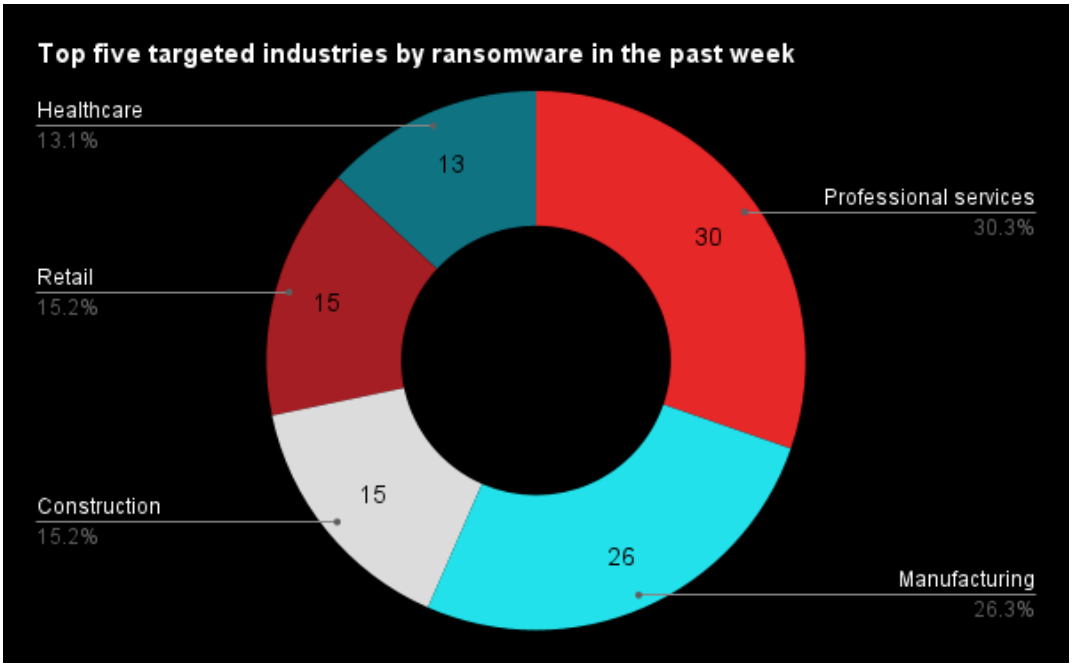
Ransomware and Breach Intelligence Key Findings

Ransomware Activities Throughout the Week



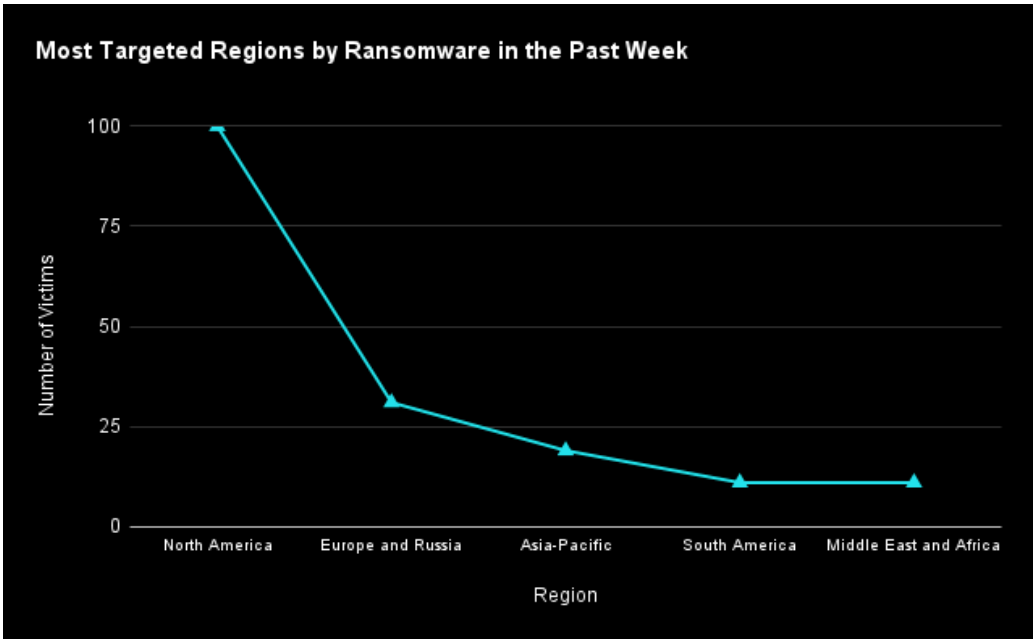
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Qilin, Play, Akira, Cl0p, and Lynx were the most active ransomware groups. ZeroFox observed close to 175 ransomware victims disclosed, most of whom were located in North America. The Qilin ransomware group accounted for the largest number of attacks, followed by Play.



Source: ZeroFox Internal Collections

Industry ransomware trend: In the past week, ZeroFox observed that professional services was the industry most targeted by ransomware attacks, followed by manufacturing.



Source: ZeroFox Internal Collections

Regional ransomware trends: Over the past seven days, ZeroFox observed that North America was the region most targeted by ransomware attacks, followed by Europe and Russia. There were at least 100 ransomware attacks observed in North America, while Europe and Russia accounted for 31, Asia-Pacific (APAC) for 19, South America for 11, and Middle East and Africa for 11.

Recap of major ransomware events observed in the past week: Oregon-based fencing and pet supply company Jewett-Cameron Company has experienced a ransomware incident, wherein attackers encrypted systems and exfiltrated IT and financial data, threatening their release unless a ransom is paid. Qilin ransomware group is reportedly abusing the Windows Subsystem for Linux (WSL) to run Linux-based encryptors directly on Windows systems, which enables them to bypass many traditional Windows security tools. The CVE-2025-61882 zero-day vulnerability in Oracle E-Business Suite (EBS) is being widely exploited by the Cl0p ransomware group to compromise dozens of organisations and industrial giants (such as Schneider Electric), which have reportedly been added to the victim list with alleged data exfiltration. Everest ransomware group claims to have breached Dublin Airport and Air Arabia, stealing passenger and employee data. An individual was extradited from Ireland to the United States for allegedly conspiring to deploy Conti ransomware, targeting networks, extorting victims, and stealing data globally. Akira ransomware group claims to have stolen 23 GB of data from Apache OpenOffice, including employee and financial records, though the claim has not been independently verified. Russian ransomware groups are reportedly increasingly weaponizing the open-source AdaptixC2 framework to facilitate advanced post-exploitation attacks.

Major Data Breaches in the Past Week

Targeted Entity	M-TIBA	Merkle	Conduent Business Solutions
Compromised Entities/victims	4.8 million users	Yet to be disclosed	10.5 million patients
Compromised Data Fields	Full names, national ID numbers, phone contacts, dates of birth, medical diagnoses, and billing records, along with data from approximately 700 health facilities	Information concerning current and former employees, including bank and payroll details, salary, National Insurance number, and personal contact details	Protected Health Information (PHI), including names, dates of birth, Social Security numbers, treatment information, and claims information
Suspected Threat Actor	Kazu	Unknown	Unknown
Country/Region	Kenya	United States	United States
Industry	Healthcare	Media/Entertainment	Healthcare/Professional Services
Possible Repercussions	Phishing or social engineering attacks, identity theft, fraud, operational disruption, extortion, account takeover, supply chain risks, and ransomware	Identity theft, financial fraud, account takeover, business email compromise (BEC), insurance scams, phishing and social engineering attacks, and extortion	Phishing and social engineering attacks, identity theft, fraud, operational disruption, and extortion

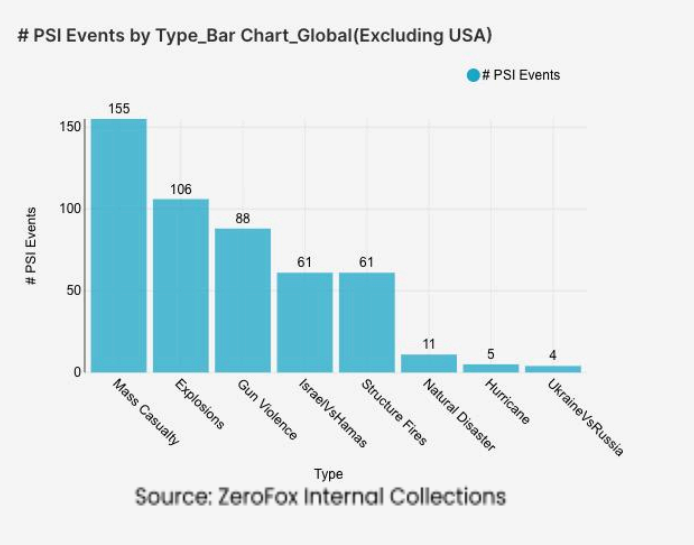
Three major breaches observed in the past week

Other major data breaches observed in the past week: Canadian authorities say that hacktivists have breached multiple critical systems in a water treatment facility, an oil and gas firm, and an agricultural facility, manipulating parameters such as water pressure and tank gauges. LG Uplus has confirmed it reported a suspected data breach to national cyber-watchdog Korea Internet & Security Agency (KISA). Ravin Academy, tied to the Ministry of Intelligence and Security of Iran

(MOIS), has suffered a breach that exposed the data of over 1,000 students and associates. Unigym Gatineau has reported a breach that exposed personal and financial data of about 21,000 members.

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

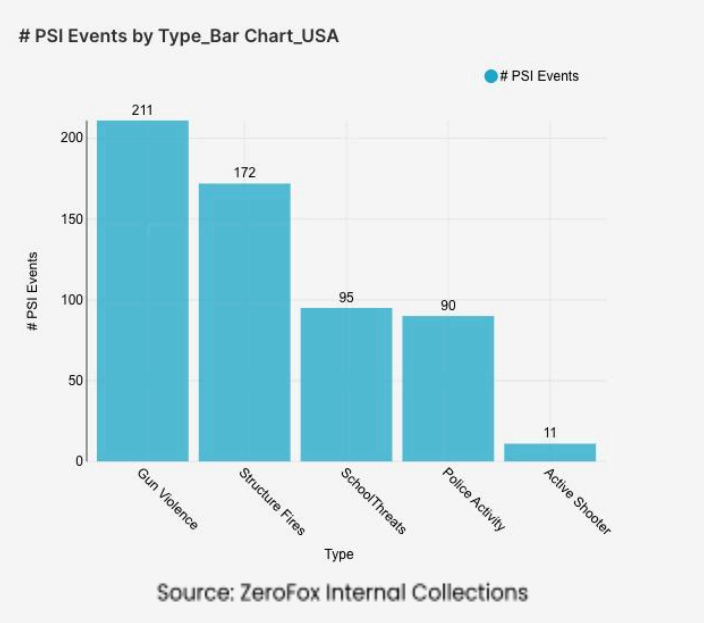


Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 19 percent decrease in mass casualty events this week from the previous week, with the top contributing countries or territories being the Palestinian territories, Pakistan, and India, in that order. Approximately 68 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 39 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict (including raids and attacks) increased by 17 percent from the previous week. Events related to Russia's war in Ukraine decreased by 56 percent. The top three most-alerted subtypes were explosions, which saw a 13 percent decrease from the previous week; gun violence, which increased by 17 percent; and structure fires, which decreased by 12 percent. Notably, natural disaster alerts increased by 57 percent; specifically, hurricane alerts were reported five times more than the week prior.

- **What this means:** The global threat landscape shifted dramatically this week as the nature of specific threats intensified and the world faced a major natural disaster crisis. Specifically, general alerts related to the highly volatile Israel-Hamas conflict saw an increase despite recent truce efforts. For instance, in the last few days of October 2025, Israeli airstrikes in Gaza killed over 100 people after renewed fighting, illustrating the fragility of the October 10 ceasefire. Global natural disaster alerts surged this week, driven by Hurricane Melissa, which made historic landfall in Jamaica on October 28, 2025, as a Category 5 storm before weakening and causing widespread destruction, including at least 23 confirmed deaths in Haiti due to catastrophic flooding. Governments in Jamaica, Cuba, and Haiti have activated nationwide emergency mechanisms, conducted mass evacuations, and opened hundreds of shelters. Escalating violence in specific conflicts underscore ongoing mass casualty threats, while the simultaneous emergence of catastrophic natural disasters highlights a compounding, major shift in the global security focus toward urgent humanitarian crises.

Physical Security Intelligence: United States



Source: ZeroFox Internal Collections

What happened: In the past week, the top three most-alerted incident subtypes in the United States were gun violence, structure fires, 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 two states with the most gun violence alerts were Illinois and California, which together made up 18 percent of this week's nationwide total. Gun violence across the United States overall decreased by 6 percent from the week prior. Police activity alerts increased by 25 percent, and the top contributing states were California and Texas. Structure fires increased by 1 percent, and the top two states for this subtype were New York and California. Notably, active shooter alerts were reported 11 times more than the week prior, and threats related to schools increased by 61 percent.

- **What this means:** The domestic security environment saw a concerning shift toward threats against sensitive locations this past week. There were seven mass shootings within the last seven days, including one in Maxton, North Carolina, that resulted in two dead and 11 injured on October 25. School threats surged this week, exemplified by a mass shooting during a homecoming celebration at Lincoln University, Pennsylvania, on October 25, which left one dead and six injured. This rise in threats targeting educational facilities—a documented trend fueled by social media and alleged mental health concerns—was further compounded by a significant increase in police activity alerts, indicating a sustained high level of generalized law enforcement response to unknown or unconfirmed domestic threats. Finally, the stability of structure fire alerts was challenged by recent major incidents, including an explosion and a subsequent three-alarm fire at a seven-story apartment building in Manhattan, New York, on October 29. Overall, the U.S. physical security landscape, comprising both crime and man-made disasters, is placing significant strain on state law enforcement resources.

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%