



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

April 26, 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 April 24, 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	2
ZeroFox Intelligence Flash Report – BreachForums Allegedly Relunched With New Domain	2
ZeroFox Intelligence Flash Report – Ransomware Incidents Reach Record High in Q1 2025	2
 Cyber and Dark Web Intelligence Key Findings	4
Hotel Staff Tricked by Fake Booking[.]com Emails to Install Malware	4
UK Veteran Retailer M&S Reports Cyber Incident as Customer Complaints Mount	4
North Korean Hackers Are Using Zoom Remote Control Feature to Steal Crypto	5
 Exploit and Vulnerability Intelligence Key Findings	7
CVE-2025-46254	7
CVE-2025-46252	7
 Ransomware and Breach Intelligence Key Findings	10
Ransomware in Focus: Most Active Actors, Affected Industries, and Regions	10
Notable Data Breaches in the Past Week	13
 Physical and Geopolitical Intelligence Key Findings	16
Physical Security Intelligence: Global	16
Physical Security Intelligence: United States	17
 Appendix A: Traffic Light Protocol for Information Dissemination	18
 Appendix B: ZeroFox Intelligence Probability Scale	19

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Flash Report – BreachForums Allegedly Relaunched With New Domain

On April 23, 2025, ZeroFox observed an announcement posted to the allegedly relaunched BreachForums site, breached[.]fi-made by the user “Normal,” stating that the forum is “officially back online.” Administrators of the previous [.]st BreachForums domain appear to have launched the new domain and have publicized efforts to reinstate the existing reputations of previous users. It is likely that BreachForums will have suffered reputational damage as a result of the April 15, 2025 outage. Returning users will very likely approach the [.]fi domain with increased caution, due to circulating speculation on deep and dark (DDW) forums regarding the potential involvement of law enforcement (LE). As of the writing of this report, ZeroFox has observed some users reporting difficulties in registering for accounts, which is likely attributed to initial launch issues. It is very likely that it will take some weeks before a fully functioning user interface is restored.

ZeroFox Intelligence Flash Report – Ransomware Incidents Reach Record High in Q1 2025

ZeroFox observed at least 1,961 separate ransomware and digital extortion (R&DE) incidents during the first three months of 2025, a significantly higher total than that observed during any previous three-month period. North America-based entities were the most targeted by a significant proportion, accounting for approximately 65 percent of incidents—slightly higher than the average of 58 percent observed throughout 2024. Organizations in the manufacturing industry were targeted by more R&DE incidents during Q1 2025 than those in other industries, a trend that has continued since at least 2021. The most active R&DE collectives during the first three months of 2025 were almost certainly Cl0p, RansomHub, Akira, Lynx, and Qilin. This is a notably different picture to that from the final quarter of 2024, with only two out of five of the same collectives appearing in both lists.

| Cyber and Dark Web Intelligence |

| Cyber and Dark Web Intelligence Key Findings



Hotel Staff Tricked by Fake Booking[.]com Emails to Install Malware

What we know:

- A phishing campaign impersonating Booking[.]com is targeting hotel staff to deploy AsyncRAT, a powerful remote access trojan.
- Victims are tricked into running malicious code via clipboard injection after interacting with a fake CAPTCHA page.
- The malware grants attackers remote access to infected systems, including keylogging, data theft, and persistent control.

Background:

- The phishing email pretends to report a guest's forgotten belongings, pressuring hotel managers to click a fake "View guest information" link.
- After CAPTCHA interaction, the site instructs users to run a hidden command via WIN + R, then CTRL + V, and Enter, exploiting clipboard commands.

What is next:

- Victims are likely to face system compromise, data breaches, financial losses, and more targeted attacks.
- Attackers could use AsyncRAT to install more malware, escalate access, or pivot to other systems in the hotel network.
- This tactic can be replicated in similar phishing campaigns targeting other industries or platforms with similar fake login pages



UK Veteran Retailer M&S Reports Cyber Incident as Customer Complaints Mount

What we know:

- UK-based retail giant Marks and Spencer (M&S) has [informed customers](#) of possible delays with their click and collect orders owing to an unspecified "cyber incident."

Background:

- Customers have been raising complaints since at least April 19, 2025, on social media sites about [delayed orders](#), [problems with returns](#) and [contactless payments](#), being [refused purchase using gift cards](#), and more. The cyber incident coincides with the Easter holiday season.

Analyst note:

- There is a roughly even chance that M&S is dealing with a ransomware attack affecting at least one system in its vast network, which could also lead to phishing attacks targeting customers.



North Korean Hackers Are Using Zoom Remote Control Feature to Steal Crypto

What we know:

- North Korean hackers are [reportedly](#) repurposing Zoom's remote-control feature and social-engineering tactics to steal cryptocurrency from targets over video calls in an ongoing campaign named "Elusive Comet."

Background:

- The hackers pose as venture capital (VC) investors, luring victims to give them remote control access while sharing screens on a Zoom call. The hackers have built legitimate-looking online presence, using names such as Aureon Capital and The OnChain Podcast as part of their deception.

Analyst note:

- Misuse of legitimate and innocuous tools like Zoom's remote-control feature is likely to enable even amateur hackers to succeed in malware installation. Cryptocurrency forums are likely to be infiltrated by hackers using elaborate online personas to seem more believable.

| **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 critical infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA) added a total of three vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on [April 17](#). CISA also released a total of 11 industrial control system (ICS) advisories on [April 17](#) and [April 22, 2025](#). Separately, [CVE-2025-42599](#) (a stack-based buffer overflow vulnerability) enables remote attackers to execute arbitrary code or cause a denial-of-service (DoS). ASUS has released a new firmware update addressing [CVE-2024-54085](#), which could enable attackers to bypass authentication remotely. [CVE-2025-46419 is a malformed ESP packet that could](#) enable affected devices, especially those used in critical infrastructure, to reboot, interrupting operations, delaying processes, or shutting down communications. A [segmentation vulnerability](#), CVE-2025-46400, could provide an attacker access to affected devices via local input manipulation. An [authentication bypass flaw](#), CVE-2025-24472, could enable a remote attacker to gain super-admin privileges via crafted CSF proxy requests, using an alternate path.



MEDIUM

CVE-2025-46254

What happened: There is a vulnerability in the Visual Composer Website Builder that enables stored cross-site scripting (XSS).

- **What this means:** Attackers could deploy malware into websites built with Visual Composer, leading to data exfiltration, denial of service, session hijack, and more.
- **Affected products:**
 - Visual Composer Website Builder versions up to and including 45.10.0



HIGH

CVE-2025-46252

What happened: An SQL injection vulnerability exists in the kofimokome Message Filter for Contact Form 7 plugin due to improper neutralization of special elements in SQL commands.

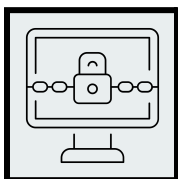
- **What this means:** This flaw enables attackers to inject malicious SQL queries, which could lead to direct access to a website's database and data theft.

➤ **Affected products:**

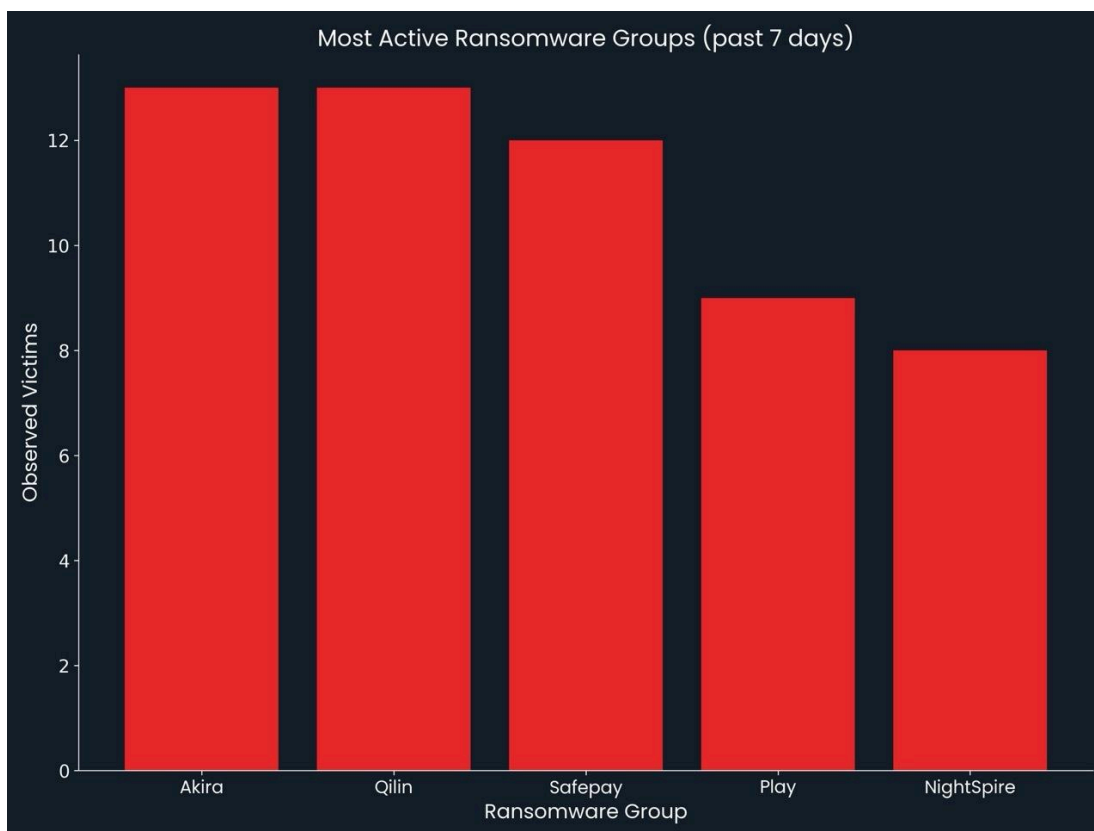
- Kofimokome Message Filter for Contact Form 7 versions up to and including 1.6.3.2

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

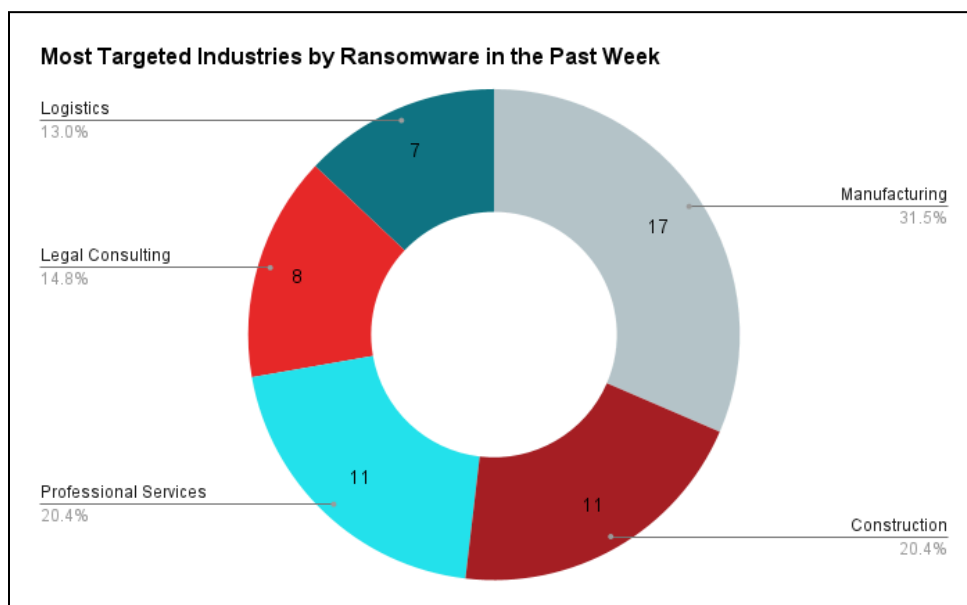


Ransomware in Focus: Most Active Actors, Affected Industries, and Regions



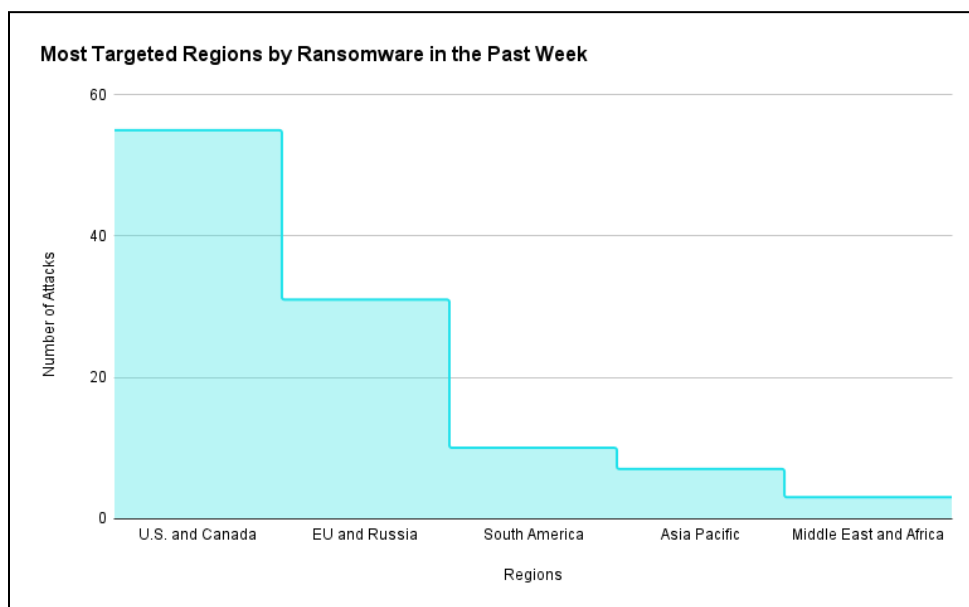
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Akira, Qilin, Safepay, Play, and NightSpire were the most active ransomware groups. ZeroFox observed at least 98 ransomware victims disclosed, most of which were located in North America. Akira and Qilin accounted for the largest number of attacks.



Source: ZeroFox Internal Collections

Industry ransomware trend: This week, manufacturing, construction, professional services, legal consulting, and logistics were the most targeted industries by ransomware attacks. This graph shows the number of ransomware attacks suffered by the industries. Manufacturing, construction, and professional services industries were targeted the most, with 17 and 11 attacks, respectively.



Source: ZeroFox Internal Collections

Regional ransomware trends: In the past seven days, ZeroFox has observed that North America was the most targeted region by ransomware attacks, followed by Europe–Russia.

Recap of major ransomware events observed in the past week: Three American healthcare organizations—DaVita dialysis firm, Bell Ambulance, and Alabama Ophthalmology Associates—[disclosed ransomware attacks this week](#). Baltimore City Public Schools notified thousands of students and staff of a [data breach following a cyberattack](#) allegedly by a ransomware group called Cloak in February. The [Interlock ransomware gang has adopted](#) ClickFix attacks that impersonate IT tools such as CAPTCHA checks to deploy malware in targeted systems. The [FBI's 2024 Internet Crime Report](#) has revealed that ransomware was the most prevalent cyber threat to critical infrastructure in 2024, with a 9% increase in complaints in 2024 over 2023.



Notable Data Breaches in the Past Week

Targeted Entity	<u>The New York Times (NYT)</u>	<u>Blue Shield of California</u>	<u>Emirates NBD</u>
Number of Victims/Amount of Data Stolen	270 GB data	4.7 million members	Yet to be determined
Compromised Data and Infrastructure	NYT source code, approximately 5,000 repositories, and 3.6 million files	Insurance plan name, type, group number, city, ZIP code, gender, family size, Blue Shield-assigned member identifiers for online accounts, medical claim details such as service date, provider, patient name, and financial responsibility, as well as "Find a Doctor" search criteria like location, plan details, provider name, and specialty.	Phone numbers and text messages (SMS) with transaction details
Suspected Threat Actor	CryptoDead	Yet to be determined	Machine1337
Country/Region	United Kingdom	United States	United Arab Emirates
Industry	Retail	Healthcare	Financial services
Possible Repercussions	Unauthorized access, content manipulation, theft of proprietary data, potential reputational/financial/legal consequences, supply chain attacks, and spread mis/disinformation	Phishing and social-engineering attacks, financial fraud, insurance fraud, identity theft, and ransomware	Smishing, account takeover, financial fraud, SIM swapping, and social-engineering attacks

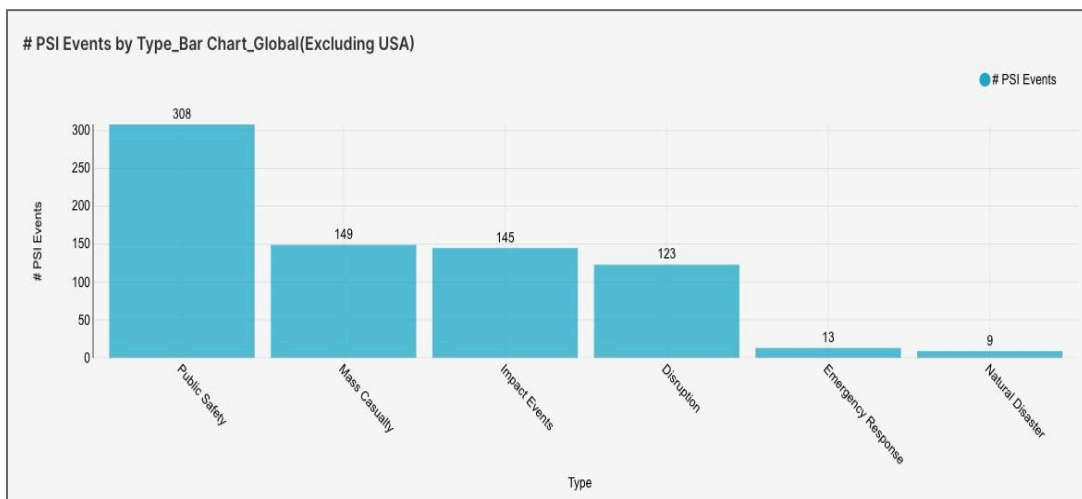
Three major breaches observed in the past week

Other major data breaches observed in the past week: Frederick Health Medical Group, a major healthcare provider in Maryland, experienced a ransomware attack that led to a [data breach affecting nearly one million patients](#). Yale New Haven Health has [informed over 5.5 million individuals](#) that their personal information was likely compromised after unauthorized individuals breached the healthcare system's network last month.

| Physical and Geopolitical Intelligence |

| Physical and Geopolitical Intelligence Key Findings

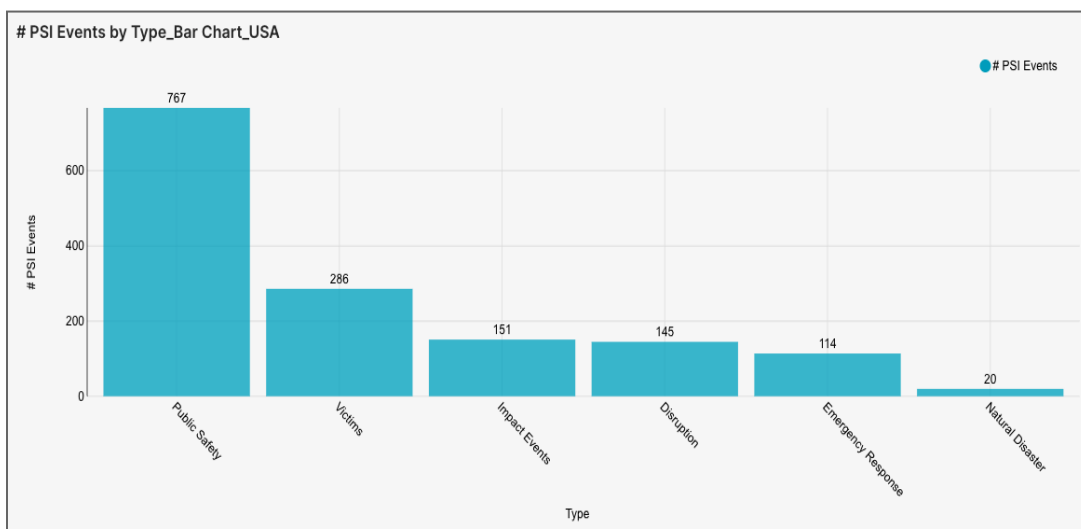
Physical Security Intelligence: Global



Source: ZeroFox Internal Collections

What happened: In the past week, ZeroFox observed at least 308 alerts related to public safety, followed by at least 149 mass casualty alerts globally, barring the United States. On April 24, an overnight [Russian missile and drone attack](#) on four districts of the Ukrainian capital Kyiv reportedly killed at least nine people and injured more than 70, including children. A [conversation between U.S. President Donald Trump and Ukrainian President Volodymyr Zelensky](#) about Russia occupying Crimean territory raised yet another barrier to reaching a permanent ceasefire between Russia and Ukraine. On April 19, 2025, Russian President Vladimir Putin [announced a 30-hour truce](#) to mark the Easter holiday. On April 20, President Zelensky accused Russia of over 2,000 violations across multiple areas of the front. Meanwhile, India has [downgraded its diplomatic ties with Pakistan](#) after a terror attack on tourists at Pahalgam in the Indian state of Jammu and Kashmir claimed at least 26 lives. The attack was [claimed by The Resistance Front](#), linked to Lashkar-e-Taiba, an Islamist group listed as a foreign terrorist organization by the United States. On April 23, Israeli airstrikes across Gaza killed at least 25 people, including children, after the Arab mediators proposed a ceasefire deal. On the same day, Turkey [experiences a series of earthquakes](#), with the biggest tremor hitting 6.2 on the Richter scale. The Turkish authorities reported at least 151 injuries because of people jumping from elevated places to seek safety.

Physical Security Intelligence: United States



Source: ZeroFox Internal Collections

What happened: In the past week, ZeroFox observed at least 767 public safety alerts and at least 20 natural disaster alerts in the United States. Improving weather conditions [helped firefighters fight a wildfire](#) that burned at least 13,250 acres in southern New Jersey since it ignited on April 22, prompting about 5,000 evacuations. As of reporting, no deaths or loss of property was recorded. On April 19, a small [plane crashed into a Nebraska river](#), reportedly killing all three passengers. On April 21, passengers on a Delta Air Lines flight in Florida were forced to evacuate onto the Orlando International Airport tarmac via emergency slides on Monday due to an engine fire. The U.S. Department of Justice has [charged an alleged high-ranking Tren de Aragua gang member](#) with terrorism-related crimes.

| 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%