ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

July 12, 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 July 10, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Weekly Intelligence Brief

ZEROFOX

Weekly Intelligence Brief

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

China-Backed Silk Typhoon Hacker Arrested

What we know:

- An individual allegedly linked to Silk Typhoon, a China-backed hacking group, was arrested in Italy on July 3 and is awaiting extradition to the United States.
- The hacker was arrested in Italy at the behest of the United States, and several documents and devices were seized.
- The person is accused of being involved in computer intrusions between February 2020 and June 2021, including the HAFNIUM campaign, and stealing groundbreaking COVID-19 research.

Background:

- The individual was accused of acting on behalf of China's Ministry of State Security's (MSS) Shanghai State Security Bureau (SSSB) while working for a company named Shanghai Powerock Network Co. Ltd. (Powerock), an "enabling" entity in the cyberespionage campaign.
- As part of the campaign, over 60,000 U.S. entities—including universities—were targeted, of which 12,700 were compromised and sensitive information was stolen.

What is next:

- The member's arrest and seizure of documents and devices are likely to expose operational details behind Salt Typhoon and China's cyberespionage activities, like its tactics, techniques, and procedures (TTPs), future plans, and attack strategies.
- Further law enforcement efforts will likely be able to identify other members of Salt Typhoon, enabling targeted sanctions and arrests in the future.

Global Scam Impersonates News Sites

What we know:

- An ongoing global scam campaign has been using fake news websites disguised as trusted media brands to lure potential online investors into fraudulent investment platforms.

Background:

- At the time of writing, there have been 17,000 fraudulent sites across 50 countries, involving brand impersonation, clickbait advertisements, and other phishing tactics to maximize victim exploitation.

Analyst note:

- These scams are likely to become more sophisticated, using AI-generated content and deepfakes of public figures promoting easy-to-execute investment strategies to lure individuals actively seeking online investment opportunities.

U.S. Sanctions North Korea-Linked Hacker in IT Worker Scam

What we know:

- The United States has sanctioned a member of the North Korean hacking group, Andariel (linked to Pyongyang's Reconnaissance General Bureau), for providing fake and stolen identities to facilitate the IT worker scam targeting U.S. companies.

Background:

- Andariel provided North Korean or contract workers based in China and Russia with false identities to gain remote employment at U.S. companies, to generate revenue for the Pyongyang regime. In certain cases, the workers introduced malware into company networks for further exploitation.

Analyst note:

- The impact of the U.S. sanctions very likely depends on its enforcement in countries like China and Russia. However, the sanctions could help U.S. companies—especially those operating in China—screen applicants more effectively by providing an official record of North Korea-linked actors.

Exploit and Vulnerability Intelligence

Exploit and Vulnerability Intelligence Key Findings

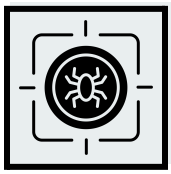
In the past week, ZeroFox observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in technology, software development, and critical infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA) added four new vulnerabilities on July 7 to its Known Exploited Vulnerabilities (KEV) catalog. CISA also issued one industrial control system (ICS) advisory on July 8. This month's Microsoft Patch Tuesday includes security fixes for at least 130 vulnerabilities, including 14 flaws rated as "Critical," 10 remote code execution flaws, one information disclosure bug, and two AMD side-channel vulnerabilities. Adobe has released security updates for 58 vulnerabilities across 13 products, including critical flaws in AEM Forms, ColdFusion, and Adobe Connect. ServiceNow has released fixes for CVE-2025-3648; this vulnerability in the ServiceNow Now Platform enables threat actors to access data through range queries when access control lists (ACLs) are misconfigured. Grafana Labs has patched four critical vulnerabilities for their Grafana Image Renderer plugin and Synthetic Monitoring Agent. The vulnerabilities include two type confusion bugs, an integer overflow bug, and a use-after-free bug. At least nine vulnerabilities, ranging from unauthenticated remote code execution (RCE) to hardcoded passwords, in Ruckus Wireless management products remain unpatched. The bugs enable attackers to fully compromise a network.

CRITICAL

CVE-2025-32463

What happened: This is a privilege escalation bug in the Sudo command-line utility for Linux and Unix-like operating systems.

- **What this means:** The bug enables local users to gain root access from a user-controlled directory. Local attackers are likely to escalate their privileges to root in compromised systems.
- **Affected products:**
  - Sudo before 1.9.17p1



CRITICAL

CVE-2025-30012

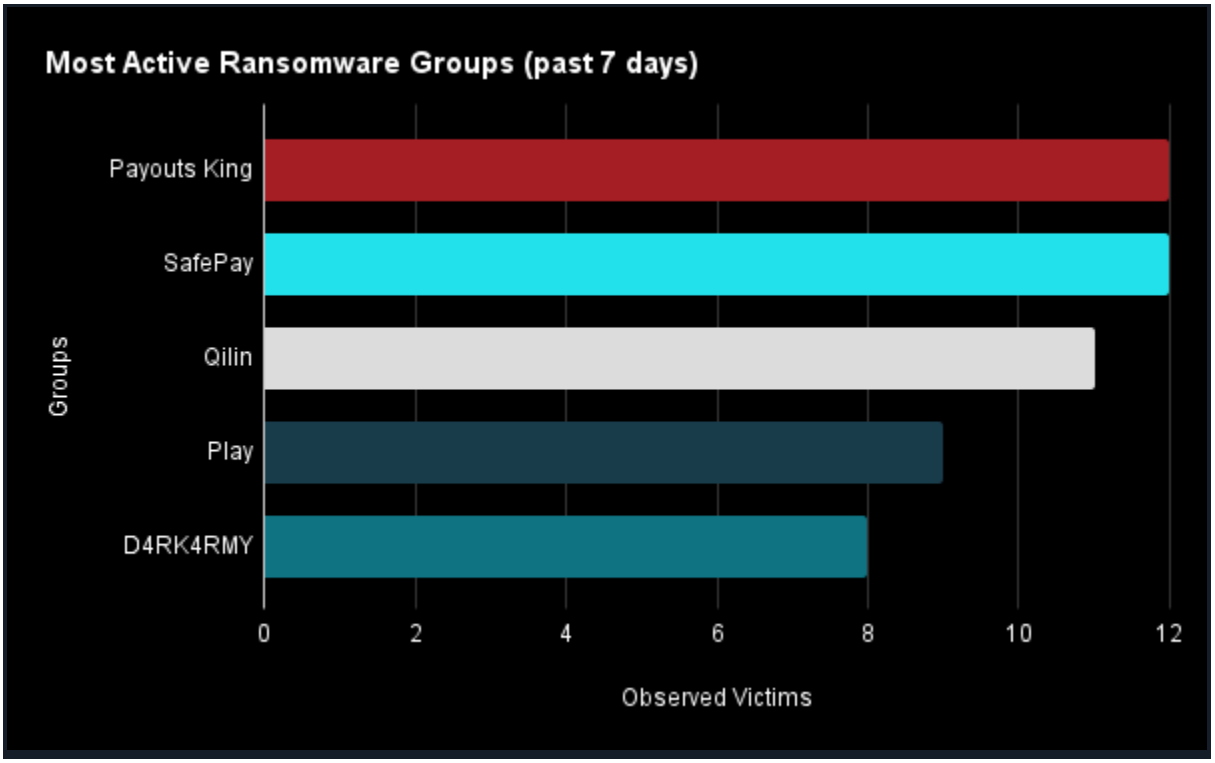
What happened: This vulnerability in SAP Supplier Relationship Management (SRM) affects the Live Auction Cockpit, which uses an outdated Java applet component.

- **What this means:** A threat actor could send a specially crafted request that triggers unsafe deserialization, leading to arbitrary operating system command execution as the SAP Administrator. Exploiting this vulnerability could threaten the confidentiality, integrity, and availability of affected systems.
- **Affected products:**
  - SAP Supplier Relationship Management (Live Auction Cockpit) SRM_SERVER 7.14

Ransomware and Breach Intelligence

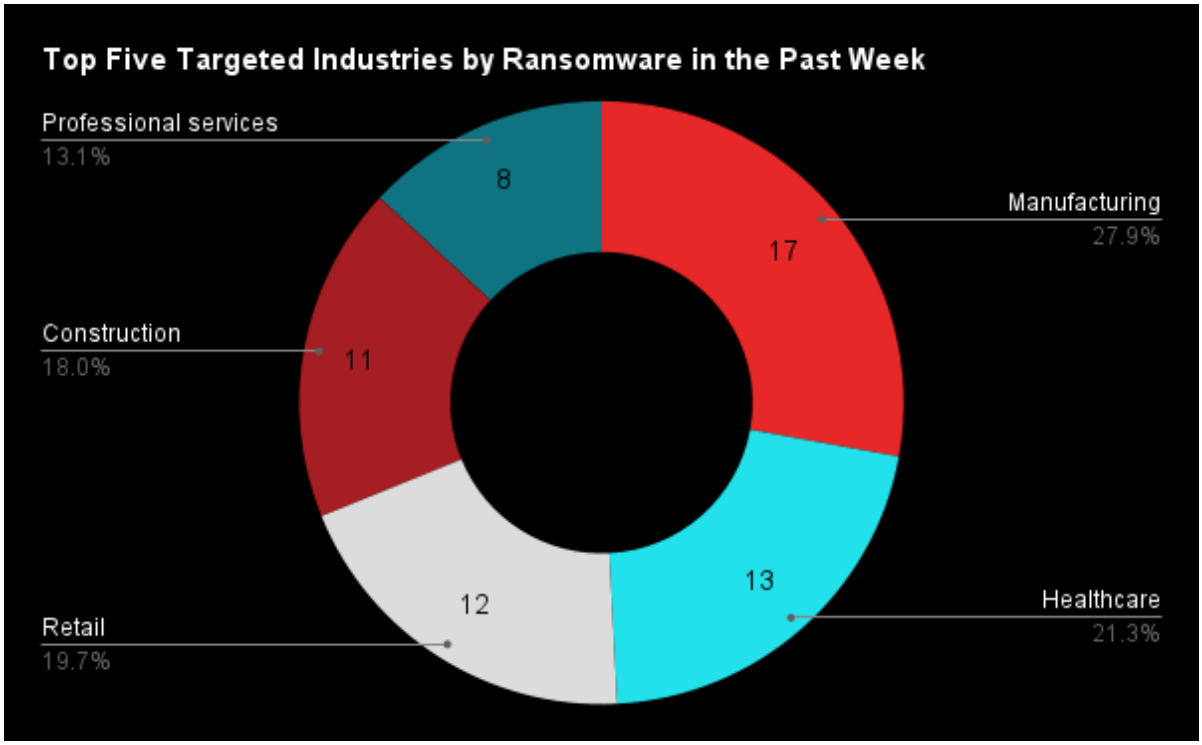
Ransomware and Breach Intelligence Key Findings

Ransomware Roundup for the Past Seven Days



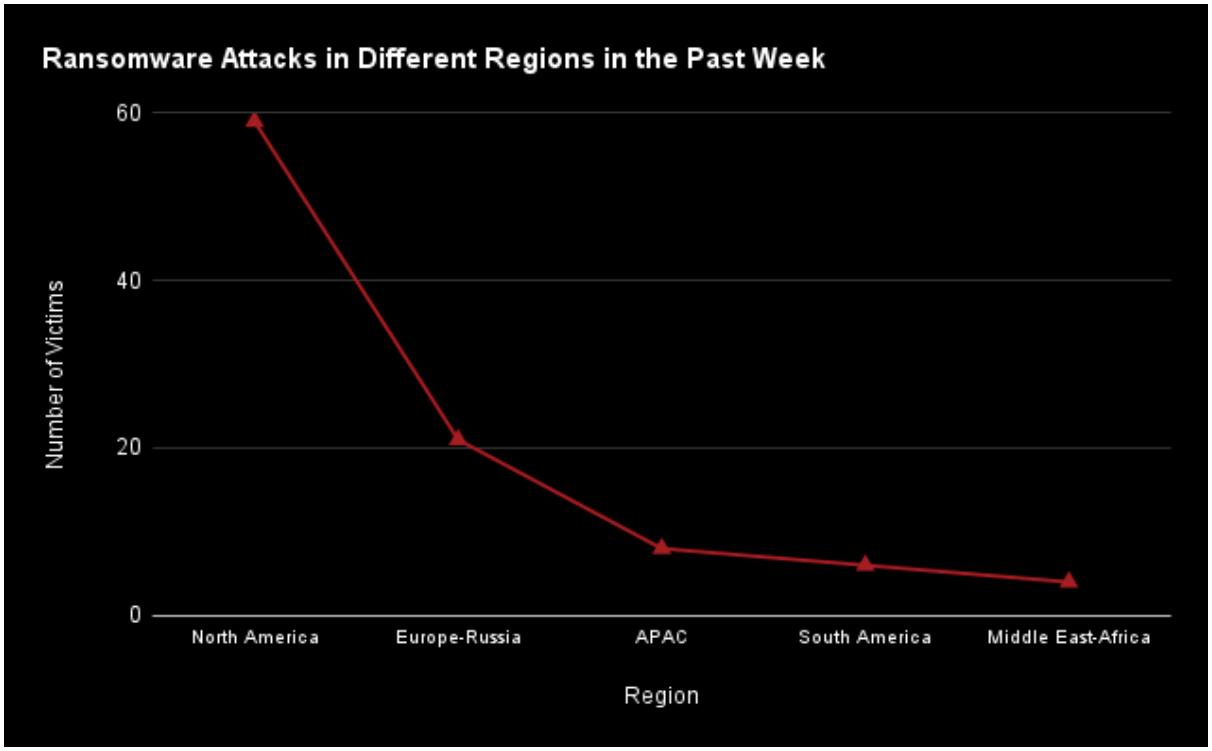
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Payouts King, SafePay, Qilin, Play, and D4RK4RMY were the most active ransomware groups. ZeroFox observed at least 98 ransomware victims disclosed, most of whom were located in North America. The Payouts King and SafePay ransomware groups accounted for the largest number of attacks.



Source: ZeroFox Internal Collections

Industry ransomware trend: In the past week, ZeroFox observed that manufacturing, healthcare, retail, construction, and professional services were the industries most targeted by ransomware attacks. The manufacturing industry was the top target, with 17 attacks identified.



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-Russia. North America saw 59 counts of ransomware attacks, while Europe-Russia accounted for 21, the Asia-Pacific (APAC) for eight, South America for six, and Middle East-Africa for four.

Recap of major ransomware events observed in the past week: An outage at IT giant Ingram Micro has been traced to a SafePay ransomware attack, which forced the company to shut down its internal systems. Meanwhile, two ransomware groups have recently announced their shutdown. The Hunters International ransomware group stated it is officially ceasing operations and will provide free decryptors to allow victims to recover their data without paying a ransom. Additionally, the newly formed SatanLock ransomware group has announced an end to its operations. However, before disappearing, the group stated it plans to release all the data stolen from its victims. A new ransomware group named BERT is using advanced virtualization attack techniques to increase disruption. It can forcibly shut down ESXi virtual machines before encryption, making recovery more difficult for victims. M&S has revealed that its retail network was initially compromised through a "sophisticated impersonation attack," which ultimately resulted in a ransomware incident carried out

by the DragonForce group. Additionally, four individuals have been arrested in the UK under suspicion of cyber offences targeting M&S and others.

Major Data Breaches in the Past Week

Targeted Entity	Louis Vuitton	Bitcoin Depot	Rockerbox
Number of Firms/Victims Affected	Yet to be determined	Around 27,000	245,949 records (286 GB data)
Compromised Data Fields	Some customer data, including contact information	Full name, phone number, driver's license number, address, date of birth, and email address	Personally identifiable information (PII), including full names, dates of birth, Social Security numbers (SSN), and physical addresses
Suspected Threat Actor	Yet to be determined	Yet to be determined	Yet to be determined
Country/Region	South Korea	United States	United States
Industry	Retail	Financial services	Professional services
Possible Repercussions	Phishing and social engineering attacks, malware distribution, impersonation scam, two-factor authentication (2FA) bypass fraud, and ransomware	Phishing and social engineering attacks, financial fraud, identity theft, fraudulent KYC bypass, and doxxing or harassment	Phishing attacks, identity theft, financial fraud, social engineering attacks, and ransomware

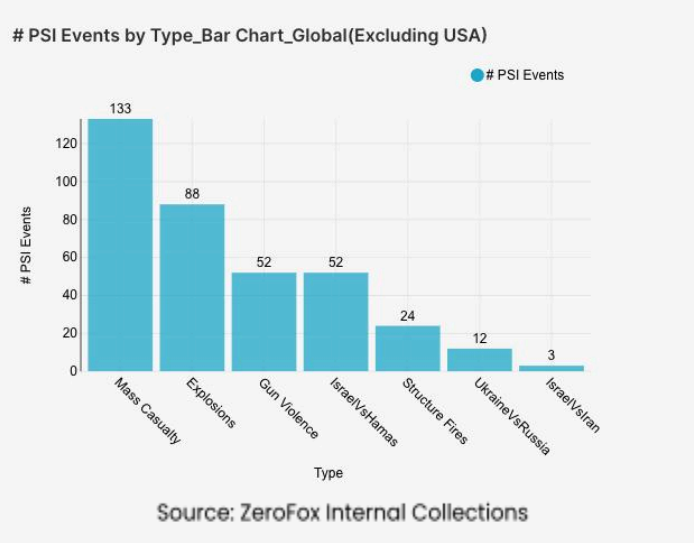
Three major breaches observed in the past week

Other major data breaches observed in the past week: An SQL injection flaw in the Catwatchful stalkerware app exposed a database of 62,000 plaintext emails and passwords linked to compromised devices. Qantas has confirmed that 5.7 million customers were impacted by a recent data breach that exposed their personal information to threat actors. Basic security flaws in

McDonald's recruiting platform, featuring an AI chatbot, has threatened the security of databases containing up to 64 million applicant records with personal details.

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

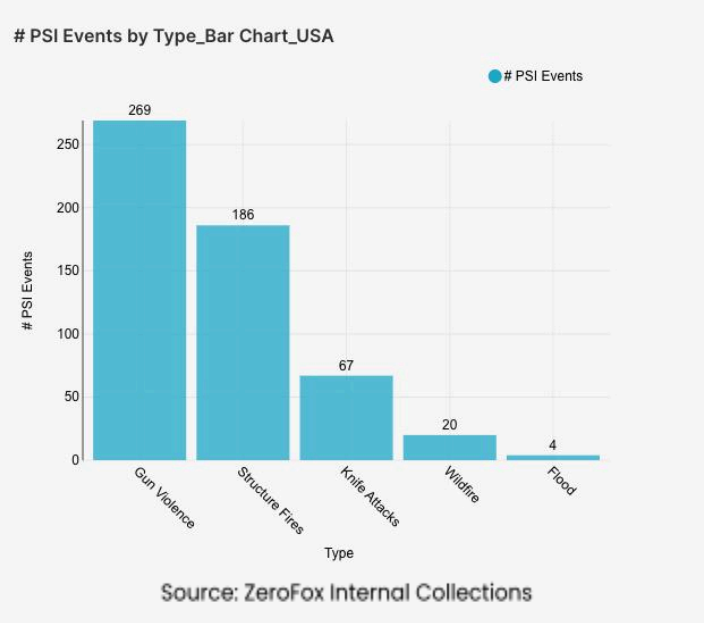


Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 27 percent decrease in mass casualty events this week from the previous week, with the top contributing countries or territories being the Palestinian territories, Ukraine, and Colombia, in that order. Approximately 66 percent of these events were explosions, and the three aforementioned regions accounted for approximately 32 percent of all mass casualty alerts. General alerts related to the Israel-Hamas war (including protests, raids, and attacks) decreased by 34 percent from the previous week, and alerts related to the Israel-Iran war decreased by 63 percent. Events related to Russia's war in Ukraine decreased by 20 percent. The top three most-alerted subtypes were explosions, which saw a 36 percent decrease from the previous week; gun violence, which increased by 6 percent; and structure fires, which decreased by 44 percent.

- **What this means:** This week, explosions, mass casualty alerts, and incidents related to the Israel-Hamas war saw decreases. This trend could be correlated to the recent meeting between U.S. President Donald Trump and Israeli Prime Minister Benjamin Netanyahu, in which the leaders discussed a 60-day ceasefire to return half of all hostages (alive and deceased) to Israel. Despite this decrease in counts, the conflict remains a significant source of mass casualty events, particularly in Gaza where a surge in deaths and injuries has been observed at aid distribution sites. In Ukraine, recorded events related to Russia's war saw a reduction as well. However, Russia launched a record 741 drones and missiles at Ukraine on July 9, targeting Lutsk. Colombia, a top contributor to mass casualty events this week, recently experienced a deadly explosion on July 9 when an ELN bomb exploded, killing a soldier and wounding two others. This incident, following the suspension of peace talks in January due to increased violence, highlights the ongoing threat of terrorism and its impact on regional physical security.

Physical Security Intelligence: United States



Source: ZeroFox Internal Collections

What happened: In the past week, the top three most-alerted incident subtypes were gun violence, structure fires, and knife attacks. Gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim; knife attacks involve confirmed slashings or stabbings; and structure fires are fires that affect man-made buildings. The top two states that had the most gun violence alerts were Pennsylvania and Illinois, which together made up 23 percent of this week's nationwide total. Gun violence across the United States increased by 23 percent from the week prior. Knife attack alerts increased by 22 percent, and the top contributing states were New York and Pennsylvania. Structure fires increased by 27 percent, and the top two states for this subtype were California and New York. Notably, there were four more instances of severe flooding noted this week compared to the week prior.

- **What this means:** In the past week, increased incident data across multiple subtypes in the United States reveals several ongoing threats to physical security. This trend is expected, however, as July 4 remains one of the most violent days of the year. Gun violence alerts saw a notable increase; for instance, Chicago, IL recorded over 40 people shot and seven killed over the Fourth of July weekend, including a mass shooting in River North that killed four and wounded 14 in July. Knife attack alerts also increased this week, with New York City experiencing a July 5 stabbing, in which one person was killed and two people were injured in Queens. Structure fires increased this week as well, primarily in California, which continues to battle significant wildfires such as the Madre Fire in San Luis Obispo County, which has now burned over 80,000 acres. Furthermore, this week's data highlights a concerning rise in natural disasters. Texas, in particular, suffered catastrophic flash floods over the Fourth of July weekend, leading to over 120 confirmed fatalities and more than 173 missing people. This event underscores the devastating physical security threats posed by extreme weather phenomena.

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%