ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

August 23, 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 August 21, 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

ZeroFox Intelligence Flash Report - Workday Breach Linked to Social Engineering Attack

On August 15, 2025, human resource (HR) management organization Workday announced that threat actors were able to access personally identifiable information (PII) from its unnamed third-party customer relationship management (CRM) platform via a social engineering campaign. Although Workday has not yet confirmed this, the attack reportedly resembles the tactics, techniques, and procedures (TTPs) seen in the recent Salesforce attacks first reported in June 2025. There is a roughly even chance that threat actors accessed a Workday-related database containing records of Salesforce CRM users, leading to the targeted campaign. Although the data exposed in this breach may not lend itself directly to extortion—given much of it is publicly accessible—it still presents significant downstream risks.

ZEROFOX
Weekly Intelligence Brief

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

Russian Government Cyber Actors Targeting Networking Devices and Critical Infrastructure

What we know:

- The FBI is warning the public and private sectors and the international community that Russian government-linked threat actors are exploiting outdated Cisco Smart Install (CVE-2018-0171) and Simple Network Management Protocol (SNMP) vulnerabilities.
- Actors linked to the Russian Federal Security Service (FSB) were observed exploiting the flaws to collect thousands of configuration files for networking devices within critical infrastructure sectors in the United States.
- They were also observed modifying some devices to enable unauthorized access to target entities in the United States and globally.

Background:

- The actors aimed to conduct reconnaissance in the victim networks, indicating an interest in industrial control systems (ICS).
- The activity is attributed to FSB's Center 16—also known as Berserk Bear or Dragonfly—which has been active for over a decade.
- The threat actors were also behind the 2015 custom malware "SYNful Knock" deployed against certain Cisco devices.

What is next:

- Unpatched devices can give attackers persistent backdoor access, enabling them to explore and manipulate networks, steal data, deploy malware, and disrupt ICS operations, causing blackouts or supply chain collapses.
- Compromised devices are likely to be exploited during geopolitical flashpoints, with real-world consequences such as the alleged Russian hack of a Norwegian dam that left the floodgates open, which went unnoticed for four hours.

Warlock Ransomware Claims to have Breached Colt Technology Services and Hitachi

What we know:

- Warlock ransomware has claimed UK-based telecom provider Colt Technology Services and Japanese conglomerate Hitachi as its latest victims on its leak site. The ransomware operation is reportedly linked to China-based threat actor “Storm-2603” and has been active since March 2025.

Background:

- Colt’s data is reportedly being sold for USD 200,000 on a Russian-language dark web forum. Hitachi’s data was listed briefly before being taken down, leading to speculations of possible ongoing negotiations.

Analyst note:

- Data leaked from telecom providers is likely to be used in surveillance and further compromise of the network, thereby posing a national security risk. However, Warlock, a newly emerged threat actor, has yet to deliver on its claims and threats.

Stolen PayPal Credentials for Sale on Dark Web Forum

What we know:

- Threat actor "Chucky_BF" is allegedly selling a dataset containing more than 15 million PayPal logins on a cybercrime forum for USD 750.

Background:

- The 1.1 GB dataset, titled “Global PayPal Credential Dump 2025,” reportedly includes emails, plaintext passwords, and URLs. Additionally, Chucky_BF claims that many of the passwords are reused.

Analyst note:

- If the leak is real, it likely exposes users to social engineering, impersonation, and financial fraud. Buyers could also exploit the stolen data for credential stuffing and brute force attacks against PayPal and other accounts.

Exploit and Vulnerability Intelligence

Exploit and Vulnerability Intelligence Key Findings

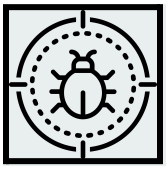
In the past week, ZeroFox observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in technology, software development, and critical infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA) added two vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on August 18 and August 21. CISA also released seven ICS advisories on August 19 and August 21. A new backdoor dubbed PipeMagic has been discovered exploiting a zero-day in Windows CLFS (CVE-2025-29824). Masquerading as a legitimate open-source ChatGPT desktop app, it secretly installs a framework designed to enable ransomware operations. Apple has issued an emergency patch for a zero-day vulnerability (CVE-2025-43300) detected in the Image I/O framework. CVE-2025-8671 enables attackers to bypass the HTTP/2 Rapid Reset fix by exploiting invalid control messages to overwhelm servers. CVE-2025-20265 is a flaw in Cisco Secure Firewall Management Center's RADIUS subsystem that enables unauthenticated remote attackers to inject arbitrary shell commands. Plex has urged users running specific versions of its media servers to update immediately due to a recently patched vulnerability. A recently patched flaw in Ollama enabled malicious websites to launch drive-by attacks, allowing attackers to spy on local chats and, in severe cases, control or replace the AI models used by a victim's app. CVE-2025-9179 enables attackers to trigger memory corruption in the GMP process that handles encrypted media.

CRITICAL

CVE-2025-31324 and CVE-2025-42999

What happened: A new exploit combining two critical flaws (CVE-2025-31324 & CVE-2025-42999) in SAP NetWeaver's Visual Composer server has surfaced. Actively exploited as zero-days since March 2025, the vulnerabilities enable attackers to bypass authentication and gain remote code execution (RCE). Multiple ransomware groups and China-linked espionage actors have already weaponized the vulnerabilities.

- **What this means:** This exploit gives unauthenticated attackers full control of vulnerable SAP systems, enabling arbitrary file uploads, command execution, and manipulation of business processes. If left unpatched, it could lead to large-scale ransomware incidents, sensitive data theft, and operational disruption. For critical infrastructure operators, the risk could extend to espionage, sabotage, and cascading business impacts.
- **Affected products:**
  - SAP NetWeaver's Visual Composer development server



CRITICAL

CVE-2023-46604

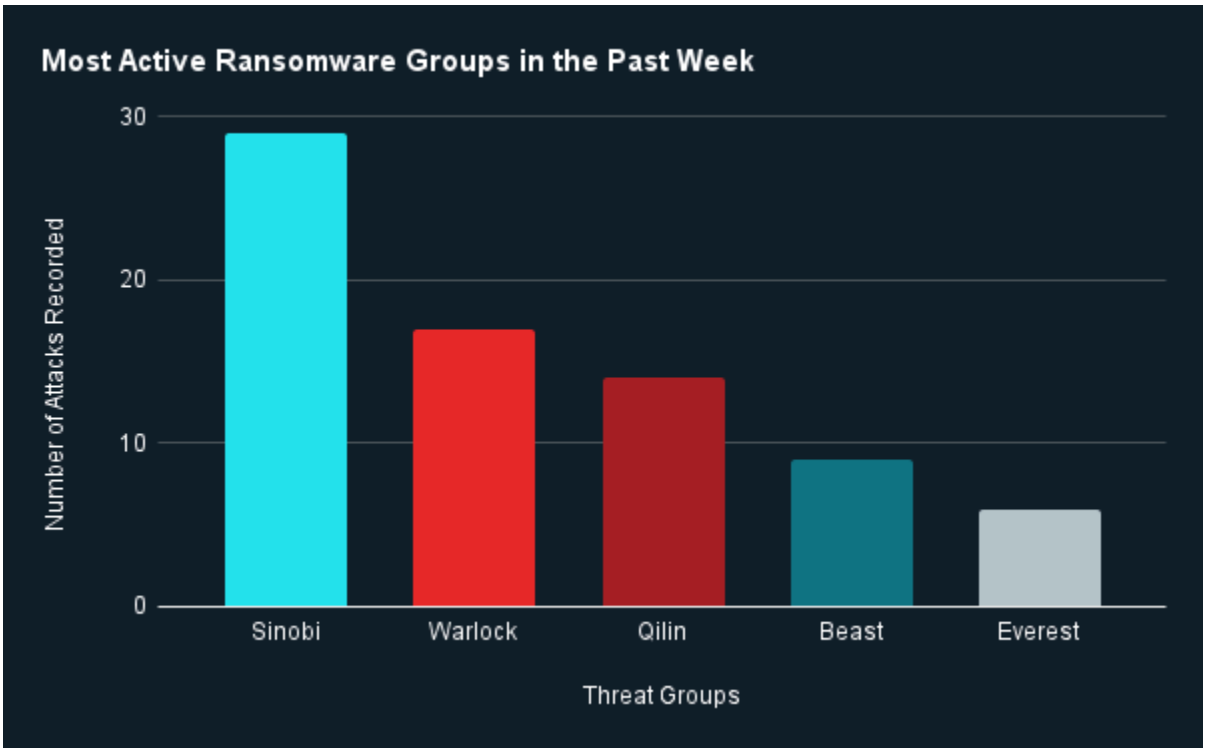
What happened: Threat actors are exploiting a two-year-old critical RCE flaw in Apache ActiveMQ—patched in October 2023—to compromise Linux cloud systems. Using this access, the attackers modify sshd configurations to enable root login and deploy a new downloader called DripDropper. The same flaw has also been leveraged to deliver ransomware, rootkits, botnet malware, and web shells.

- **What this means:** Even long-patched vulnerabilities remain high-value targets when systems are left unpatched. By enabling persistent root access, attackers can maintain long-term control, deploy additional malware, and expand across environments. Potential impacts include ransomware attacks, data theft, system hijacking, and large-scale disruption in cloud infrastructure.
- **Affected products:**
  - Apache ActiveMQ

Ransomware and Breach Intelligence

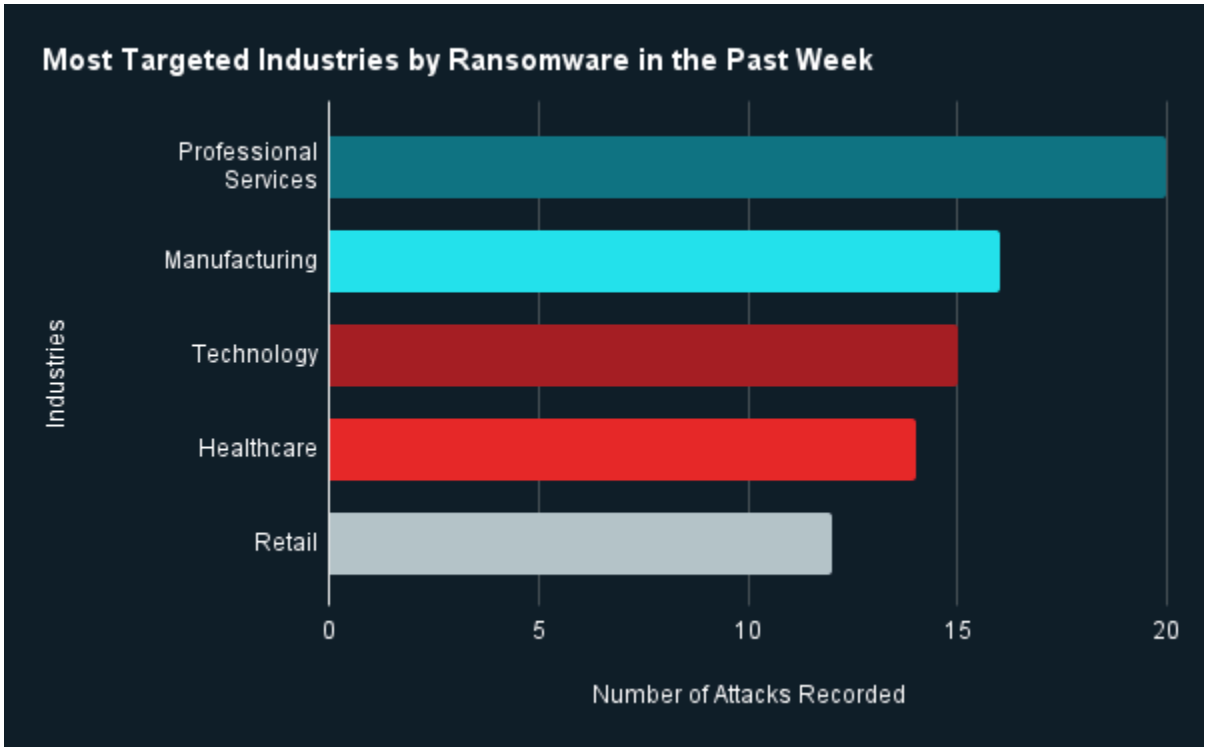
Ransomware and Breach Intelligence Key Findings

Ransomware Groups in Focus and Trends



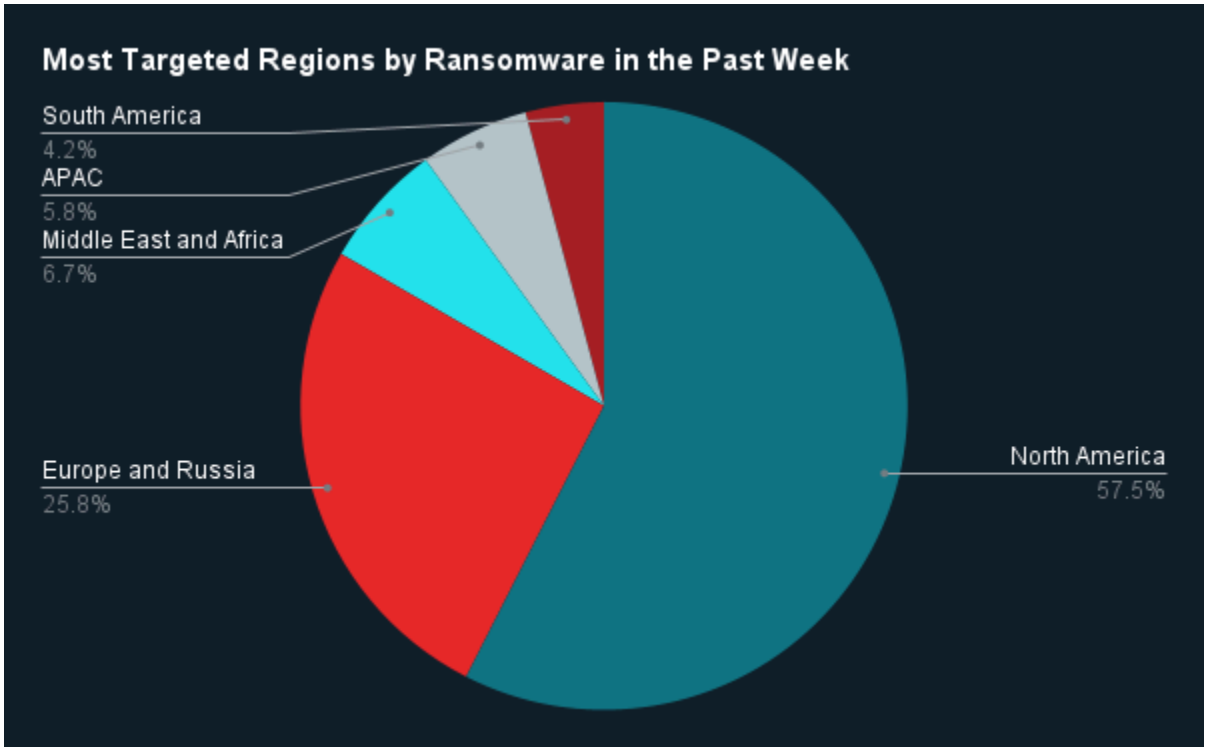
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Sinobi, Warlock, Qilin, Beast, and Everest were the most active ransomware groups. ZeroFox observed at least 114 ransomware victims disclosed, most of whom were located in North America. The Sinobi ransomware group accounted for the largest number of attacks, followed by Warlock.



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, technology, healthcare, and retail.



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 69 ransomware attacks in North America, while Europe and Russia accounted for 31, Middle East and Africa for eight, Asia-Pacific (APAC) for seven, and South America for five.

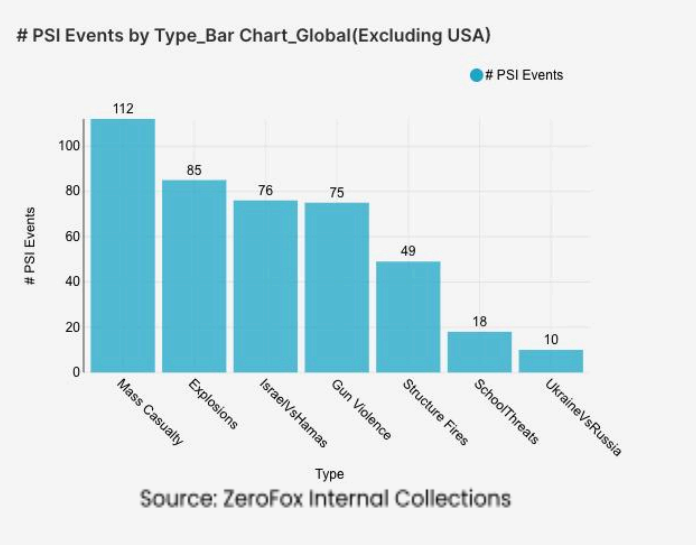
Three Prominent Breaches Across Multiple Industries

Targeted Entity	IIT Roorkee	Business Council of New York State (BCNYS)	Workday
Impacted Entities	30,000 students and alumni	Over 47,000 individuals	Unavailable
Compromised Data Fields	Mobile numbers, financial details, email addresses, photographs, and other personal data	Personal, financial, and health information	Names, emails, and phone numbers
Suspected Threat Actor	Unavailable	Unavailable	ShinyHunters
Country/Region	India	United States	United States
Industry	Education	Legal/Consulting	Professional Services
Possible Repercussions	Fraudulent transactions, account takeovers, and impersonation, as well as loan and credit card scams	Illegal obtaining of prescriptions, as well as insurance frauds and extortion	Phishing, spams, credential theft of employee records, compromise of job applicant data, and interception of internal communication

Three major breaches observed in the past week

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

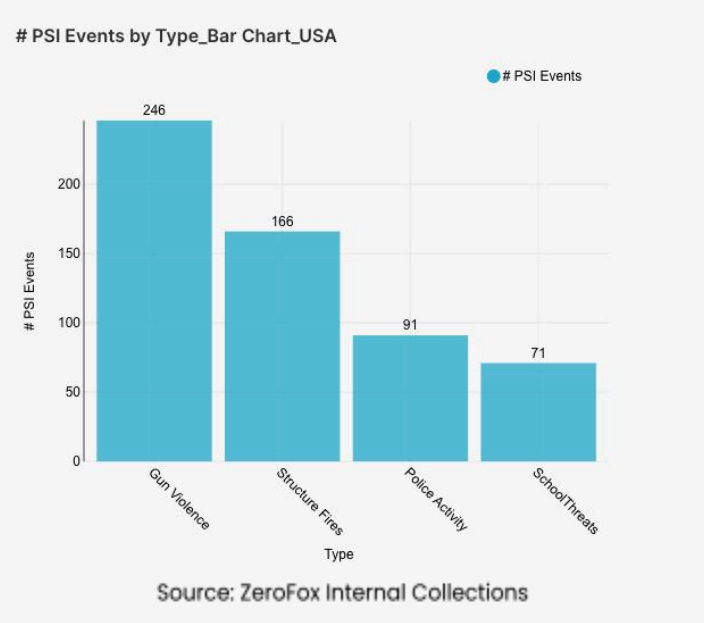


Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 1 percent increase in mass casualty events this week from the previous week, with the top contributing countries or territories being the Palestinian Territories, India, and Syria, in that order. Approximately 76 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 38 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict (including protests, raids, and attacks) increased by 27 percent from the previous week. Events related to Russia's war in Ukraine increased by 150 percent. The top three most-alerted subtypes were explosions, which saw a 16 percent increase from the previous week; gun violence, which increased by 7 percent; and structure fires, which increased by 23 percent. Global protest activity increased by 19 percent. Threats related to schools (excluding protests) increased by 38 percent.

- **What this means:** Global events related to conflict and mass casualty have seen a notable increase, with specific regions and event types accounting for a significant portion. For instance, over 60 schools in India received hoax bomb threats from a group demanding a ransom, contributing to the increase of school-related threat alerts this week. Meanwhile, Russia launched 574 drones and 40 ballistic and cruise missiles on August 21 in one of its biggest aerial attacks on Ukraine this year, as seen by the sharp rise in alerts related to this conflict as well as explosions in general. Similarly, Israel has ramped up its attacks on Gaza as part of a new ground offensive despite Hamas recently accepting a ceasefire proposal from Arab mediators. Israel's defiance of global pressure has led to growing tensions with its allies, and it is unclear whether it will accept the terms of the proposed ceasefire. On August 19, the United States carried out a raid in Syria that killed a senior ISIS figure poised to become the group's next leader in the country. The data and recent events of the week indicate a global trend of escalating conflict and violence.

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 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 that had the most gun violence alerts were Illinois and Pennsylvania, which together made up 21 percent of this week's nationwide total. Gun violence across the United States overall increased by 3 percent from the week prior. Police activity alerts increased by 14 percent, and the top contributing states were California and Texas. Structure fires decreased by 8 percent, and the top two states for this subtype were California and New York. Threats related to schools (excluding protests) increased by 4 percent. Nationwide protest activity increased by 6 percent.

- **What this means:** The past week has seen increases across various subtypes. Gun violence alerts rose somewhat; for instance, a mass shooting at a nightclub in Brooklyn, New York, left three people dead and 11 others injured. There have been eight mass shootings nationwide within the last six days alone. Police activity and protests have risen in conjunction with one another; the Trump administration recently made a decision to assert federal control over the Metropolitan Police Department (Washington, D.C.) and deploy National Guard troops to patrol the capital, which sparked "Free D.C." protests over the weekend. Since last week, hundreds of National Guard troops have set up on the streets of the nation's capital, and many more are expected to arrive in the coming days. School threats also rose; this is expected, as the FBI has noted that there is typically an uptick in threats at the beginning of the academic year. For instance, Shaler Area Elementary School in Pennsylvania postponed the first day of school this week due to a shooting threat. Overall, the past week in the United States demonstrates a fluctuating landscape of domestic incidents, marked by a rise in both violent crime and civil unrest.

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%