ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

December 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 6:00 AM (EST) on December 11, 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

United States and Allies Release Advisory on Attacks by Pro-Russia Hacktivist Groups

What we know:

- The United States and allies have released a joint advisory detailing pro-Russia hacktivist groups' attack methodology, which often involves targeting minimally secured, internet-facing Virtual Network Computing (VNC) connections to infiltrate critical infrastructure systems.
- Hacktivist groups, including Z-Pentest, NoName057(16), and Sector16, carry out lower-impact attacks compared to advanced persistent threat (APT) groups.
- The threat actors have targeted water and wastewater systems, food and agriculture, and energy sectors.

Background:

- An individual allegedly linked to NoName057(16) and CyberArmyofRussia_Reborn (CARR) has also been charged for their alleged role in cyberattacks.
- Hacktivist group CARR is assessed by the authoring agencies to be supported by the Main Directorate of the General Staff (GRU) Main Center for Special Technologies (GTsST) military unit 74455.
- NoName057(16) is assessed to be a covert project created by the Center for the Study and Network Monitoring of the Youth Environment (CISM) on behalf of the Kremlin.
- On the other hand, Z-Pentest is reportedly composed of members from CARR and NoName057(16), while Sector16 is a new group carved out of Z-Pentest.
- The U.S. government has also offered rewards for information on several of these groups, including a USD 10 million reward for information on NoName057(16).

Analyst note:

- Hacktivist groups are very likely to make exaggerated claims about their attacks and impact, which can result in loss of time and resources in inspecting systems for damages.
- They are likely to cause some damage through relentless targeting and duplication of attacks against less secured entities such as Supervisory Control and Data Acquisition (SCADA) networks.
- The involvement of state actors likely indicates the hacktivist groups' purpose is to sow chaos and distract targets from more significant threats.

Evilginx Phishing Campaign Targets 18 U.S. Universities

What we know:

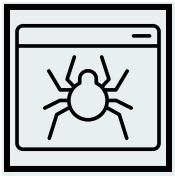
- Between April and November 2025, a phishing campaign targeted at least 18 U.S. universities and deployed nearly 70 phishing domains using the Evilginx adversary-in-the-middle (AiTM) phishing kit.
- This campaign reportedly successfully bypassed multi-factor authentication in victim systems.

Background:

- The campaign impersonated university login portals using short-lived TinyURLs and Single Sign-On (SSO) phishing pages to harvest both credentials and post-authentication session cookies, enabling threat actors to perform full account takeover.

Analyst note:

- Threat actors are likely to exploit compromised accounts to access tuition payments, payroll deposits, grants, and financial aid funds and hold this sensitive information for ransom from affected universities.



React2Shell Vulnerability Continues to Be Actively Exploited

What we know:

- React2Shell, a critical vulnerability in popular open source tool React Server Components (RSC) tracked as CVE-2025-55182, has continued to be actively exploited by various threat actors including those linked to North Korea and China.

Background:

- At least 30 organizations across various sectors (prominently in construction and entertainment sectors) have been affected.
- Threat actors are exploiting the flaw to deploy cryptocurrency miners and undocumented malware families.
- The flaw enables remote code execution (RCE) in cloud environments via unsafe deserialization.

Analyst note:

- Threat actors are almost certainly actively scanning for vulnerable systems. The large-scale activity likely indicates an automated scanning process.
- In case of compromise of cloud environments, downstream entities and systems are also very likely to be impacted, which will result in financial losses and disruption.

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 December 8 and three more on December 9 (CVE-2025-55182, CVE-2025-6218, and CVE-2025-62221). CISA also released three Industrial Control Systems (ICS) advisories on December 9, 2025. Microsoft has patched 57 vulnerabilities, including one actively exploited zero-day in Windows Cloud Files and two publicly disclosed zero-days in GitHub Copilot and PowerShell. The updates also address three RCE flaws and multiple privilege, information disclosure, and denial-of-service (DoS) vulnerabilities. Three vulnerabilities (CVE-2025-9612, CVE-2025-9613, and CVE-2025-9614) in Peripheral Component Interconnect Express (PCIe) are under investigation by major hardware vendors Intel and AMD. The flaws impact the PCIe Integrity and Data Encryption (IDE) standard and enable attackers to feed corrupted data to the receiver. Over 30 flaws, dubbed IDEsaster, expose AI-powered IDEs to prompt injection-driven data theft and RCE. SAP has released its December 2025 security updates, which fix 14 vulnerabilities, including three critical flaws in SAP Solution Manager, SAP Commerce Cloud, and SAP jConnect. Fortinet released security updates that fix two critical FortiCloud SSO authentication bypass vulnerabilities (CVE-2025-59718 and CVE-2025-59719) affecting FortiOS, FortiWeb, FortiProxy, and FortiSwitchManager. Ivanti has also released security updates for its Endpoint Manager (EPM) solution to fix multiple vulnerabilities, including two high-severity flaws (CVE-2025-13659 and CVE-2025-13662) that could allow RCE. Additionally, Adobe has addressed nearly 140 vulnerabilities across its products, including critical flaws in ColdFusion and Experience Manager (AEM).

CRITICAL

CVE-2025-66516

What happened: Apache has issued an updated security patch for a critical XML External Entity (XXE) vulnerability in Apache Tika after an earlier patch (CVE-2025-54988) failed to address the full issue.

- **What this means:** Threat actors are likely to exploit the flaw to steal sensitive data, carry out DoS attacks, and gain persistent access to isolated internal and third party systems.
- **Affected products:**
  - Tika Core versions 1.13 to 3.2.1

- Apache Tika PDF Module versions 1.13 before 2.0.0, and 2.0.0 through 3.2.1

HIGH

CVE-2025-66644

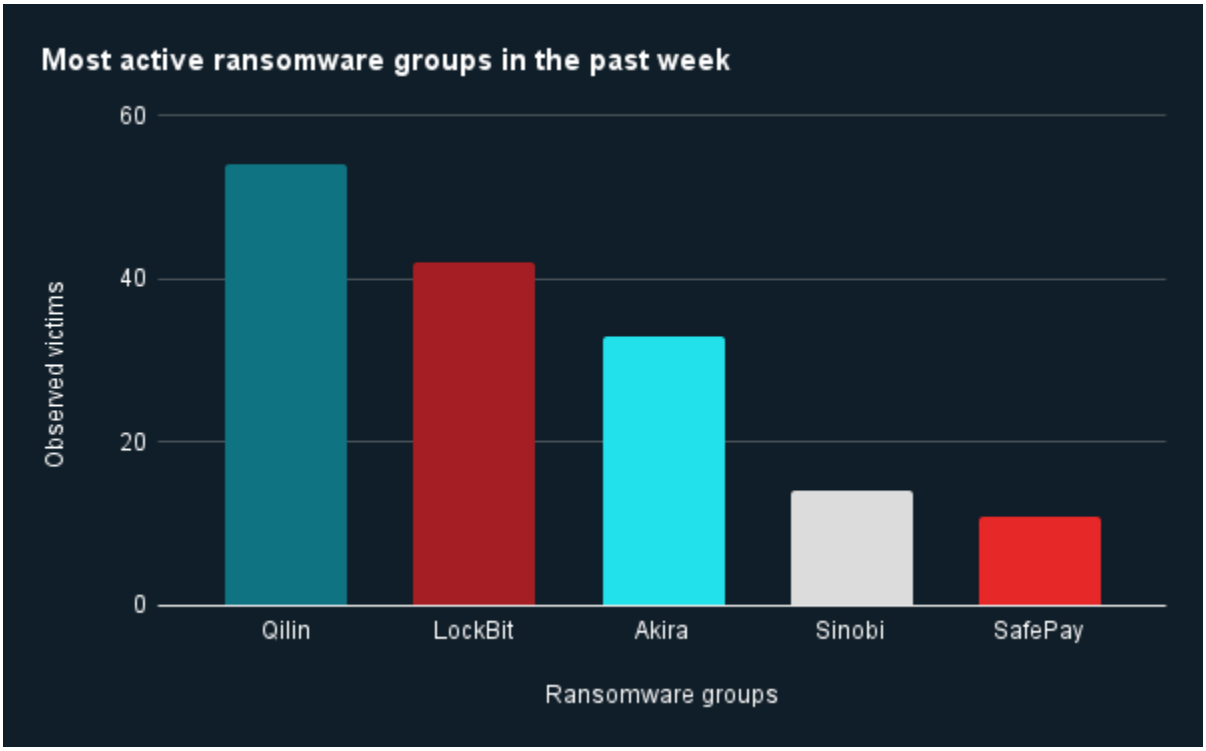
What happened: CVE-2025-66644 is an Operating System (OS) command injection vulnerability in ArrayOS AG (prior to version 9.4.5.9). This vulnerability has reportedly been exploited in the wild between August and December 2025.

- **What this means:** A malicious actor with the appropriate privileges can likely send crafted network input that gets improperly sanitized, leading to execution of arbitrary OS commands on the device.
- **Affected products:**
  - ArrayOS AG versions 0 before 9.4.5.9

Ransomware and Breach Intelligence

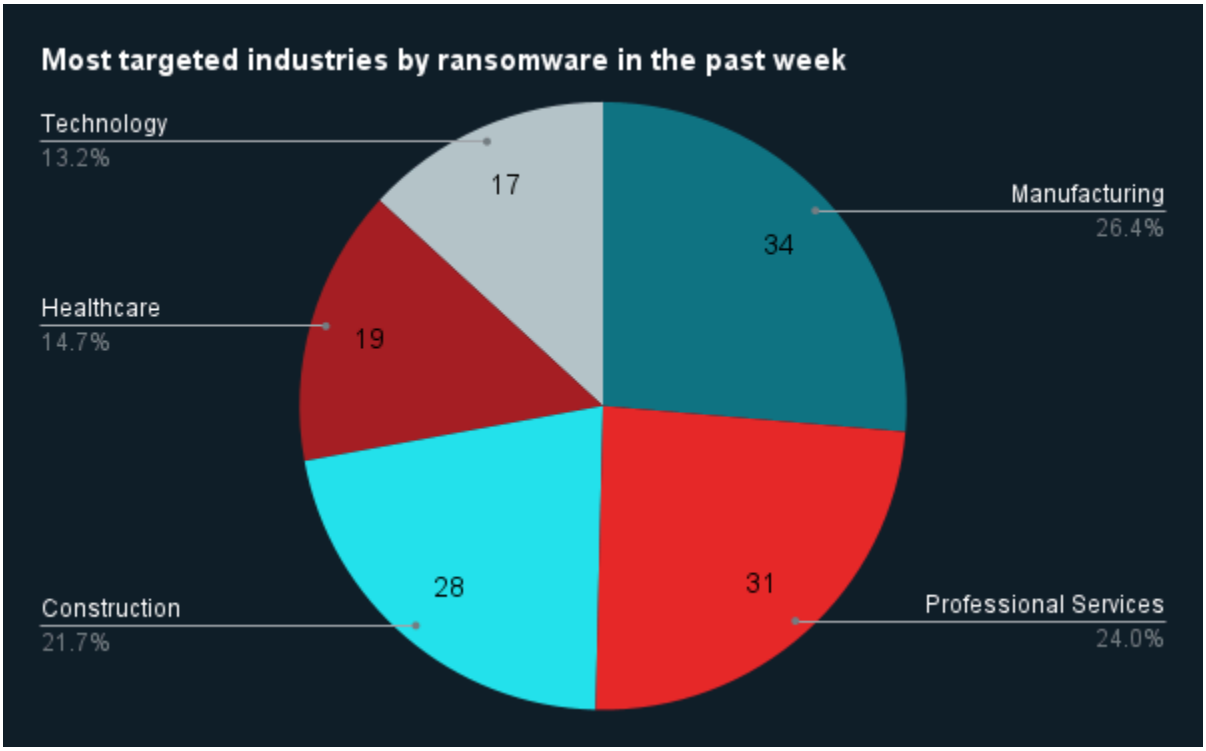
Ransomware and Breach Intelligence Key Findings

Ransomware Trends and Activities



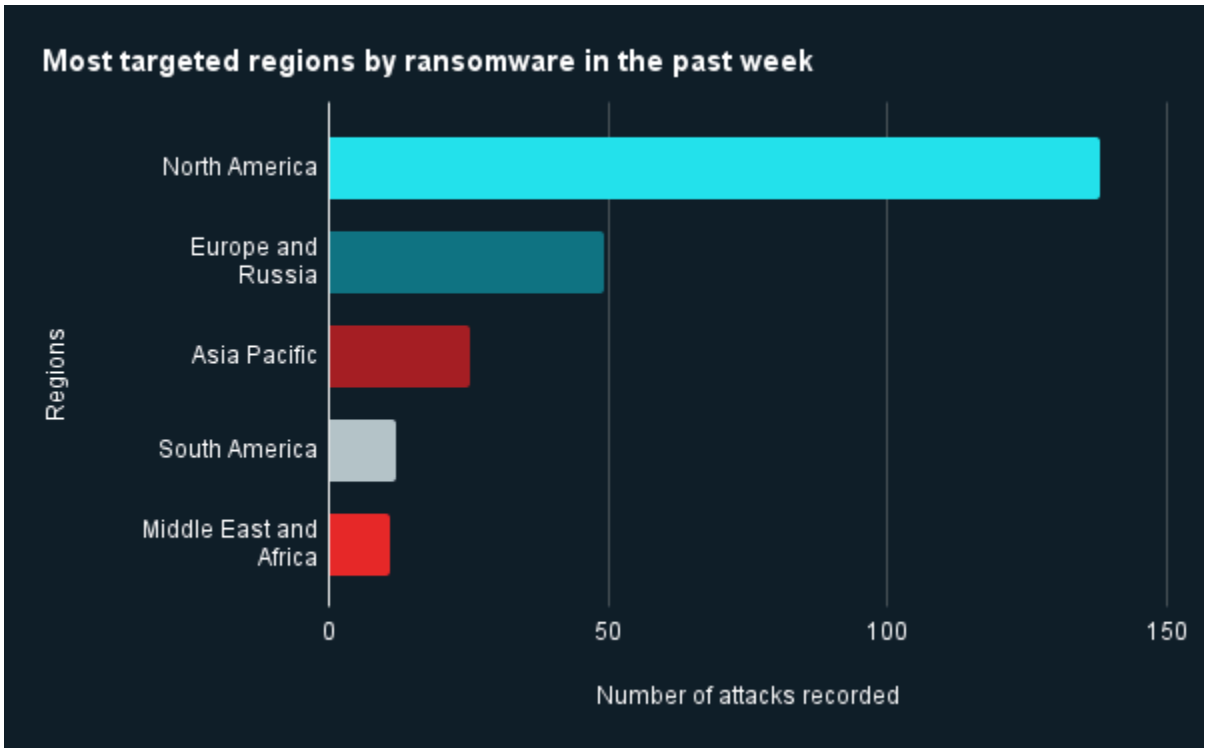
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Qilin, LockBit, Akira, Sinobi, and SafePay were the most active ransomware groups. ZeroFox observed close to 211 ransomware victims disclosed, most of whom were located in North America. The Qilin ransomware group accounted for the largest number of attacks, followed by LockBit.



Source: ZeroFox Internal Collections

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



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 138 ransomware attacks observed in North America, while Europe and Russia accounted for 49, Asia-Pacific for 25, South America for 12, and Middle East and Africa for 11.

Top Data Breaches of the Week

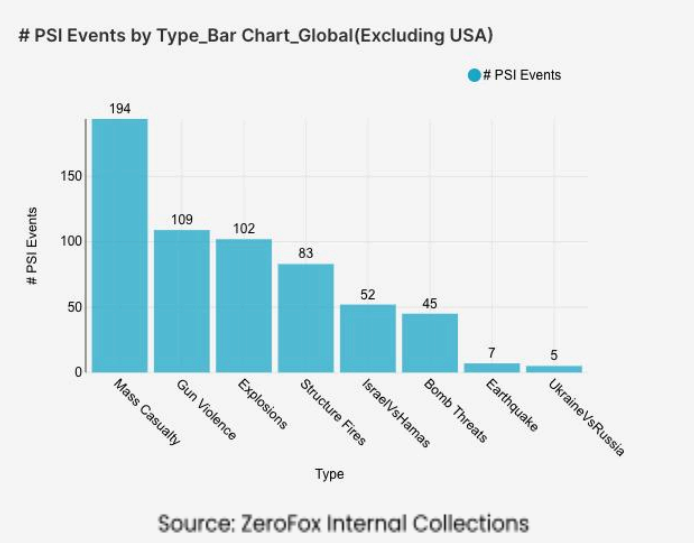
Targeted Entity	Petco	Vitas Healthcare	Morton Drug Company
Compromised Entities/victims	At least 500 customers	300,000 individuals, including current and former patients	40,051 individuals
Compromised Data Fields	Names, Social Security numbers (SSNs), driver's license numbers, financial information (such as account numbers and credit or debit card numbers), and dates of birth	Names, addresses, phone numbers, dates of birth, driver's license numbers, SSNs, medical information, insurance information, and contact information for next of kin	Names, addresses, prescription information, and, in some cases, SSNs.
Suspected Threat Actor	N/A	Unidentified	Unidentified
Country/Region	United States	United States	United States
Industry	Consumer Services	Healthcare	Healthcare
Possible Repercussions	Phishing, social engineering, identity theft, and financial fraud	Social engineering, blackmail, spearphishing, insurance fraud, and identity fraud	Identity theft and fraud, extortion, phishing, and social engineering

Three major breaches observed in the past week

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

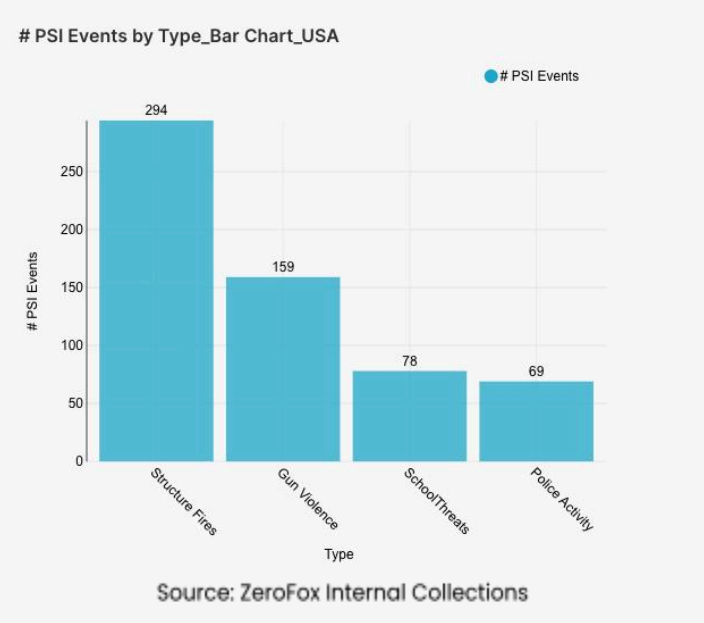


Source: ZeroFox Internal Collections

What happened: Excluding the United States, there was a 5 percent increase in mass casualty events this week from the previous week, with the top contributing countries or territories being India, the Palestinian territories, and Mexico, in that order. Approximately 53 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 40 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict (including raids and attacks) decreased by 20 percent from the previous week. Events related to Russia's war in Ukraine decreased by 17 percent. The top three most-alerted subtypes were explosions, which saw a 14 percent decrease from the previous week; gun violence, which decreased by 37 percent; and structure fires, which increased by 11 percent. Notably, bomb threats increased by 29 percent from the week prior, and earthquake alerts more than tripled from the previous week.

- **What this means:** While overall mass casualty event subtypes such as explosions and gun violence saw decreases, the total count of mass casualty events still increased. This risk is compounded by natural disasters, as earthquake alerts more than tripled from the previous week—a trend highlighted by the 7.5-magnitude earthquake off northern Japan on December 8, which injured 51 people and triggered a tsunami advisory. The Japan Meteorological Agency (JMA) has warned that another quake of similar or greater magnitude is possible in the coming week. Furthermore, instability is reflected in an increase in bomb threats, an issue immediately visible in India, where multiple Delhi schools received threat emails on December 10, prompting widespread evacuations. Lastly, the increase in structure fires is linked to the early start of the bushfire season in Australia; over 75 wildfires have occurred across New South Wales and Tasmania in early December and destroyed several homes. The overall state of global physical security is characterized by a continued high risk in conflict zones and a significant vulnerability arising from both natural disasters and targeted threats.

Physical Security Intelligence: United States



What happened: In the past week, the top three most-alerted incident 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 two states with the most gun violence alerts were New York and California, which together made up 17 percent of this week's nationwide total. Gun violence across the United States overall increased by 5 percent from the week prior. Police activity alerts increased by 77 percent, and the top contributing states were California and New York. Structure fires decreased by 8 percent, and the top two states for this subtype were also California and New York. Notably, threats related to schools increased by 117 percent.

- **What this means:** Domestic security this past week was defined by a surge in law enforcement intervention and persistent fatal violence. The jump in threats related to schools underscores a growing trend of security risk against educational institutions and reflects the daily environment of hoaxes, swatting incidents, and real threats that force constant law enforcement response, explaining the increase of both police activity and school threat alerts. This surge is reflected in recent incidents such as a bomb threat that forced an evacuation at Liberty County High School in Georgia on December 9, as well as a shelter-in-place at Nipomo High School in California on December 9 due to a similar threat. Meanwhile, gun violence alerts increased somewhat, with eight total mass shootings occurring last week. Finally, structure fires, while decreasing nationally, remained a persistent man-made disaster risk in these same two states; for instance, on December 10, a fuel truck and a house caught fire in Staten Island, New York, and one resident and one firefighter were injured. The overall state of domestic physical security is characterized by elevated risks due to an increase in police intervention and school-related threats despite some volatility and localized decreases in other categories.

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%