ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

March 21, 2026

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 12:00 PM (EDT) on March 20, 2026; 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 - SITREP #26 - Military Strikes on Iran - March 20, 2026

Israel and Iran have intensified attacks on key regional energy facilities, signaling a significant escalation in the conflict. While U.S. President Donald Trump has denied involvement and warned both nations against further targeting of energy infrastructure, his comments likely reflect diverging strategic aims between the United States and Israel. Energy prices have surged as these latest strikes increase the prospect of a long-term impact on global supplies and suggest a slower resumption of production once the conflict ends. Furthermore, Israel's targeting represents a notable shift toward degrading Iran's economic infrastructure to limit its combat capabilities. The United States and Israel continued a campaign targeting senior Iranian security officials, a tactic which is very likely part of efforts to set the conditions for a civil uprising in Iran. In turn it has left the IRGC in control of most decision making at the political and military level. To know more about how the conflict has progressed, read previous SITREPs.

ZeroFox Intelligence Brief - Underground Economist: Volume 6, Issue 6

The Underground Economist is an intelligence-focused series illuminating Dark Web findings in digestible tidbits from our ZeroFox Dark Ops intelligence team.

ZEROFOX®

Weekly Intelligence Brief

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

Phishing Attack Impersonates Major Brands to Target C-Level Executives

What we know:

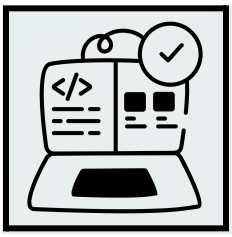
- A cybersecurity company has reportedly intercepted a sophisticated phishing attack that impersonated major technology and financial companies.
- The phishing attempt was aimed at the company's C-level executives to lead them to a page requesting their credentials.

Background:

- The attack was engineered to bypass multiple layers of enterprise email security without triggering alerts using anti-bot and human verification services to evade automated detection.
- The attacker behind this attempt was suspected to have used a phishing-as-a-service toolkit called Kratos.

Analyst note:

- Given this attack's elaborate infrastructure, it is likely a strong threat against users who are less technically aware and those whose device security relies heavily on anti-virus software alone.
- A phishing campaign of this sophistication can likely succeed and remain undetected if it targets general consumers, small businesses, or organizations without advanced security training.



New GlassWorm Campaign Found in 433 Compromised Code Repos

What we know:

- The GlassWorm supply chain malware has been found in 433 compromised components in March 2026.

- Researchers described it as a new campaign targeting hundreds of packages, repositories, and extensions on software development platforms.
- The malware is designed to steal crypto wallets, credentials, and compromise developer environments.

Background:

- The campaign begins with compromised GitHub accounts, which then publish obfuscated malicious packages on npm and OpenVSX.
- Instructions are hidden using Solana transactions to deliver a Node.js infostealer.
- A single Russian-language threat actor is suspected to be behind the campaign.

Analyst note:

- Indicators of compromise (IoCs) include the presence of persistence files (~/init[.]json), unexpected Node[.]js installations, suspicious i[.]js files in new projects, and anomalous Git commit histories.
- Successful intrusion is likely to result in complete compromise of developer environment and downstream impacts.

SocksEscort Residential Proxy Network Disrupted for Enabling Large-Scale Criminal

What we know:

- Law enforcement has disrupted the SocksEscort proxy network, which allegedly compromised 369,000 routers and Internet of Things (IoT) devices and sold access to over 35,000 proxy nodes.
- Researchers previously disrupted the network in 2023, but operators later rebuilt the infrastructure and resumed infections using AVRecon malware.

Background:

- Investigators linked the SocksEscort proxy network to crimes, including a USD 1 million cryptocurrency theft, a USD 700,000 fraud against a Pennsylvania manufacturer, and a USD 100,000 fraud targeting military personnel.
- Proxy networks such as SocksEscort are commonly used by threat actors by routing malicious traffic through legitimate residential IP addresses.

Analyst note:

- Blocking over 35,000 proxy nodes is likely to decrease malicious traffic routed through residential IPs in the short term.
- However, given that operators previously rebuilt the AVRecon botnet, threat actors are likely to reconstitute the proxy network or migrate to other residential proxy services in the near term.

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 five vulnerabilities on March 18, March 16, and March 13, 2026, to its Known Exploited Vulnerabilities (KEV) catalogue. Additionally, on March 17, 2026, CISA released four Industrial Control Systems (ICS) advisories featuring a total of 134 vulnerabilities, including CVE-2026-25569, CVE-2025-13957, CVE-2026-0667, and CVE-2025-2595**.** Google has released an emergency update for Google Chrome 146 to patch two actively exploited zero-day vulnerabilities, tracked as CVE-2026-3909 and CVE-2026-3910. CISA has warned U.S. agencies of an already patched vulnerability tracked as CVE-2025-47813 in their Wing FTP Servers that is still observed to be exploited as part of a chained remote code execution (RCE) attack. Apple has released a security patch for a WebKit flaw CVE-2026-20643 that enabled malicious web content to bypass the browser's Same Origin Policy.

CRITICAL

CVE-2026-3564

What happened: ConnectWise has confirmed this critical vulnerability in its ScreenConnect that could enable attackers to bypass authentication and gain unauthorized access. The flaw enables extraction of ASP.NET machine keys, potentially leading to session hijacking and privilege escalation, with reports of attempted abuse observed in the wild.

- **What this means:** Exploiting this vulnerability can likely lead to threat actors forging authenticated sessions and bypass login controls on victim devices.
  - **Affected products**: ScreenConnect version prior to 26.1

CRITICAL

CVE-2026-32746

What happened: This bug enables unauthenticated RCE via Port 23 using crafted Set Local Characters (SLC) messages during pre-authentication handshake, granting root-level access.

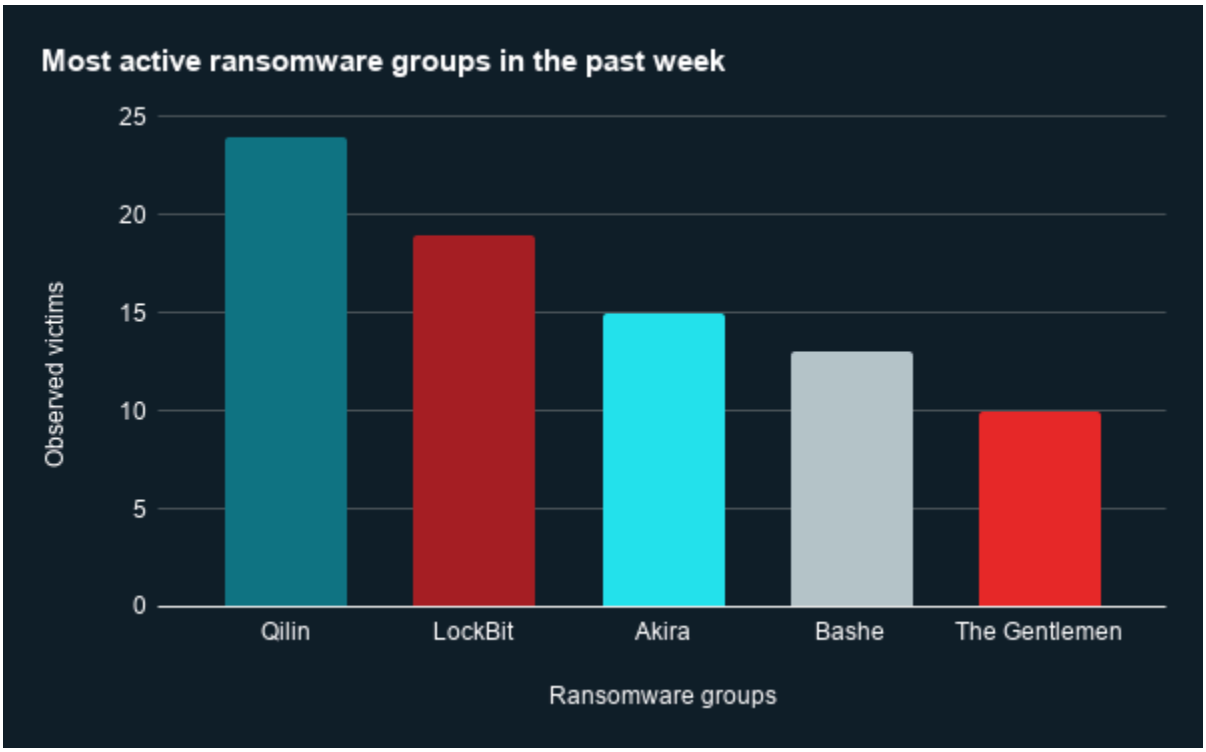
- **What this means:** Threat actors are likely to exploit this bug in unpatched systems to maintain access and move across connected networks, especially where internal segmentation and access controls are limited.
    - **Affected products:** GNU InetUtils telnet daemon

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

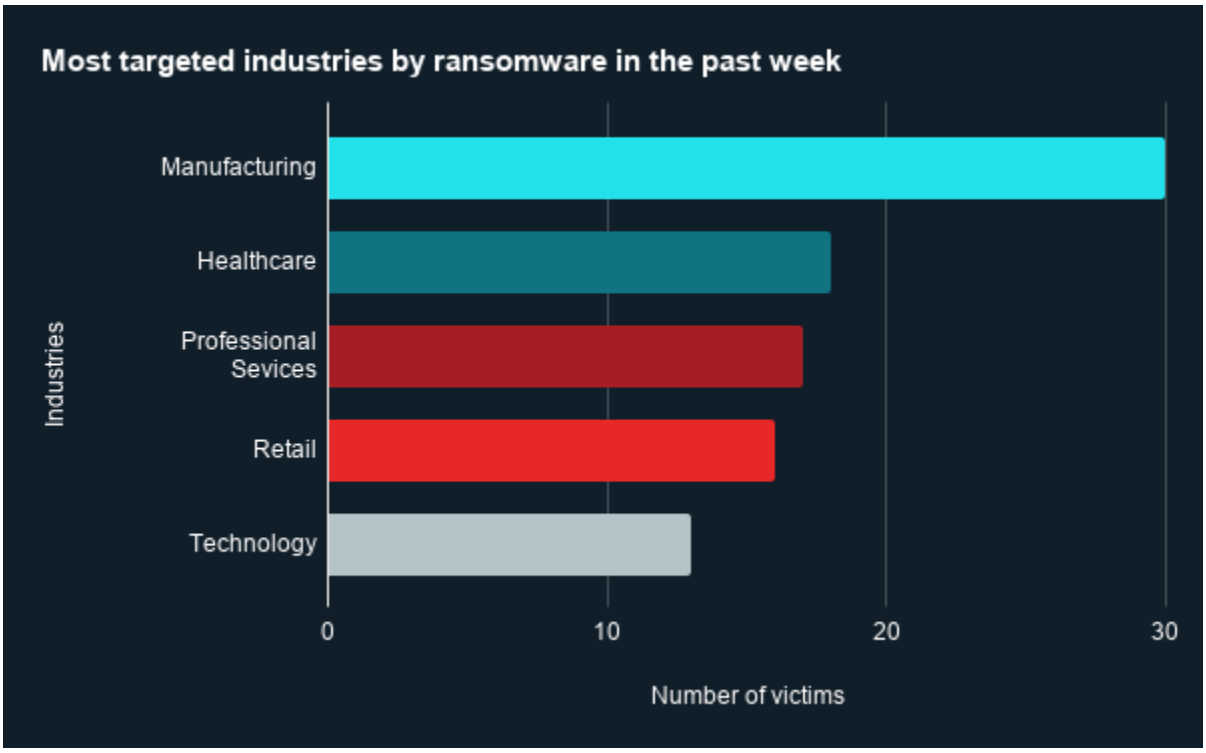
Ransomware Group Trends across Industries and Regions

Last week in ransomware: In the past week, Qilin, LockBit, Akira, Bashe, and The Gentlemen were the top five most active ransomware groups. ZeroFox observed at least 162 ransomware attacks. The Qilin ransomware group accounted for the largest number of attacks. Meanwhile, North America was the region most targeted.



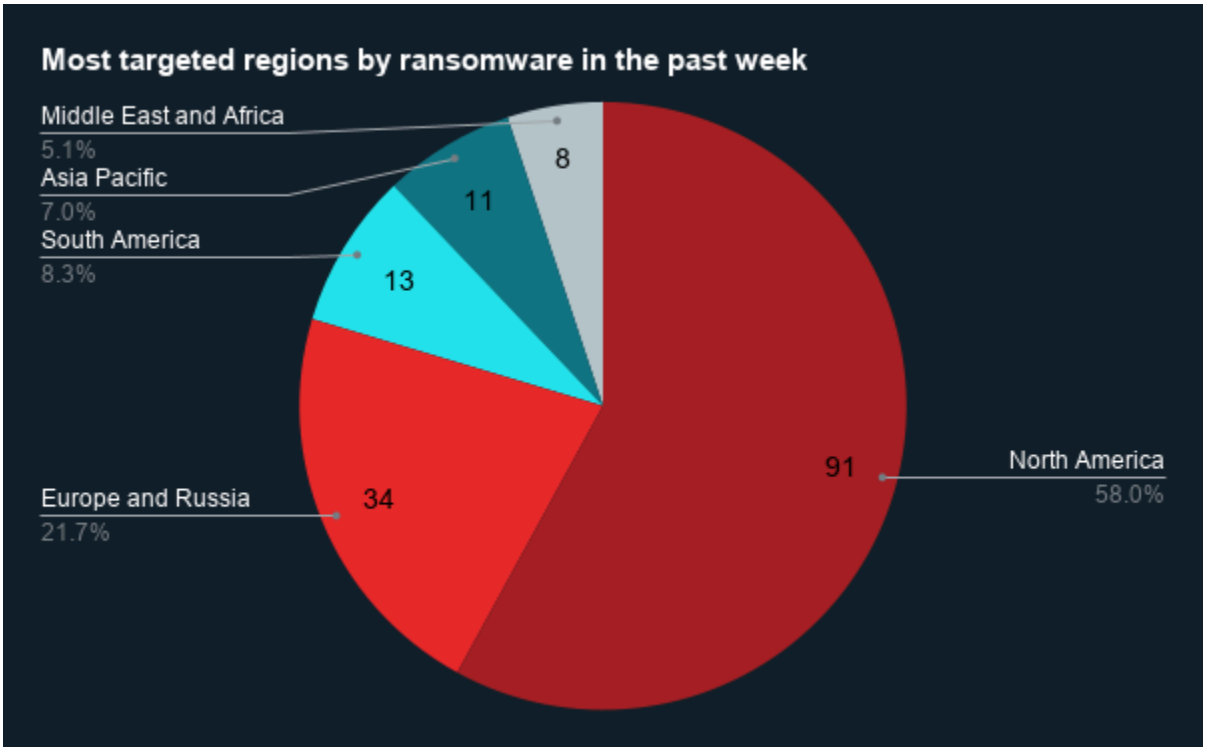
Source: ZeroFox Internal Collections

Industry ransomware trends: In the past week, ZeroFox observed that manufacturing was the industry most targeted by ransomware attacks, followed by healthcare, professional services, retail, and technology.



Source: ZeroFox Internal Collections

Regional ransomware trends: In the past week, ZeroFox observed that North America was the region most targeted by ransomware attacks. North America accounted for 91 attacks, while Europe and Russia accounted for 34, South America for 13, Asia-Pacific for 11, and the Middle East and Africa for eight.



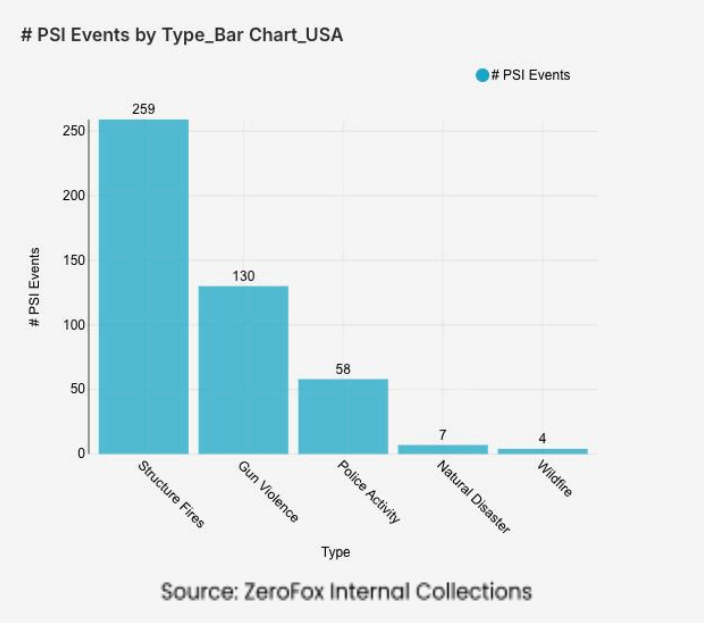
Source: ZeroFox Internal Collections

Major Data Breaches in the Past Week

Targeted Entity	Navia Benefit Solutions	Community Nurse	Deaconess Health System
Compromised Entities/Victims	Approximately 2.7 million individuals	6,746 individuals	Multiple individuals' records
Compromised Data Fields	Full name, date of birth, Social Security Number (SSN), phone number, email address, HRA/FSA participation data, COBRA enrollment information	Names, addresses, dates of birth, Medicare numbers, medical record numbers, provider details, diagnoses/health status, medication lists, treatment orders, care timelines, and advance directives	Personal information, contact details, and medical history and health records
Suspect	N/A	N/A	N/A
Country/Region	United States	United States	United States
Industry	Professional services	Healthcare	Healthcare
Possible Repercussions	Identity theft, financial fraud, social engineering campaigns, account takeover attempts, and potential follow-on attacks targeting employers or related service providers	Medical identity theft, insurance fraud, and targeted phishing and social engineering campaigns	Privacy violations, stalking, and targeted harassment, identity theft, and social engineering

Three major breaches observed in the past week

Physical and Geopolitical Intelligence Key Findings



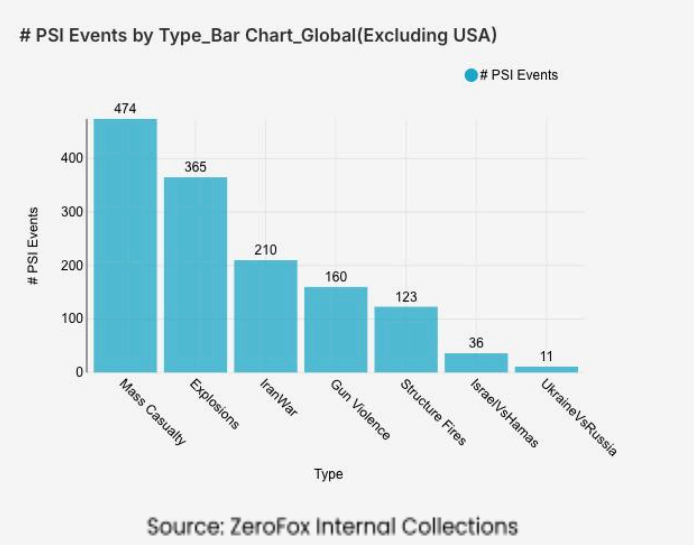
Source: ZeroFox Internal Collections

Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 2 percent decrease in mass casualty events this week from the previous week, with the top contributing countries or territories being Iran, Iraq, and Lebanon, in that order. Approximately 77 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 36 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict decreased by 41 percent from the previous week, and alerts related to the war in Iran decreased by 13 percent. Events related to Russia's war in Ukraine increased by 57 percent. The top three most-alerted subtypes were explosions, which saw a 4 percent decrease from the previous week; gun violence, which increased by 5 percent; and structure fires, which increased by 14 percent.

- **What this means:** Global security data from the past week reveals a slight decline in mass casualty events outside the United States. However, the Middle East remains a primary driver of these incidents. Iran, Iraq, and Lebanon accounted for a large portion of all alerts, fueled by a cycle of assassinations and retaliatory strikes. For instance, on March 17, Israeli airstrikes in Tehran killed Iranian security chief Ali Larijani, while simultaneous explosions rocked the U.S. embassy compound in Baghdad. There have also been repeated attacks by Iran around the Erbil International Airport and U.S. Consulate General Erbil. While general alerts for the Israel-Hamas conflict dropped following the implementation of the "Board of Peace" oversight, Russia's war in Ukraine saw a significant increase in activity as Russian forces claimed control of 12 new settlements in early March and launched a major attack in the Zaporizhzhia region on March 19 that caused mass power outages. Overall, while specific regional hotspots around the globe show signs of de-escalation, the global physical security landscape remains volatile, characterized by a shift in conflict intensity and a rise in infrastructure-related emergencies.

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 22 percent of this week's nationwide total. Gun violence across the United States overall decreased by 22 percent from the week prior. Police activity alerts decreased by 24 percent, and the top contributing states were California and Florida. Structure fires increased by 1 percent, and the top two states for this subtype were New York and California. Notably, there were four times as many wildfire alerts this week than the week before.

- **What this means:** The past week across the United States has seen a specific shift in public safety concerns, characterized by a decrease in interpersonal violence but a sharp rise in environmental hazards. Most notably, the fourfold increase in wildfire alerts is highlighted by the current situation in Nebraska, where the Morrill and Cottonwood fires have spearheaded a historic fire season with one fatality, burning over 800,000 acres and becoming the largest in state history. While structure fires overall saw only a small increase, significant regional activity in New York and California contributed to the nation's fire statistics. For instance, on March 16, a four-alarm fire in Queens, NY, claimed four lives, including a three-year-old child, while a major commercial blaze at an auto shop in Los Angeles, CA, on March 16 required a 40-firefighter response. This week saw three mass shootings, the most recent of which occurred on March 16 in Riviera Beach, FL, and resulted in five victims. Overall, while the United States saw a reprieve in the frequency of interpersonal violence and police interventions this week, the domestic security landscape remains high-risk due to a volatile combination of fatal urban structure fires and record-breaking wildfire activity.

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%