ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

March 14, 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 6:00 AM (EST) on March 12, 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 #21 - Military Strikes on Iran - March 12, 2026

Iran continued attacks on oil tankers and cargo vessels in the Persian Gulf overnight, with two tankers struck in the Umm Qasr port in the Iraqi city of Basra. Both this port and the Mina Al Fahal port in Oman have ceased operations. Iran is very likely seeking to impose financial costs on the region in an effort to force the United States to stop hostilities on Iranian terms. In addition to oil shipping, Iran has threatened to target U.S. economic and banking interests in the region that it believes have contributed to the hostilities against it. Iran likely maintains the capability to conduct sophisticated cyberattacks against the financial sector, as well as technology companies contributing to the war effort. To know more about how the conflict has progressed, read previous SITREPs.

ZEROFOX®

Weekly Intelligence Brief

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

High-Profile Signal and WhatsApp Accounts Targeted

What we know:

- Dutch security and military services have revealed that Russian state-linked threat actors have taken over Signal and WhatsApp accounts belonging to some government officials, military personnel, and other high-profile targets.

Background:

- Russian state-linked actors reportedly impersonated a Signal support chatbot to trick victims into sharing verification or PIN codes, enabling them to take over their messaging accounts.
- In the case of WhatsApp, they abused the "linked devices" feature to connect attacker-controlled devices to victims' accounts. Once linked, attackers could silently read incoming messages and group chats, likely enabling them to access sensitive information.

Analyst note:

- Signal and WhatsApp are two communication platforms that users generally trust, given their claims of anonymity and encryption.
- These account takeover maneuvers likely enable threat actors to observe high-profile users that trusted the apps with their confidential conversations.
- The threat actors are likely to leverage the compromised accounts to impersonate victims in spear phishing campaigns, spread misinformation, or manipulate internal discussions on these platforms.
- Monitoring group chats and real-time communications can likely provide these threat actors insight into government decisions, crisis responses, or upcoming actions.

Lazarus Group Uses Deepfaked Recruiter in Fake Interview

What we know:

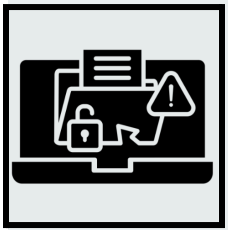
- North Korean threat group Lazarus Group targeted a security company's CEO through a fake job interview arranged via a popular job portal.
- They tried to trick the CEO into opening a malicious coding project in Visual Studio Code as part of a fake technical interview, with a recruiter impersonating a real person for the "interview."

Background:

- The CEO suspected a deepfake impersonation after noticing that the recruiter's voice did not match the real individual's voice in publicly available videos.
- Additionally, the project contained the group's BeaverTail malware, but the CEO analyzed it in a sandbox, prompting the attackers to activate a kill switch and erase activity.

Analyst note:

- A CEO's laptop typically contains privileged emails, credentials, and internal documents that are likely to enable further infiltration or intelligence-gathering.
- Lazarus Group was likely trying to collect intelligence on security defenses and potentially gain access to networks monitored or protected by the CEO's company, which can enable the group to improve future cyber operations.



Poland Uncovers Minors Selling DDoS Tools

What we know:

- Poland's cyber police has identified seven minors who allegedly ran a scheme selling tools used to conduct distributed denial-of-service (DDoS) attacks.
- The suspects sold tools that were reportedly used to target popular websites, including auction platforms, hosting services, IT domains, and accommodation booking sites.

Background:

- During the searches, officers seized smartphones, laptops, storage drives, a ledger, and handwritten notes, along with tools and infrastructure allegedly used to launch DDoS attacks.
- As the suspects are minors, the case will be handled by family courts to determine further action.

Analyst note:

- It is likely that the suspects sold these tools to buyers who wanted to disrupt websites to cause them operational harm and disrupt transactions.
- Seizing the infrastructure is likely to provide law enforcement with information to identify affected businesses and uncover other cybercrimes that the DDoS attacks veiled.

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 vulnerabilities on March 9 and March 11, 2026, to its Known Exploited Vulnerabilities (KEV) catalogue. Additionally, on March 10, 2026, CISA released four Industrial Control Systems (ICS) advisories featuring a total of 13 vulnerabilities, including CVE-2025-11126, CVE-2025-67039, CVE-2026-3611, and CVE-2025-57176. Microsoft patched 84 vulnerabilities across its products for March 2026 Patch Tuesday, including eight critical and two publicly known flaws. Adobe has released patches for 80 vulnerabilities across eight products (including Adobe Illustrator and Acrobat Reader) that address multiple high-severity flaws that could enable arbitrary code execution, privilege escalation, and security feature bypasses. SAP has released 15 security notes addressing critical vulnerabilities in SAP Quotation Management Insurance (FS-QUO) and SAP NetWeaver Enterprise Portal that could enable remote code execution, privilege escalation, and denial-of-service attacks. Ivanti has released an update for Ivanti Desktop and Server Management (DSM) addressing a high-severity vulnerability that could allow attackers to elevate local privileges if exploited.

HIGH

CVE-2025-20105

What happened: Improper input validation in a Unified Extensible Firmware Interface (UEFI) System Management Mode (SMM) on certain Intel(R) reference platforms could enable privilege escalation and local code execution when exploited by a privileged attacker with low attack complexity.

- **What this means:** Intel has disclosed nine vulnerabilities in the UEFI firmware affecting certain reference platforms. Threat actors are likely to exploit unpatched versions to gain control of affected devices before operating systems load, enabling code execution and bypassing security controls.
  - **Affected products** are included in this advisory.

CRITICAL

CVE-2026-32136

What happened: A flaw in AdGuard Home prior to version 0.107.73 allows an unauthenticated remote attacker to bypass authentication by sending an HTTP/1.1 request that upgrades the connection to HTTP/2 cleartext (h2c).

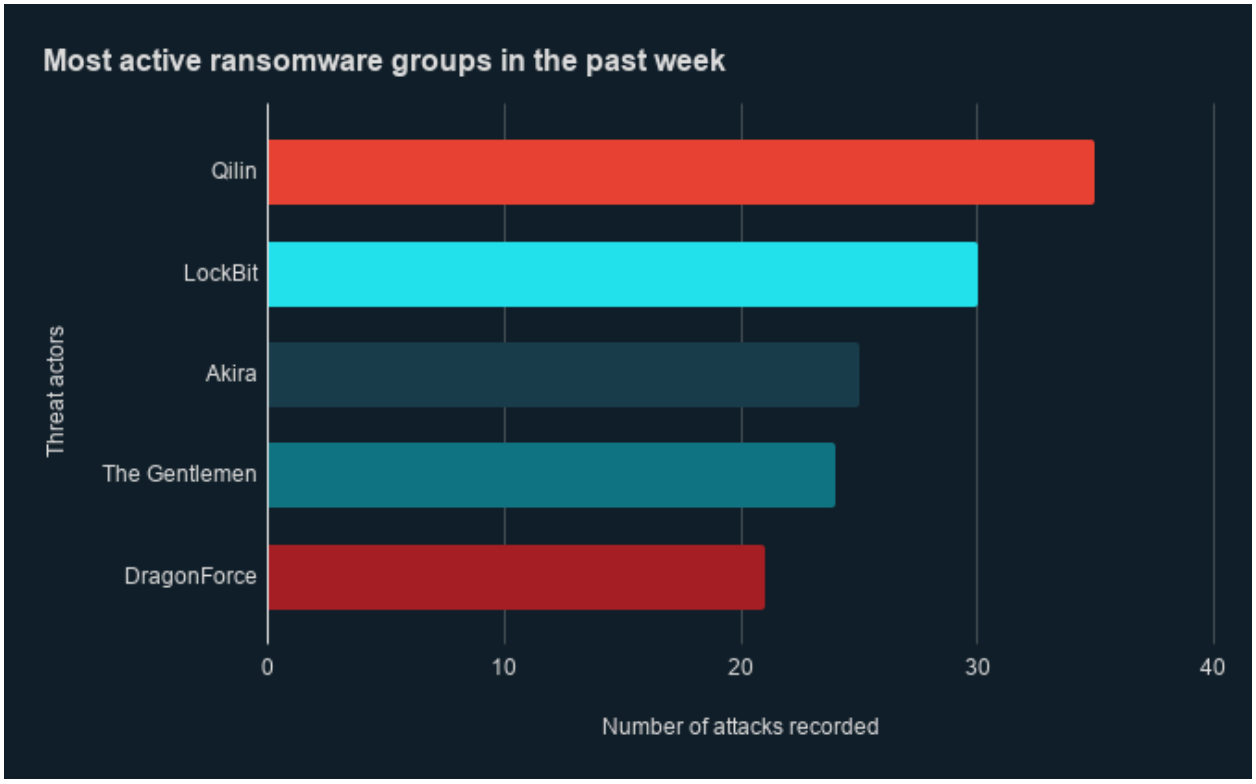
- **What this means:** By sending a specially crafted request that forces the server to switch from HTTP/1.1 to HTTP/2 (h2c), the request gets routed to a component that does not enforce authentication checks. Consequently, the server treats the attacker as if they are already logged in, enabling them to access or modify settings. Attackers are likely to exploit unpatched versions to take control of the AdGuard Home admin interface.
  - **Affected products:** AdGuardHome version prior to 0.107.73

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

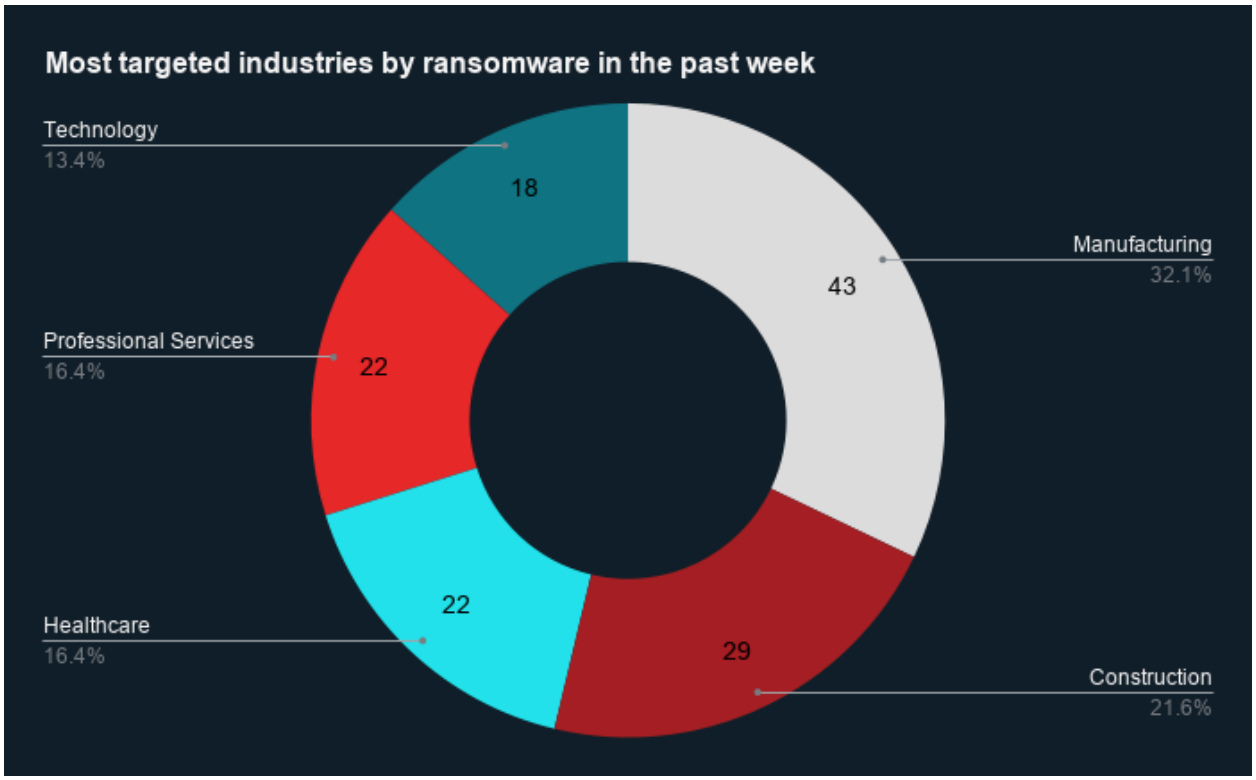
Ransomware Trends Observed in the Past Week

Last week in ransomware: In the past week, Qilin, LockBit, Akira, The Gentlemen, and DragonForce were the top five most active ransomware groups. ZeroFox observed at least 195 ransomware attacks. The Qilin ransomware group accounted for the largest number of attacks. Meanwhile, North America was the region most targeted.



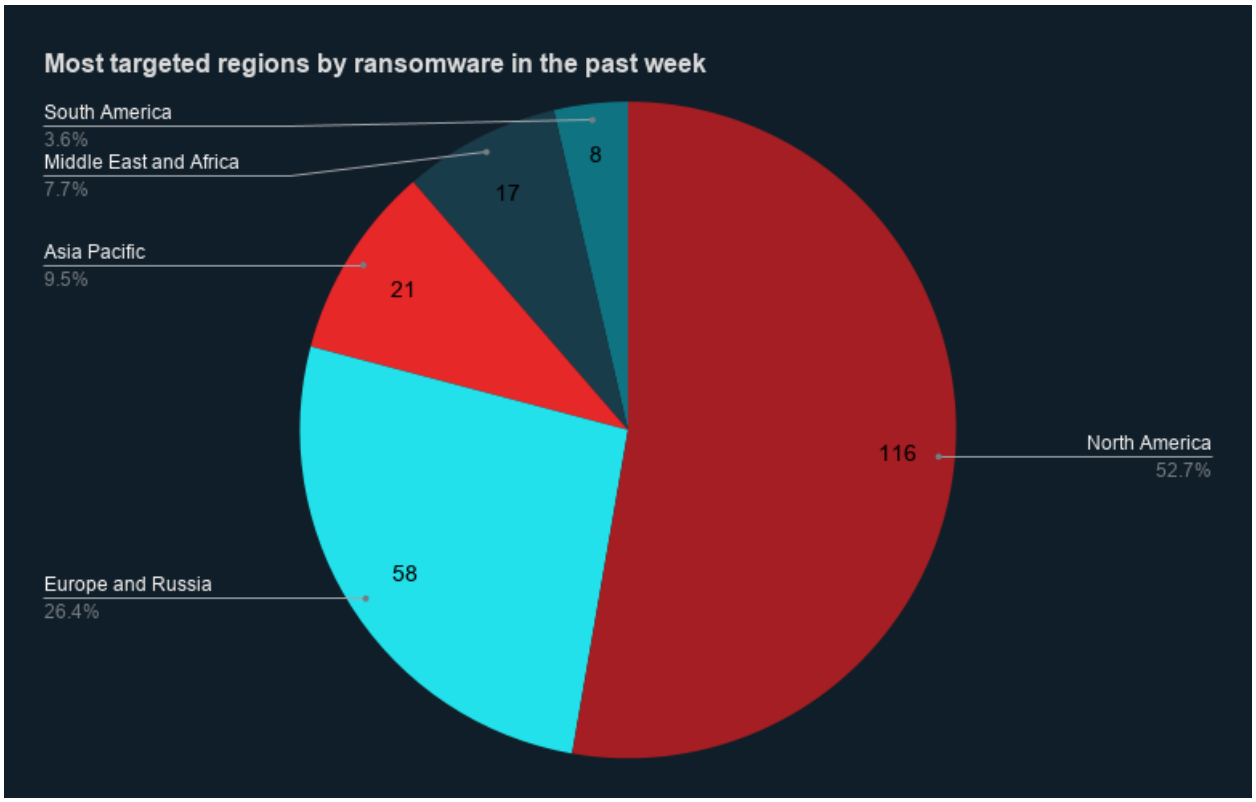
Source: ZeroFox Internal Collections

Industry ransomware trends: In the past week, ZeroFox observed that manufacturing was the industry most targeted by ransomware attacks, followed by construction, healthcare, professional services, 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 116 attacks, while Europe and Russia accounted for 58, Asia-Pacific for 21, the Middle East and Africa for 17, and South America for eight.



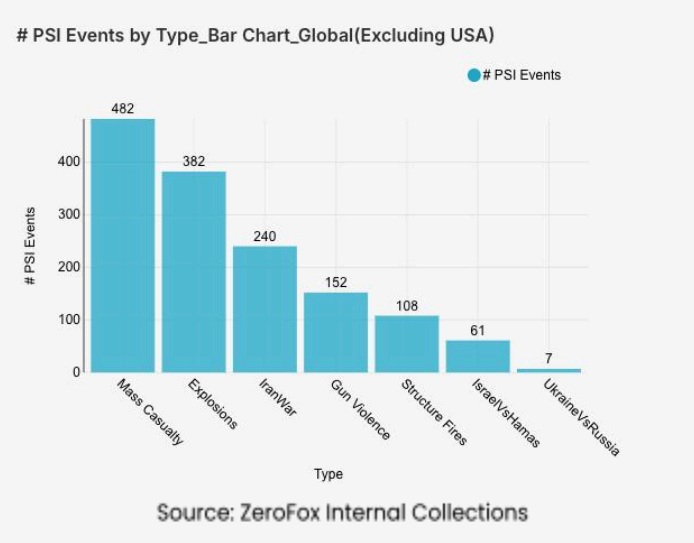
Source: ZeroFox Internal Collections

Significant Data Breaches Reported in the Past Week

Targeted Entity	Kafese	Loblaw	Bell Ambulance
Compromised Entities/Victims	Customer data	Customer information	237,830 individuals
Compromised Data Fields	Full names, dates of birth, physical addresses, email addresses, phone numbers, applicant income details, bank verification results (including bank names, routing, and account numbers), credit and vantage score ranges, and Know Your Customer (KYC) documentation (including government-issued ID scans, and associated sales personnel)	Names, phone numbers, and email addresses	First and last names, birth dates, Social Security numbers (SSNs), driver's license numbers, financial account information, medical information, and health insurance information
Suspected Threat Actor	DarkForums user ResPublica	N/A	N/A
Country/Region	United States	Canada	Wisconsin, United States
Industry	Financial Services	Retail/CPG	Healthcare
Possible Repercussions	Identity theft, financial fraud, and phishing attacks	Phishing and social engineering attacks	Insurance fraud, identity theft, phishing, and social engineering attacks

Three major breaches observed in the past week

Physical and Geopolitical Intelligence Key Findings

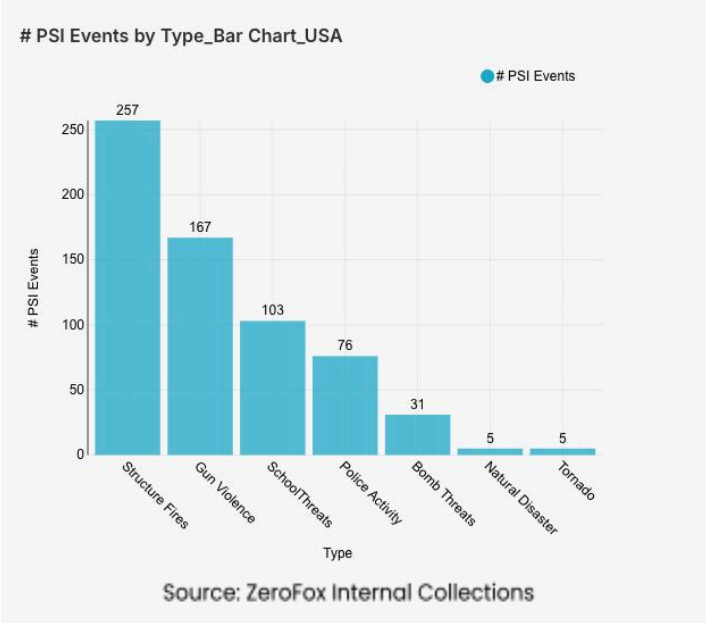


Physical Security Intelligence: Global

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 India, in that order. Approximately 79 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 41 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict increased by 91 percent from the previous week, and alerts related to the war in Iran increased by 293 percent. Events related to Russia's war in Ukraine increased by 250 percent. The top three most-alerted subtypes were explosions, which saw an 8 percent decrease from the previous week; gun violence, which decreased by 1 percent; and structure fires, which decreased by 10 percent.

- **What this means:** The significant surge in alerts related to the war in Iran reflects the intensification of Operation Epic Fury. As the conflict entered its 13th day this Thursday, the civilian death toll in Iran surpassed 1,348, highlighted by events like the Minab school bombing on February 28, when a Tomahawk missile strike resulted in at least 175 casualties. In Iraq, recent explosive attacks on March 12 by Iranian-laden boats on oil tankers near Basra have mirrored the global trend of explosion-related events. Meanwhile, the increase in Israel-Hamas conflict alerts is driven by a wave of Israeli strikes in Lebanon, including an attack in Beirut's Ramlet al-Baida neighborhood on March 11 that killed seven civilians. Similarly, the increase in Ukraine-related alerts is fueled by Russia's recent aerial campaign; in the first week of March alone, Russia deployed nearly 1,750 kamikaze drones and over 1,500 glide bombs, targeting energy grids and residential areas in cities such as Kharkiv, where a missile strike on March 7 killed 11 civilians. The overall current global landscape is defined by a volatile shift toward high-intensity regional warfare and large-scale aerial campaigns, resulting in a significant number of conflict zones despite a minor technical decrease in isolated mass casualty events.

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 Illinois and Texas, which together made up 19 percent of this week's nationwide total. Gun violence across the United States overall decreased by 18 percent from the week prior. Police activity alerts decreased by 12 percent, and the top contributing states were California and New York. However, nationwide school-related threats increased by 18 percent, and bomb threats by 94 percent. Structure fires decreased by 16 percent, and the top two states for this subtype were California and New York. Notably, natural disaster alerts across the country increased by 150 percent.

- **What this means:** In the past week, the United States has navigated a complex landscape of public safety challenges, including weather-related physical security concerns. A severe storm system claimed at least eight lives across Michigan and Oklahoma on March 7 and an additional five lives in Indiana and Illinois between March 10 and 11, as tornadoes destroyed homes in communities such as Lake Village, Indiana, and Aroma Park, Illinois. Simultaneously, school-related threats and bomb threats saw sharp increases this week. For instance, on March 11, two students were arrested at Adams City High School in Colorado after calling in false bomb and shooter threats. While gun violence overall saw a decline, there were eight mass shootings in the country within the last week, including one during the Bridge Crossing Jubilee in Selma, Alabama, that resulted in six victims. With St. Patrick's Day coming up, which has a precedent of mass shooting incidents, law enforcement departments across the country have been making preparations to ensure safe celebrations. Overall, the current domestic security landscape is defined by an intersection of school-targeted hoaxes, high-impact natural disasters, and impromptu gun violence.

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%