ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

August 15, 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 (EDT) on August 13, 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 Brief – Cumulative Energy and Food Crisis Inspiring Cyber Actors

Three simultaneous conflicts—the war in Iran, the Russia-Ukraine war, and Iran-allied Houthi attacks in the Red Sea—are converging with extreme weather to disrupt global energy and food supply chains. On the energy side, the fighting in Iran has kept oil prices elevated; meanwhile, Iran-allied Houthi rebels in Yemen have begun attacking tankers in the Red Sea, which had served as a backup export route since the war in Iran began. Ukrainian strikes on Russian ships and oil refineries have sharply limited Russian exports and led Russia to respond in kind with highly damaging strikes on Ukraine's port infrastructure. On the food side, these same conflicts are squeezing grain and fertilizer exports; Russia and Ukraine are leading grain exporters, while the Middle East is a fertilizer exporter. Lastly, a global heatwave is damaging crops across the world, pushing food prices to a three-year high while simultaneously triggering increased demand for air conditioning, further straining energy supplies. These overlapping shocks are set to ripple through global supply chains, lifting costs for fuel and food staples alike. Further, both geopolitically and financially motivated cyber threat actors are likely to view the affected sectors as vulnerable targets.

ZeroFox Intelligence Assessment – July 2026 Ransomware Wrap-Up

ZeroFox observed at least 776 separate ransomware and digital extortion (R&DE) incidents in July 2026, an increase of approximately 22 percent from June 2026. Additionally, July 2026 marked a 78 percent increase in R&DE incidents year-over-year from July 2025 and a 101 percent increase from July 2024. ZeroFox observed a decline in North America's global share of R&DE incidents for Q2 2026, with European organizations increasing their share. Overall, this trend continued into July 2026; North American targets saw a 12 percent decrease in year-over-year incidents from July 2025, suggesting threat actors are very likely expanding targeting efforts in other regions at a faster rate. The Gentlemen remained the most prominent R&DE collective in July 2026, accounting for at least 125 incidents; Qilin was the second most prominent with at least 121 incidents over the course of the month. Thus far, 2026 has seen an average of at least one new threat actor per week, and CRPx0 is very likely the latest new group to establish itself as a serious threat.

ZeroFox Intelligence Flash Report – Turkey, Saudi Arabia, and Pakistan Pact Reorders Middle East

On August 7, 2026, Saudi Arabia, Pakistan, and Turkey signed a mutual defense pledge, aligning three major Sunni Muslim countries amid concerns that the U.S.-Iran conflict could spread. The arrangement (known as the Mecca Joint Defense Agreement) does not include specifics on the commitments of each member, making their obligations for each others' defense unclear in the event of any particular military action. The treaty is likely equal parts mutual defense pact and wider alliance system designed to replace the U.S. force posture in the Middle East.

ZeroFox Intelligence Brief - Underground Economist: Volume 6, Issue 17

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

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

Delta Flight 591 Investigating Suspected Wi-Fi Spoofing Incident

What we know:

- A Delta Air Lines flight from Las Vegas to Atlanta, Flight 591, had an unauthorized Wi-Fi network appear onboard while several passengers were returning from the DEF CON hacker convention.

Background:

- One or more passengers are suspected to have conducted a Wi-Fi deauthentication attack to send fake disconnect messages to devices already connected to the real in-flight Wi-Fi and repeatedly knock them offline.
- Investigators are also examining reports of a fake network named “Delta WiFi Fast” possibly aimed at tricking other passengers into connecting to it.

Analyst note:

- Threat actors are also likely to attend hacking conventions such as DEF CON because the events provide opportunities to test tools and sharpen skills.
- If deliberate, the activity was likely opportunistic and financially motivated, with the rogue wireless network enabling credential harvesting and other short-duration access opportunities against DEF CON attendees and other passengers on the flight.

Extortion Group BlackFile Reportedly Linked to Cyberattacks Against Finance Sector

What we know:

- A recent series of cyberattacks targeting hedge funds, private equity firms, and financial organizations at Wall Street has reportedly been attributed to the BlackFile extortion group.
- In May 2026, BlackFile had announced that it was rebranding under the name “Redact”.

Background:

- BlackFile also reportedly operates under various public brands such as Pink, Helix, and Falcon.

- In the recent campaign, BlackFile operators reportedly contacted employees on personal mobile phones spoofing corporate help desks and directed them to adversary-in-the-middle (AitM) phishing sites that stole single sign-on (SSO) credentials and session cookies in real time.
- Automated tools then exfiltrated data across all linked cloud platforms while security notifications were deleted to delay detection.

Analyst note:

- The public attribution of BlackFile's infrastructure and tactics is likely to prompt the group to rotate domains and rebrand.
- However, because the operation very likely depends on human operators conducting live vishing (voice phishing) calls, operational disruption to the threat group's activity is unlikely without direct law enforcement action against the individuals.

U.S. Defense Manufacturer IEH Corporation Hit by Phishing Attack

What we know:

- U.S.-based defense and aerospace supplier IEH Corporation has disclosed a security breach after threat actors used an alias to trick an employee via a phishing email.

Background:

- IEH Corporation manufactures connectors used in aircraft, fighter jets, missiles, satellites, and other defense systems, including the PATRIOT, AMRAAM, and THAAD programs.
- Threat actors reportedly accessed mailbox content, including customer communications, engineering documentation, and export-controlled technical information, with no reported evidence of data exfiltration or operational disruption.

Analyst note:

- Threat actors are likely to conduct further email-based reconnaissance, monitor communications tied to defense programs, procurement, and supply chain activity, and identify additional accounts or systems to launch spear phishing campaigns against downstream aerospace partners and government entities.

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 new vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue on August 7 and August 11, 2026. Additionally, on August 7 and August 11, 2026, CISA released four Industrial Control Systems (ICS) advisories. Flaws in the Connective digital identity system, a browser extension used by over two million users in Belgium including major banks and government agencies, enables malicious websites to communicate with the eID application without proper authorization. Additionally, a zero-day vulnerability in Metabase under active exploitation enables threat actors to inject arbitrary Structured Query Language (SQL) into the application database, grant themselves administrator access, and exfiltrate customer data. Cisco has released patches for 24 vulnerabilities across Catalyst SD-WAN, IOS XE, Secure Firewall Management Center (FMC), and Integrated Management Controller (IMC).

HIGH

CVE-2026-68820

What happened: CVE-2026-68820 is among the 421 vulnerabilities Microsoft patched for August 2026 Patch Tuesday.

- **What this means:** The flaw is an elevation-of-privilege flaw in Windows Ancillary Function Driver for WinSock that is being actively exploited and can enable unauthenticated attackers to gain SYSTEM-level access.
- **Affected products:**
  - The affected products are listed in the advisory.

CRITICAL

CVE-2026-71362

What happened: CVE-2026-71362 is an authorization flaw in Adobe Commerce and Magento that can enable unauthenticated customer account takeover.

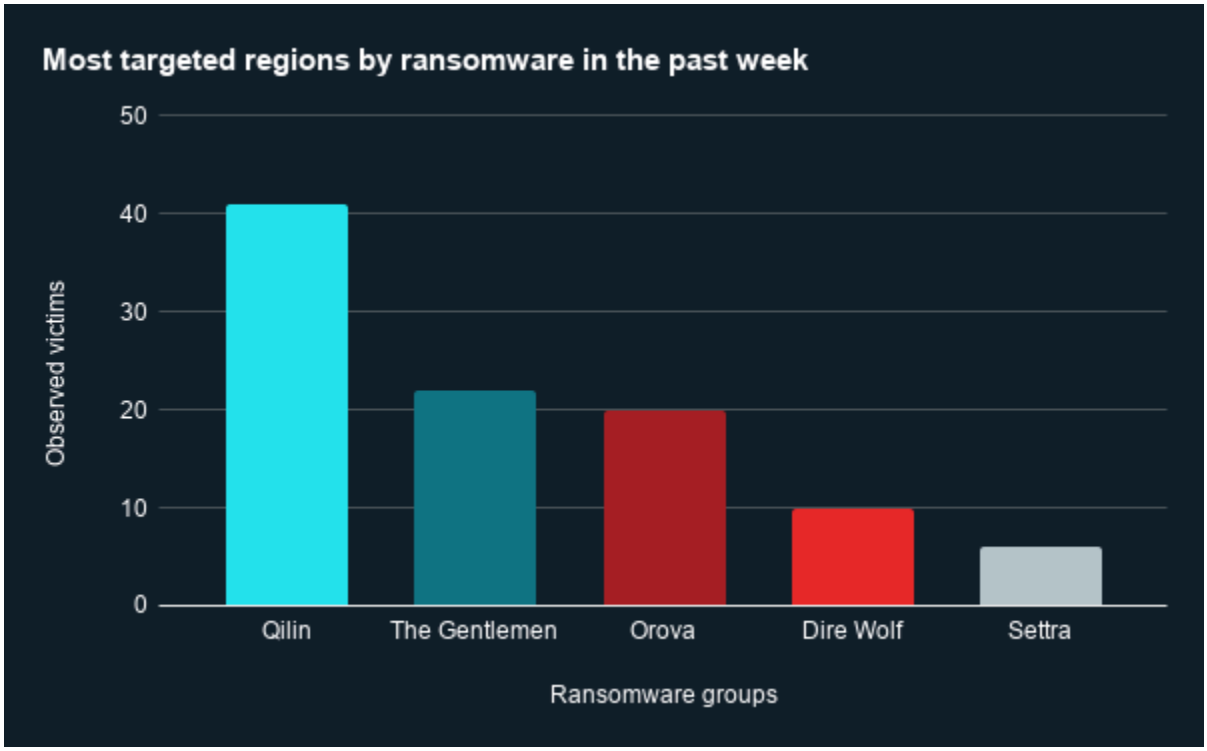
- **What this means:** The vulnerability can enable attackers to manipulate customer session identity and switch to another customer's account, which can potentially expose private customer data.
- **Affected products:**
  - The affected products are listed in the advisory.

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

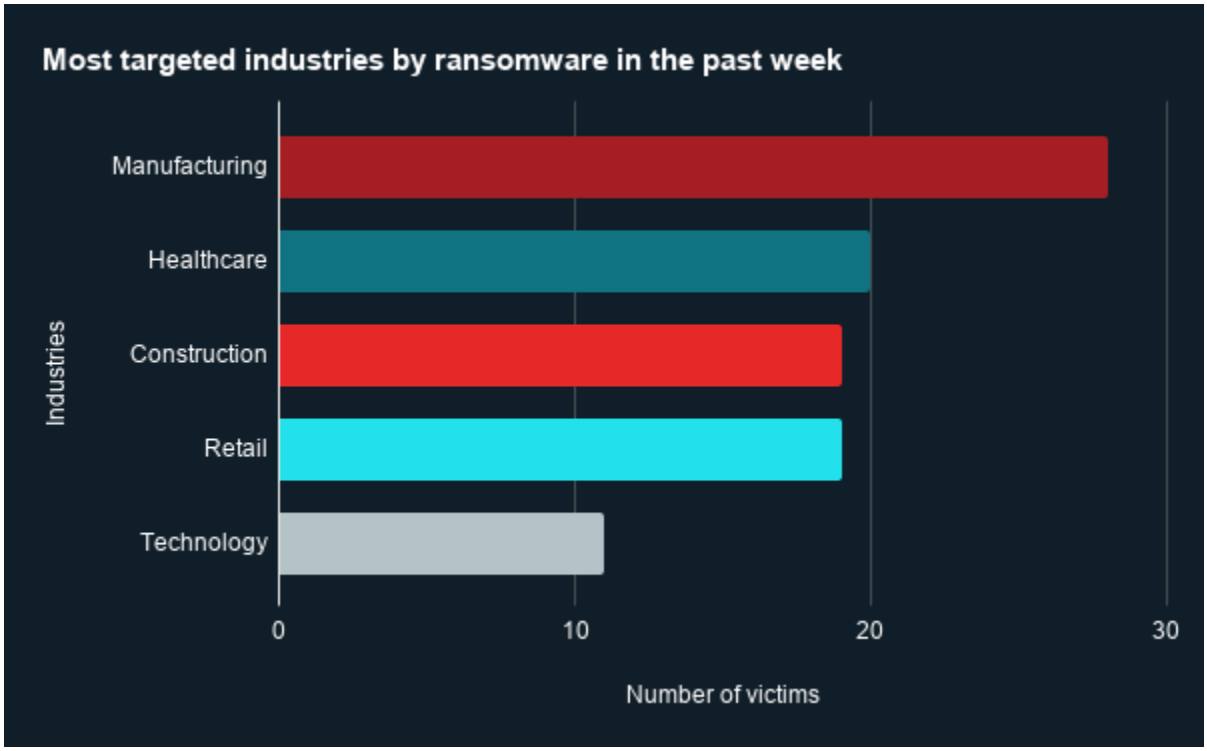
Ransomware Group, Industry, and Regional Trends

Last week in ransomware: In the past week, Qilin, The Gentlemen, Orova, Dire Wolf, and Settra were the most active ransomware groups. ZeroFox observed close to 156 ransomware victims disclosed, most of whom were located in North America. The Qilin ransomware group accounted for the largest number of attacks, followed by The Gentlemen.



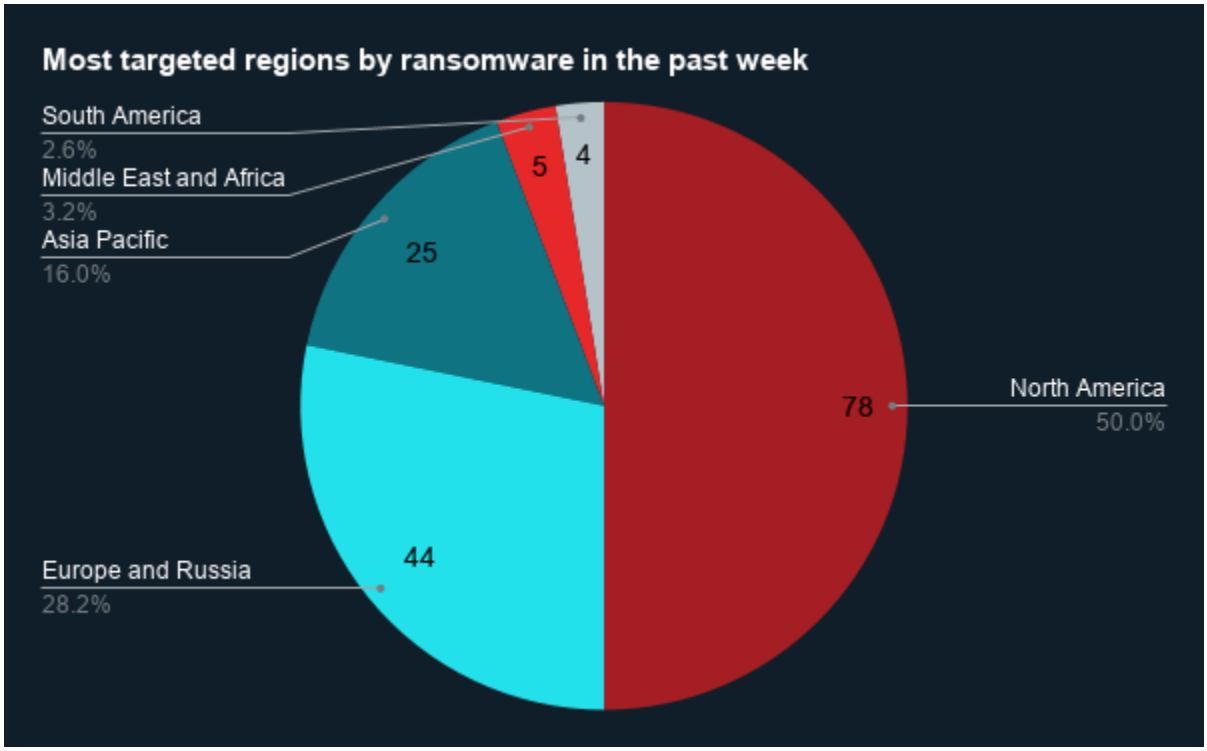
Source: ZeroFox Internal Collections

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



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 78 ransomware attacks observed in North America, while Europe and Russia accounted for 44, Asia-Pacific for 25, the Middle East and Africa for five, and South America for four.



Source: ZeroFox Internal Collections

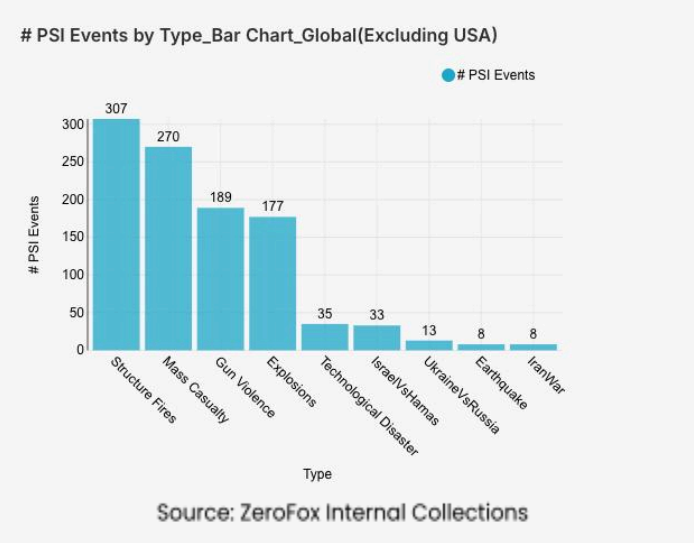
Notable Data Breaches Observed

Targeted Entity	Wesco	CEVA Logistics	The Shrewsbury and Telford Hospital Charity
Compromised Entities/Victims	Customer and employee records (2.6 million records claimed)	Eight European warehouses	Details related to donors, supporters, and community members
Compromised Data Fields	Customer and employee personally identifiable information (PII), account information, and customer relationship management (CRM) profiles	PII of customers, including delivery address	PII, membership details, and donation information
Suspected Threat Actor	ExfilSquad	CoinbaseCartel	N/A
Country/Region	United States	Europe	United Kingdom
Industry	Supply Chain	Logistics	Healthcare
Possible Repercussions	Identity theft, targeted phishing, social engineering, and unauthorized account access	Cargo theft, phishing, social engineering, and supply chain operational disruption	Phishing, social engineering, and impersonation attempts

Three major breaches observed in the past week

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

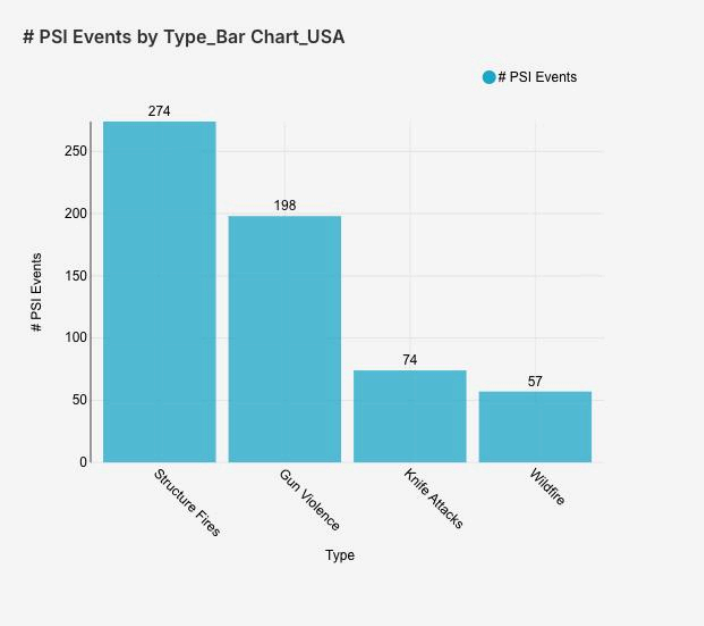


Physical Security Intelligence: Global

What happened: Excluding the United States, there was no change in the percentage in mass casualty events this week compared to the previous week, with the top contributing countries or territories being Mexico, Colombia, and Yemen, in that order. Approximately 66 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 24 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict decreased by 23 percent from the previous week, and alerts related to the war in Iran decreased by 65 percent. Events related to Russia's war with Ukraine decreased by 35 percent. The top three most-alerted subtypes were structure fires, which saw a 31 percent increase from the previous week; gun violence, which decreased by 23 percent; and explosions, which decreased by 3 percent. Notably, earthquakes increased by 14 percent; consequently, technological disasters increased by 119 percent.

- **What this means:** This week's mass casualty landscape held steady overall, but the individual events behind the numbers were severe. Colombia experienced a 7.4 magnitude earthquake on August 10 that killed at least 265 people, injured more than 3,700, and left over 4,100 still missing, making it the country's most powerful earthquake in a decade. The incident also collapsed buildings in Pereira and a hospital wing in Cali, explaining the surge in earthquake and technological-disaster-linked alerts noted in the data. Yemen contributed heavily to the number of explosions this week, with Houthi forces launching ballistic missile and drone strikes on the Red Sea port of al-Makha and the city of Marib following an August 9 barrage that killed seven people. The number of alerts related to Israel-Hamas dropped under the fragile ceasefire, and Iran-related alerts also fell alongside ongoing U.S.-mediated talks, even as Israel kept striking Gaza and Lebanon. Together, these events illustrate how explosions, natural disasters, and entrenched regional conflicts continue to drive the bulk of global mass-casualty alerting.

Physical Security Intelligence: United States



What happened: In the past week, the top three most-alerted incident subtypes were structure fires, gun violence, and knife attacks. Gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim, knife attacks include confirmed stabbings or slashings, and structure fires are fires that affect man-made buildings. The top two states with the most gun violence alerts were Ohio and Illinois, which together made up 23 percent of this week's nationwide total. Gun violence across the United States overall decreased by 3 percent from the week prior. Knife attacks increased by 30 percent, and the top contributing states were California and New York. Structure fires increased by 6 percent, and the top two states for this subtype were New York and California. Notably, wildfires increased by 63 percent nationwide.

- **What this means:** Over the past week, gun violence remained concentrated in Illinois, where Chicago recorded at least five people killed and 14 wounded in a single weekend of shootings from August 7–10. Multi-victim knife violence also surfaced this week; in Hopkins, Minnesota, three people, including a child, were fatally stabbed at a home daycare on August 12, with six other children present but unharmed. Structure fires were reflected in an August 11 incident at a 10-story senior housing building in San Francisco, California, where a fire broke out on the eighth floor and injured one person. Meanwhile, wildfire activity accelerated sharply in California, where the Bug Fire ignited on August 8 in Lassen and Sierra counties and had already grown to over 70,000 acres as the state worked to manage 17 active large fires. Taken together, these examples illustrate persistent, multi-victim gun violence, sporadic but severe multi-victim knife attacks, elevated structure fire activity, and a sharp nationwide jump in wildfires.

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%