ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

AUGUST 29, 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 27, 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 – ZeroBytes Targets French Agencies

On August 13, 2026, threat actor "ZeroBytes" posted on the dark web forum PwnForums claiming to have breached France's Ministry of National Education; several days later, the group reposted the claim on its public X profile. The Ministry of National Education disclosed a breach on July 25, 2026, but claims that no student information, bank details, or passwords were stolen in the breach. This is the largest breach claimed by ZeroBytes and the second French central-government-body victim the group has claimed in under two months. There is a roughly even chance the threat actor maintains access to the data. If ZeroBytes' claim is legitimate, the group will almost certainly sell that access in addition to the exfiltrated data. ZeroBytes is almost certain to continue targeting French government agencies, and there is a roughly even chance the group will continue using social engineering and credential stuffing to gain ever-increasing levels of access to more secure data.

ZeroFox Intelligence Flash Report – Cl0p Shifts from Personal Data to Intellectual Property Theft

Between August 14 and August 19, 2026, Cl0p posted 43 organizations to its dark web leak site and began issuing extortion demands tied to data allegedly stolen from internet-exposed server instances of product lifecycle management platforms Windchill and FlexPLM, both of which are made by software-as-a-service (SaaS) company PTC, Inc. The type of data targeted and the small population of Windchill and FlexPLM users mark a significant change for Cl0p and likely suggests the threat actor is entering a new phase of operations. Cl0p was first observed in 2019 and has shifted its operations twice before: first from strict encryption to double extortion in 2020 and then to mass data exfiltration in 2021. Both prior significant operational changes marked a new phase of threat activity and sustained campaigns. Cl0p is likely in the early stages of a new campaign targeting engineering-focused intellectual property on vulnerable product lifecycle management servers.

ZeroFox Intelligence Brief – U.S. China Tensions Simmer Ahead of Key Summit

The ZeroFox 2026 Geopolitical Forecast Assessment projected that the United States and China would likely avoid major policy decisions in 2026 that reignited their 2025 trade war, although relations between the United States and China were forecast to remain acrimonious over the long term. In the last few weeks, both sides have carried out a range of trade restrictions ahead of a key September

summit between U.S. President Donald Trump and his Chinese counterpart, Xi Jinping. These measures are unlikely to derail the truce agreed to in October 2025 that halted the rapid tariff escalation between the two nations. Individually, they have likely been structured to maintain the truce by not causing immediate economic damage. However, the restrictions likely signal areas where the two sides will diverge more seriously in the coming years.

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

Norway's Government Digital Infrastructure Hit by DDoS

What we know:

- A large distributed denial-of-service (DDoS) attack has reportedly disrupted Norway's shared government digital infrastructure, affecting public sector services operated by the Norwegian Digitalization Agency (Digdir) and its operations provider, Vivicta.

Background:

- Digdir operates critical shared government infrastructure including public service logins, electronic IDs, secure digital mail, and data exchange between agencies.
- Several services were completely unavailable for short periods.
- Digdir confirmed no security breach or compromise of personal data occurred.
- Downstream services relying on Digdir's infrastructure also reported login issues and operational disruptions.

Analyst note:

- The targeting of a European country's centralized digital government infrastructure likely reflects Russian hybrid warfare tactics.
- Similar incidents have been documented against North Atlantic Treaty Organization (NATO) member countries and other European nations for their support of Ukraine.
- Government digital infrastructure is likely to remain an attractive target for state-aligned actors seeking to disrupt crucial communications and/or steal valuable data for intelligence-gathering.

ShinyHunters Claims Major Breach Targeting U.S. Data Center Operator

What we know:

- Threat group ShinyHunters has claimed to have targeted a major U.S. data center operator and has demanded USD 13 million in ransom.
- As of writing, the group has not published any sample data.

Background:

- The group claims to have stolen close to 13 million Salesforce records and hundreds of gigabytes of SharePoint data from the data center operator.
- The stolen information allegedly includes employees' personally identifiable information (PII), contracts, facility floor plans, electrical diagrams, access-control records, physical key inventories, security documentation, and credential-related data.
- The victim organization's customers include Meta, AT&T, and others.

Analyst note:

- If the claims are legitimate and the data is leaked following failed negotiations, the exposed information is likely to be valuable to hacktivists and nation-state actors, particularly given the heightened physical and cyber threat activity targeting critical infrastructure owing to the Iran conflict.
- Detailed information on data center layouts, access controls, and power and cooling systems is likely to provide useful intelligence for reconnaissance or disruption attempts.

China-Linked Threat Group Targets 170,000 Web Servers in AI-Assisted Attacks

What we know:

- China-linked threat group UAT-10147 is reportedly integrating artificial intelligence (AI) across its attack chain, using AI-powered tools such as DeepAudit and PentestGPT for vulnerability scanning, exploit development, reconnaissance, payload generation, troubleshooting, and post-exploitation.

Background:

- UAT-10147 is reportedly targeting web servers at scale, with a list of approximately 170,000 URLs spanning multiple countries, including the United States, India, the United Kingdom, Germany, and the Netherlands.
- The group combines exploitation with persistent access and data theft, deploying web shells and malware strains such as BadIIS, Quasar RAT, and SPECTRE.

Analyst note:

- UAT-10147's activity suggests AI is increasingly being used to support the operational side of cybercrime rather than solely to develop malware or code.
- The target pool of roughly 170,000 URLs is likely to have been enabled by AI usage.

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 11 new vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue on August 21, August 24, August 25, and August 26, 2026. Additionally, CISA released eight Industrial Control Systems (ICS) advisories on August 25, 2026. An unpatched missing authentication flaw in Calix residential routers (CVE-2026-75501) enables unauthenticated remote attackers to manipulate port-forwarding rules via UPnP control endpoints. Google has released Chrome 152 with patches for 327 vulnerabilities, including 10 critical and 61 high-severity flaws. Most of the critical vulnerabilities are use-after-free issues affecting components such as Angle, Aura, Chromecast, Views, and SafeBrowsing.

HIGH

CVE-2026-75149

What happened: This is a code injection vulnerability in Marimo that could enable the execution of an attacker-supplied Model Context Protocol (MCP) command as a local subprocess when a malicious notebook is opened in edit mode.

- **What this means:** The vulnerability requires user interaction but does not require attacker authentication. Successful exploitation can lead to arbitrary command execution on the targeted system.
- **Affected products:**
  - Marimo versions prior to 0.23.15

CRITICAL

CVE-2026-72529

What happened: This is an unauthenticated script execution vulnerability in the TrueConf Server self-hosted communications platform.

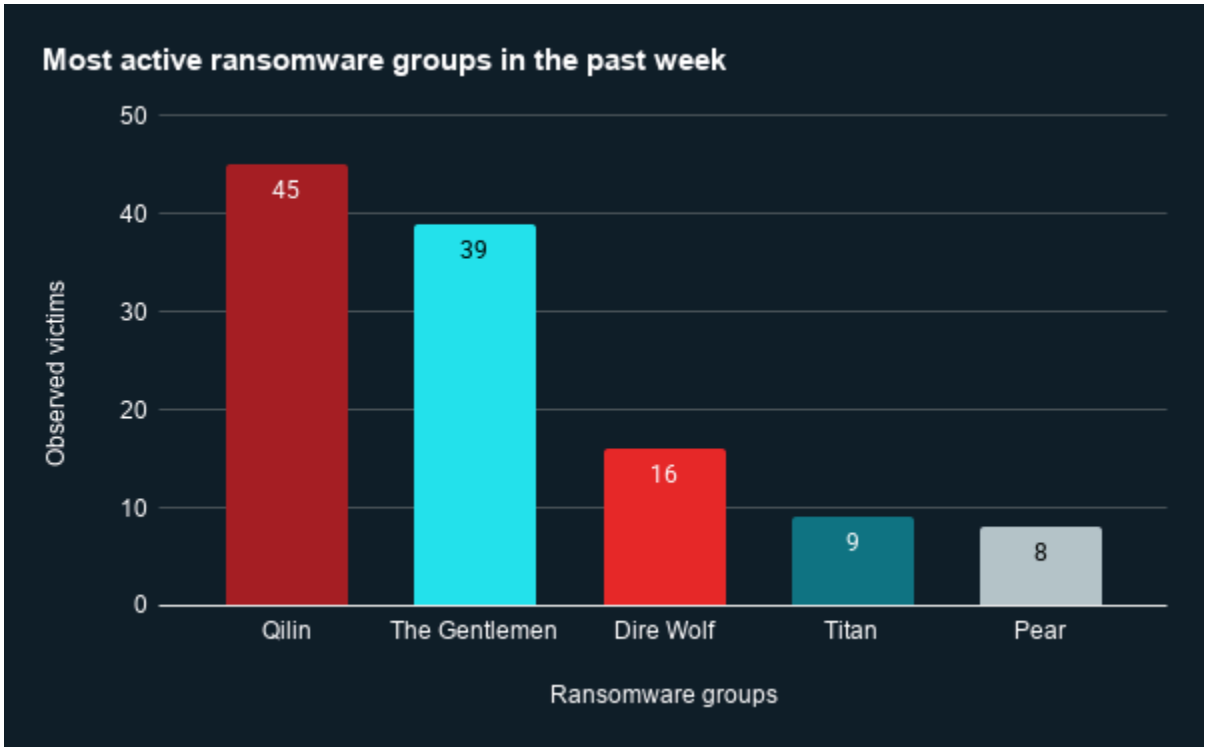
- **What this means:** A remote unauthorized attacker with network access via TCP port 4307 can call an undocumented function to achieve arbitrary code execution as NT AUTHORITY\SYSTEM.
- **Affected products:**
  - TrueConf Server versions prior to 5.3.9, 5.4.9, and 5.5.5

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

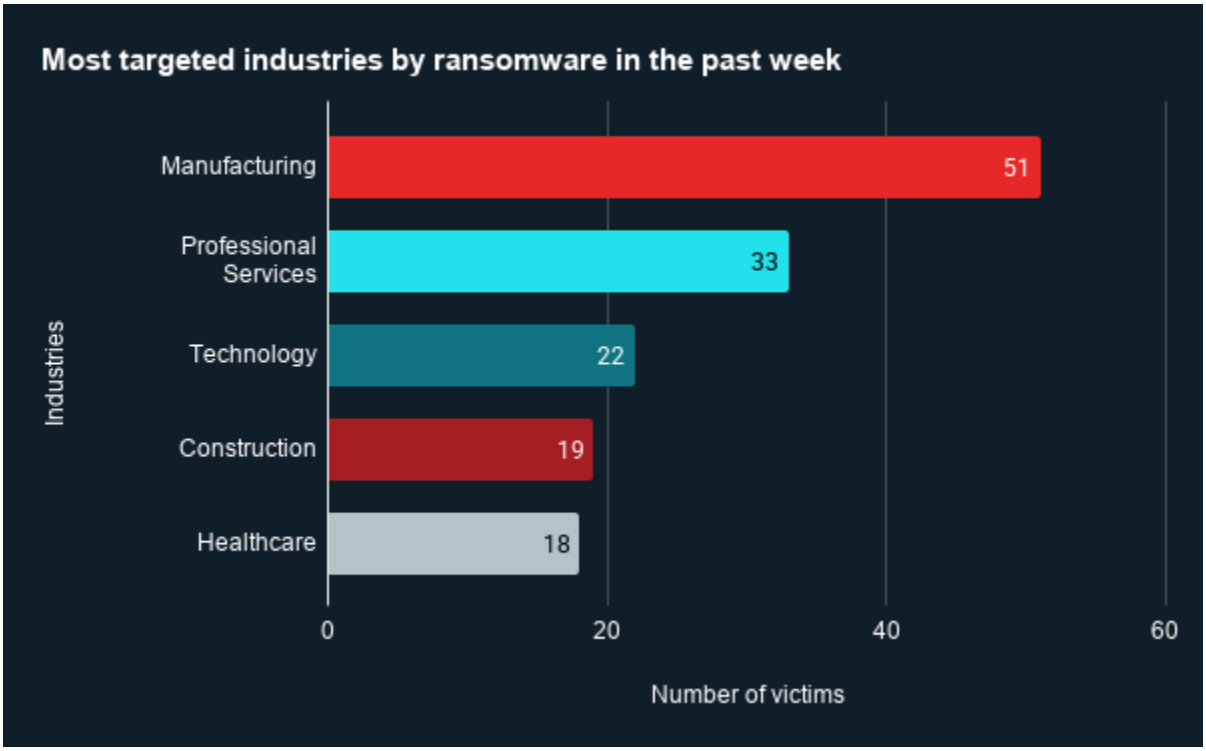
Ransomware Group, Industry, and Regional Trends

Last week in ransomware: In the past week, Qilin, The Gentlemen, Dire Wolf, Titan, and Pear were the most active ransomware groups. ZeroFox observed approximately 243 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.



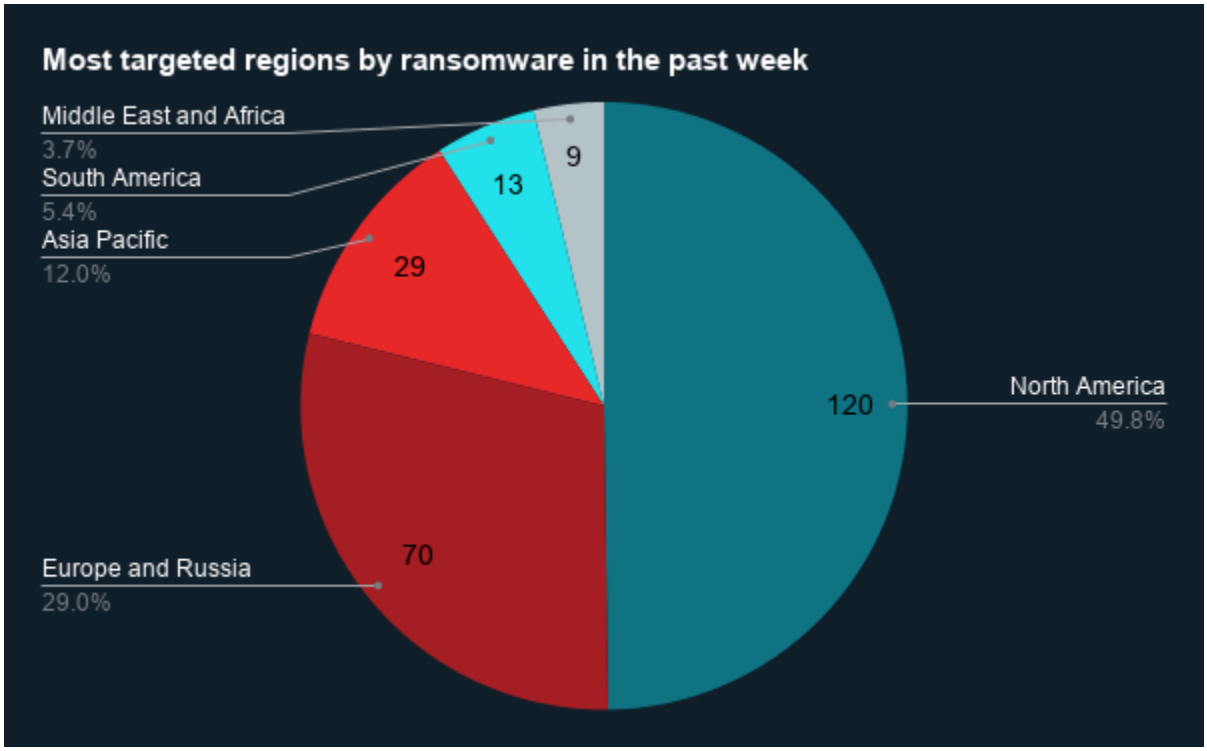
Source: ZeroFox Internal Collections

Industry ransomware trends: In the past week, ZeroFox observed that manufacturing was the industry most targeted by ransomware attacks, followed by 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 120 ransomware attacks observed in North America, while Europe and Russia accounted for 70, Asia-Pacific accounted for 29, South America for 13, and Middle East and Africa for nine.



Source: ZeroFox Internal Collections

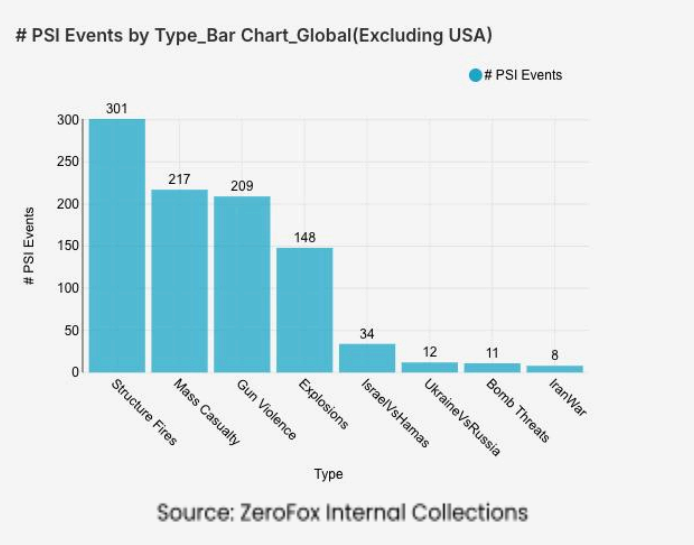
Notable Data Breaches in the Past Week

Targeted Entity	Mercor	Nutex Health	Connecticut Medicaid provider portal
Compromised Entities/Victims	4 TB of data pertaining to users, candidates, and potentially client organizations	Nutex Health's network and server	Approximately 41,000 HUSKY Health/Connecticut Medicaid members
Compromised Data Fields	User logs, prompts, user accounts and roles, database contents, and source code	Potentially patient, employee, provider, business, financial, and intellectual property information.	Member names, provider payment or Medicaid claim ID numbers, service dates, billing details, payment amounts, and information related to other health insurance policies (including group and policy numbers).
Suspected Threat Actor	N/A	N/A	N/A
Country/Region	United States	United States	United States
Industry	Technology	Healthcare	Healthcare
Possible Repercussions	Phishing, impersonation, identity theft, and targeted social engineering, exposed, confidential conversations, hiring activity, and internal workflows.	Exposure of sensitive healthcare and employee information; privacy violations; and exfiltration of business, financial, or intellectual property information	Identity fraud, insurance fraud, targeted phishing, or social engineering

Three major breaches observed in the past week

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

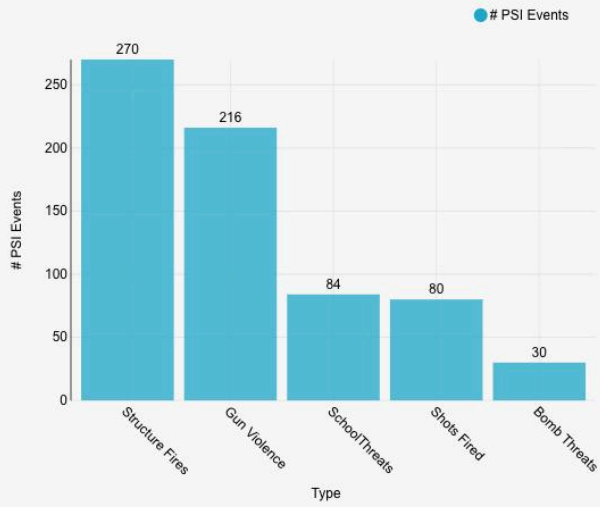


Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 9 percent decrease in mass casualty events this week from the previous week, with the top contributing countries or territories being Mexico, Ukraine, and India, in that order. Approximately 68 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 increased by 10 percent from the previous week, and alerts related to the war in Iran increased by 33 percent. Events related to Russia's war with Ukraine decreased by 33 percent. The top three most-alerted subtypes were structure fires, which saw a 7 percent decrease from the previous week; gun violence, which decreased by 3 percent; and explosions, which decreased by 15 percent. Notably, bomb threats increased by 57 percent.

- **What this means:** This week's slight drop in mass casualty events was led by Mexico, Ukraine, and India, with explosions accounting for roughly two-thirds of incidents. In Mexico, cartel violence remains active; on August 26, security forces in Oaxaca killed a leading figure in a criminal cell tied to ongoing Pacific coast violence. Ukraine's war-related alerts declined, thoughRussia launched 162 drones at Ukraine on August 26, striking 18 locations; additionally, separate attacks on August 25 killed one and injured 12 in Kherson Oblast. The rise in Israel-Hamas alerts tracks a fragile ceasefire; on August 24, Israeli strikes killed at least four people in Gaza, causing the United Nations (UN)'s Gaza envoy to warn that continued strikes risk a "point of no return" for the truce. Meanwhile, the jump in Iran-war alerts coincides with Iran's continued closure of the Strait of Hormuz despite de-escalation talks. India contributed to the sharp rise in bomb threats this week, as a bomb threat letter found aboard an IndiGo flight in Karnataka on August 26 prompted a security response before being declared a hoax. Overall, global physical security conditions were mixed, with declines in some conflict zones offset by intensifying flashpoints in the Middle East.

Physical Security Intelligence: United States



Source: ZeroFox Internal Collections

What happened: In the past week, the top three most-alerted incident subtypes were structure fires, gun violence, and shots fired. Gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim, shots fired are shootings with no confirmed victims, and structure fires are fires that affect man-made buildings. The top two states with the most gun violence alerts were Illinois and California, which together made up 24 percent of this week's nationwide total. Gun violence across the United States overall increased by 8 percent from the week prior. Shots fired alerts declined by 1 percent, and the top contributing states were Illinois and Ohio. Structure fires increased by 3 percent, and the top two states for this subtype were New York and California. Notably, school-related threats nationwide increased by 29 percent, and bomb threat numbers doubled compared to the previous week.

- **What this means:** This week's data reflects national trends already visible on the ground. Gun violence and structure fires converged in a single, particularly severe event in Billings, Montana, on August 23, where a gunman opened fire inside a home before setting it ablaze, killing eight victims, including four children. Consistent with the reported spike in school-related threats and bomb threats, multiple U.S. campuses were evacuated this week over unconfirmed explosive threats, including schools in Buckeye, Arizona; Challis, Idaho; Leesville, Louisiana; Texarkana, Texas; and Lexington, Kentucky; none of these yielded a confirmed device, mirroring the hoax-heavy pattern typically seen in bomb threat surges at the start of the school year. Illinois again anchored the week's gun violence totals, with Chicago police reporting at least four people killed and 17 wounded over the August 22–24 weekend alone, underscoring the city's continued status as a top contributor to national shots-fired and gun violence figures. Overall, domestic physical security this week remained under heightened strain, driven by a mix of lethal armed violence, fatal structure fires, and a surge in disruptive but largely unconfirmed school and bomb threats.

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%