ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

December 20, 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 18, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Weekly Intelligence Brief

This Week's ZeroFox Intelligence Reports

Geopolitical Forecast Assessment 2026

ZeroFox assesses that the most significant geopolitical shift of 2025 was the Trump administration's restructuring of U.S. national security priorities to curtail the United States' role as a primary enforcer and financier of international security commitments. Therefore, in 2026, the greatest geopolitical impact will likely stem from these changing priorities. In 2026, the United States will very likely redirect further resources towards establishing a secure foothold in Latin America, countering Chinese influence, and tackling narcotrafficking and immigration priorities. The shifting U.S. focus towards Latin America will likely coincide with the region electing more political leaders focused on addressing crime and security concerns. With the United States less focused on Eastern Hemisphere security, there will very likely be an increase in armed conflict and social unrest there—particularly in southeast and west Asia and parts of Africa. Settlements in the Israel-Hamas and Russia-Ukraine wars, if reached, are unlikely to hold in the long term—a trend that is likely to apply to other conflicts where U.S. interests have diminished. U.S. tariffs were very likely the most important supply chain development of 2025. In 2026, affordability and limiting the inflationary impact of U.S. tariffs will likely be prominent supply chain concerns. Unlike in 2025, the United States and China are likely to avoid major policy decisions that reignite the trade war in 2026. However, over the long term, U.S-China relations will likely remain acrimonious.

ZeroFox Intelligence Brief - Underground Economist: Volume 5, Issue 25

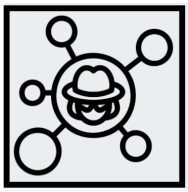
The Underground Economist is an intelligence-focused series illuminating Dark Web findings in digestible tidbits from our ZeroFox Dark Ops intelligence team.

ZEROFOX®

Weekly Intelligence Brief

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings



French Interior Ministry Hacked as BreachForums Re-emerges

What we know:

- The French Interior Minister confirmed a cyberattack targeting the Ministry of the Interior's email servers, stating that some files were accessed.
- Around the same time, a BreachForums administrator, "Indra", claimed responsibility for the attack and stated data linked to more than 16 million individuals were stolen from French law enforcement databases, though these claims remain unverified.

Background:

- French authorities later arrested a 22-year-old suspect in connection with the intrusion, which is being investigated as unauthorized access to a state-run system conducted as part of an organized group.
- Indra's announcement coincided with the brief reappearance of BreachForums under a new domain, where the group asserted its return and threatened to release evidence of the breach before the site went offline for "technical maintenance."

Analyst note:

- The coincidence likely suggests that BreachForums' admin's claims are opportunistic and inflated, intended to draw attention to the forum's return and gain credibility.
- The arrest does not likely confirm the scale or nature of Indra's claims of possessing data, as it remains unclear, as of reporting, whether the suspect is directly connected to the forum's administrators.

Legitimate PayPal Emails Used in Social Engineering Attacks

What we know:

- Scammers are abusing PayPal's legitimate Subscriptions feature to send real PayPal emails that look like fake purchase confirmations.

- By reportedly manipulating the Customer Service URL field in a subscription, they embed scam text claiming an expensive device purchase and listing a fake “PayPal support” phone number.

Background:

- The emails bypass spam filters, as they are sent from service@paypal[.]com and pass email authentication protocols.
- The scammers then forward these legitimate emails to targets via a mailing list.

Analyst note:

- Since threat actors are successfully abusing PayPal’s legitimate platform functionality to deliver phishing emails, they are likely to test and exploit similar automated workflows on major e-commerce and payment platforms to replicate the attack.

CISA Releases Guide for Stadium and Arena Owners Ahead of Major Events

What we know:

- The Cybersecurity and Infrastructure Security Agency (CISA) has released a guide for stadium and arena owners and operators to help them mitigate the consequences of potential cyber and physical disruptions to four critical lifeline sectors (energy, water and wastewater systems, communications, and transportation).

Background:

- The guide is tailored for major public gathering events, such as FIFA World Cup 2026, America250, and 2028 Summer Olympics.
- It aims to address potential disruptions such as cyberattacks, physical attacks, or aging infrastructure.
- Venue operators are advised to understand how critical infrastructure systems and assets are interconnected via dependencies.

Analyst note:

- CISA’s mention of upcoming major events in the United States likely indicates that there is a risk of threat actors, including nation-state actors, targeting venues and critical infrastructure during the event period with various types of cyberattacks.

Exploit and Vulnerability Intelligence

Exploit and Vulnerability Intelligence Key Findings

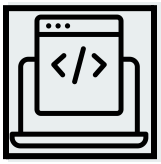
In the past week, ZeroFox observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in technology, software development, and critical infrastructure. CISA added six vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on December 15, December 16, and December 17 and released six industrial control advisories. The React2Shell vulnerability (CVE-2025-55182) is still being exploited; in the past week, a ransomware gang exploited the vulnerability to obtain initial access to corporate networks and deploy file-encrypting malware. Researchers have also tracked Chinese state-linked actors exploiting this bug in several campaigns. Hackers are exploiting two Fortinet vulnerabilities (CVE-2025-59718 and CVE-2025-59719) across multiple products to gain unauthorized admin access and steal system configuration files. Both Apple and Google urgently released patches to address zero-day vulnerabilities that were actively exploited in "sophisticated" real-world attacks. A high-severity vulnerability (CVE-2025-34352) found in the JumpCloud Remote Assist Windows agent enables a standard user on a company device to gain full, persistent control.

CRITICAL

CVE-2025-20393

What happened: Attackers are actively exploiting this unpatched, maximum-severity Cisco AsyncOS zero-day against Secure Email Gateway and Secure Email and Web Manager appliances with exposed Spam Quarantine features. Researchers have linked the campaign to UAT-9686, a Chinese-nexus Advanced Persistent Threat (APT).

- **What this means:** Threat actors are likely to exploit this bug to target organizations running vulnerable systems for full system takeover and long-term stealth access. Rebuilding compromised appliances is likely the only way to fully remove the attacker's persistence.
- **Affected products:**
  - Physical and virtual Cisco Secure Email Gateway
  - Physical and virtual Cisco Secure Email and Web Manager appliances



MEDIUM

CVE-2025-40602

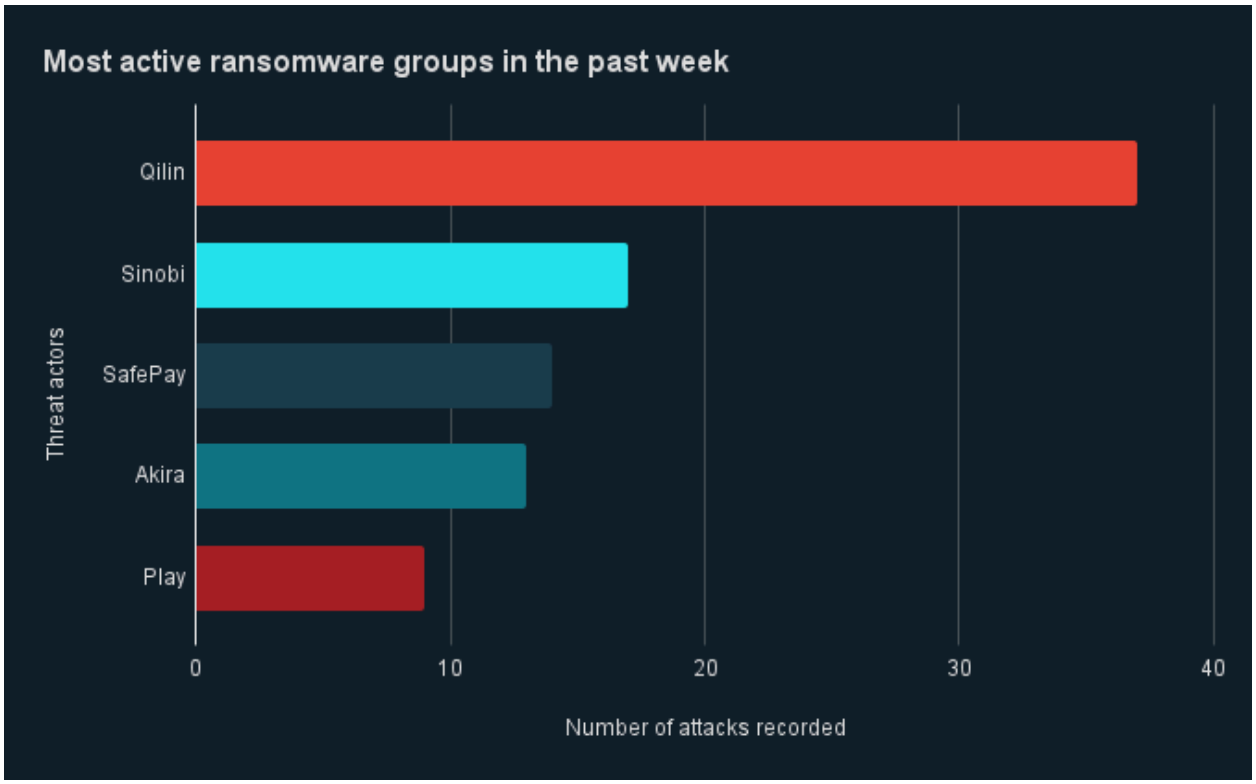
What happened: SonicWall has issued an urgent advisory asking customers to patch a newly disclosed SMA1000 Appliance Management Console privilege-escalation flaw. This bug was chained with a previously fixed critical pre-auth bug in real-world zero-day attacks to give remote, unauthenticated attackers root-level command execution on exposed devices.

- **What this means:** Any organization running an unpatched, internet-facing SMA1000 risks attackers moving from zero access to complete control of the device, effectively turning a Virtual Private Network (VPN) gateway into an entry point inside the network. With hundreds of exposed appliances and SonicWall repeatedly targeted over the past year, patch delays invite fast, opportunistic attacks rather than rare, highly sophisticated ones.
- **Affected products:**
  - SMA1000 12.4.3-03093 (platform-hotfix) and earlier versions
  - SMA1000 12.5.0-02002 (platform-hotfix) and earlier versions

Ransomware and Breach Intelligence

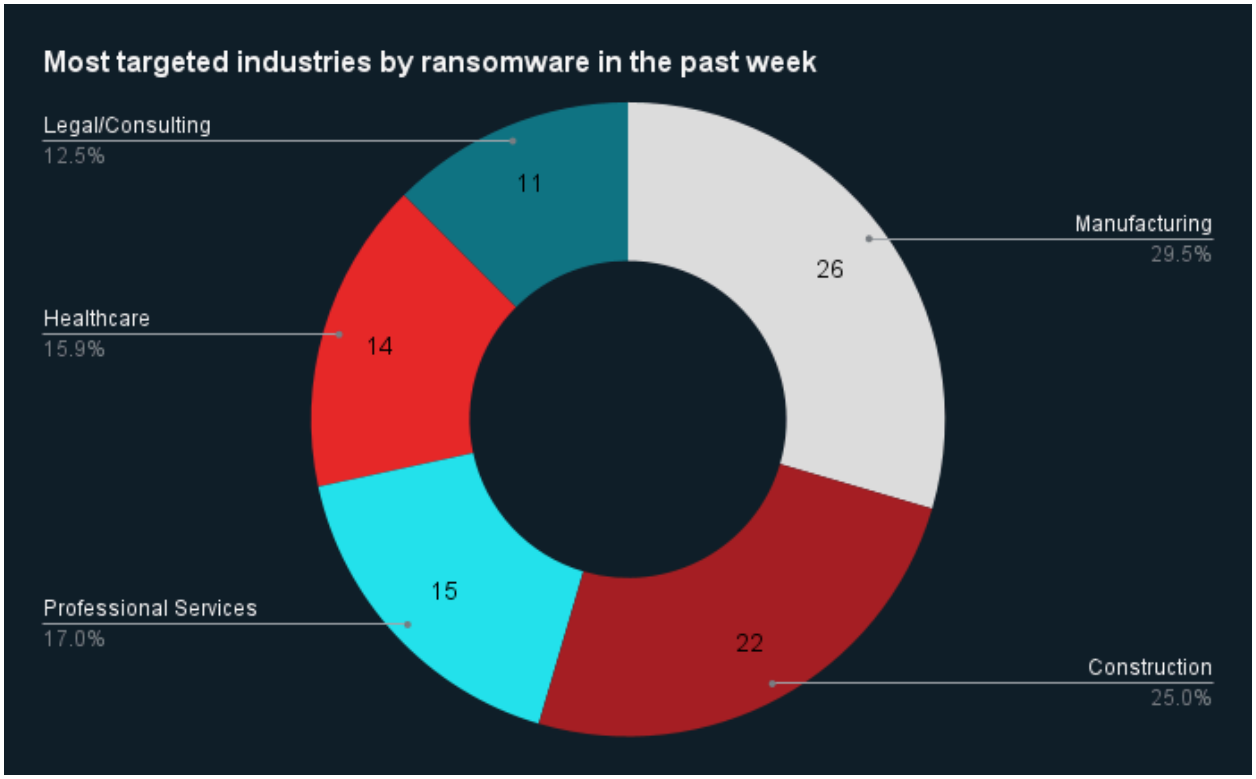
Ransomware and Breach Intelligence Key Findings

Ransomware Trends: Groups, Industry, and Region



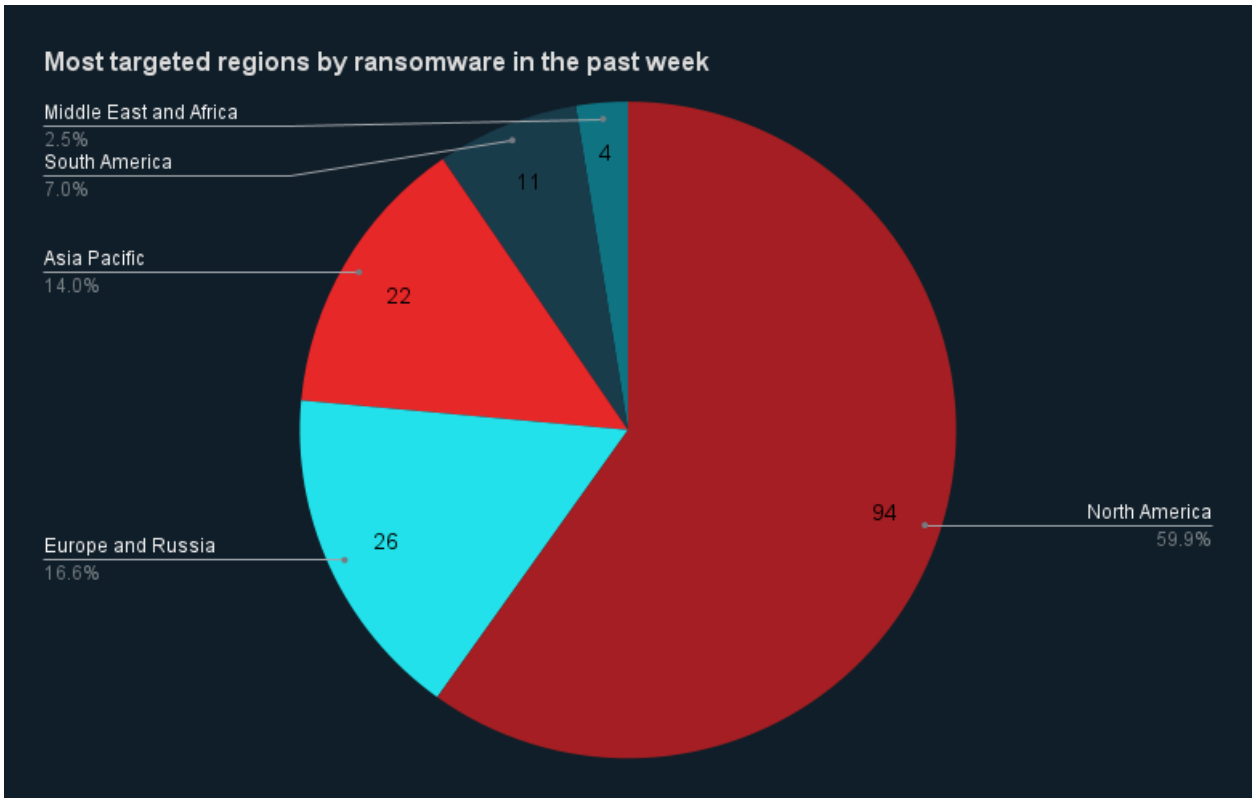
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Qilin, Sinobi, SafePay, Akira, and Play were the most active ransomware groups. ZeroFox observed close to 132 ransomware victims disclosed, most of whom were located in North America. The Qilin ransomware group accounted for the largest number of attacks, followed by Sinobi.



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 construction.



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 94 ransomware attacks observed in North America, while Europe and Russia accounted for 26, Asia Pacific for 22, South America for 11, and Middle East and Africa for four.

Major Data Breaches Reported in the Past Week

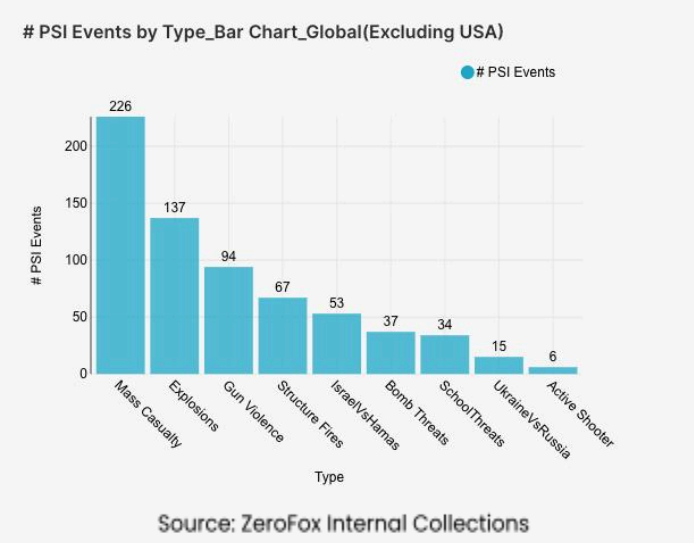
Targeted Entity	700Credit	Pornhub	SoundCloud
Compromised Entities/victims	5.6 million customers	Premium subscribers	User accounts
Compromised Data Fields	Names, addresses, dates of birth, and Social Security numbers (SSNs)	Reportedly, email addresses, location, activity type such as videos and channels watched, keywords, and date and time	Email addresses and mostly publicly visible profile information
Suspected Threat Actor	N/A	ShinyHunters	N/A
Country/Region	United States	N/A	N/A
Industry	Transportation	Media/Entertainment	Media/Entertainment
Possible Repercussions	Phishing, social engineering, and impersonation attacks	Blackmail scams and sextortion	Phishing

Three major breaches observed in the past week

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

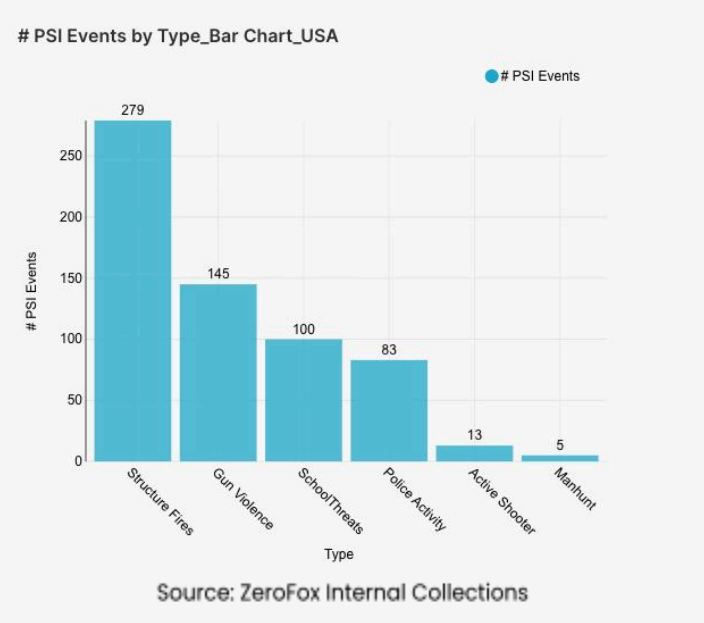
Physical Security Intelligence: Global



What happened: Excluding the United States, there was a 16 percent increase in mass casualty events this week from the previous week, with the top contributing countries or territories being India, Colombia, and the Palestinian territories, in that order. Approximately 61 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 31 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict (including raids and attacks) increased by 2 percent from the previous week. Events related to Russia's war in Ukraine increased by 200 percent. The top three most-alerted subtypes were explosions, which saw a 34 percent increase from the previous week; gun violence, which decreased by 14 percent; and structure fires, which decreased by 19 percent. Notably, there were six times as many active shooter alerts this week as compared to the previous week.

- **What this means:** This past week has seen a significant rise in global mass casualty events, including a sixfold increase in active shooter alerts. This spike is illustrated by the Bondi Beach mass shooting in Sydney, Australia, on December 14, in which a father and son linked to the Islamic State targeted a Hanukkah celebration, killing 15 people and wounding over 40. Concurrently, the Russia-Ukraine war, as well as explosions, saw a notable increase in alerts as both countries exchanged overnight drone and missile strikes on December 18; Russia launched an 82-drone attack targeting infrastructure in Ukraine's Cherkasy region, injuring six people and triggering significant blackouts. India saw the highest number of mass casualty alerts, largely driven by bomb threats toward multiple courts and banks on December 18, as well as toward several schools on December 15 and December 17, all of which caused public panic and mass evacuations. Overall, the global security landscape is currently defined by a sharp escalation in high-lethality active shooter events and an intensification of aerial warfare, alongside a surge in coordinated bomb threat hoaxes targeting civil infrastructure.

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 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 Ohio and Illinois, which together made up 17 percent of this week's nationwide total. Gun violence across the United States overall decreased by 9 percent from the week prior. Police activity alerts increased by 20 percent, and the top contributing states were California and Florida. Structure fires decreased by 5 percent, and the top two states for this subtype were New York and California. Notably, active shooter alerts increased by 333 percent, and threats related to schools increased by 28 percent.

- **What this means:** Domestic security data this week reveals a sharp rise in high-lethality incidents despite a general decrease in overall gun violence. Active shooter alerts and school-related threats saw significant escalations, headlined by the December 13 mass shooting at Brown University in Rhode Island, wherein a gunman killed two students and wounded nine others. A manhunt remains active for the unidentified suspect. While structure fires decreased by 5 percent nationally, significant instances persisted in major hubs like New York, evidenced by a recent apartment building fire in the Bronx on December 18, which resulted in four victims. Police activity alerts increased as well, driven by both high-stakes criminal investigations and public safety initiatives such as "Operation Holiday Cheer," involving 60 law enforcement agencies across California. Even though gun violence decreased nationally, there were six mass shootings within the last week, including an incident in Brooklyn, New York, on December 14 that injured six teenagers. The overall state of U.S. physical security is defined by an increase in concentrated, high-lethality threats and a notable rise in protective law enforcement measures.

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%