ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

November 15, 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 November 13, 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

ZeroFox Intelligence Brief: Russian Disinformation Surrounding Drone Incursions into Poland

Between September 9–10, 2025, there were at least 19 overnight violations of Polish airspace due to drone incursions, which closed at least four Polish airports. In the aftermath of these drone incursions, well-known Russian propaganda networks flooded social and traditional media channels, amplifying pro-Russia, anti-NATO, and anti-West narratives surrounding the airspace violations and shifting the blame to Ukraine. ZeroFox assesses this coordinated effort was likely aimed at deflecting blame from Moscow, undermining NATO unity, and weakening public support for Ukraine, particularly in frontline states like Poland.

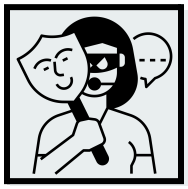
.

ZEROFOX

Weekly Intelligence Brief

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings



New Scam Center Strike Force Formed to Disrupt Southeast Asian Crypto Scams Targeting Americans

What we know:

- The U.S. Department of Justice (DOJ) and its partners have launched the Scam Center Strike Force to counter Southeast Asian crypto-investment fraud targeting Americans.
- Early operations have already recovered over USD 400 million in stolen cryptocurrency.
- The initiative brings together federal law enforcement, financial crime units, and international partners under one coordinated structure.

Background:

- These scams operate from large criminal compounds in Cambodia, Laos, and Burma, largely run by Chinese transnational criminal groups (TCOs).
- Scammers use social media outreach, social engineering tactics, and fake investment platforms to deceive victims.
- Scammers persuade victims to invest real cryptocurrency and redirect those funds into fake U.S.-hosted investment sites, after which the stolen crypto is quickly moved into accounts outside U.S. jurisdiction, making recovery extremely challenging.

What is next:

- The strike force will likely increase crypto-asset seizures and disrupt overseas enablers supporting these schemes.
- Greater cooperation with Southeast Asian authorities and Office of Foreign Assets Control (OFAC) sanctions will likely disrupt scam operations and raise operational costs for Chinese TCOs.
- Efforts could lead to more arrests, more fraudulent platforms being taken offline, and recovery for victims.
- Ongoing intelligence sharing and cross-agency coordination could further limit scammers' ability to target Americans.

Europol Dismantles Rhadamanthys, VenomRAT, Elysium in Operation Endgame

What we know:

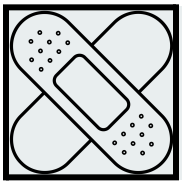
- Europol announced the takedowns of Rhadamanthys, the Remote Access Trojan VenomRAT, and the botnet Elysium infostealers as part of Operation Endgame between November 10 and November 13, 2025.

Background:

- The alleged main suspect behind VenomRAT was arrested in Greece on November 3, 2025, with access to over 100,000 victim crypto wallets worth millions.
- Law enforcement searched 11 European locations, took down 1,025 servers worldwide, and seized 20 domains.

Analyst note:

- Europol's animated video showing infostealer admins hoarding valuable data and giving customers low-value scraps, likely aims to undermine trust in the malware-as-a-service market.
- The VenomRAT suspect's arrest, along with the alleged Rhadamanthys admin's November 11 alert to customers, is likely to help authorities find further leads.



CISA Reissues Alert for Federal Agencies to Patch Cisco ASA and Firepower Devices

What we know:

- The Cybersecurity and Infrastructure Security Agency (CISA) has released an alert warning federal agencies that threat actors have continued to target vulnerabilities in Cisco Adaptive Security Appliances (ASA) and Firepower devices, directing agencies to update affected devices to the correct minimum versions.

Background:

- The U.S. cybersecurity agency flagged CVE-2025-20333 and CVE-2025-20362 in the alert. Additionally, separate research revealed that an "advanced" threat actor exploited Citrix Bleed 2 (CVE-2025-5777) and Cisco Identity Service Engine (ISE) (CVE-2025-20337) flaws as zero-days to deploy malware before the issues were publicly disclosed and patched.

Analyst note:

- These threat actors are likely to be state-backed hackers leveraging advanced resources to exploit high-value targets such as network security and edge-facing devices for cyber espionage.
- Threat actors are likely to achieve persistent access, exfiltrate sensitive data, move laterally to target more entities, and disrupt operations.

Exploit and Vulnerability Intelligence

Exploit and Vulnerability Intelligence Key Findings

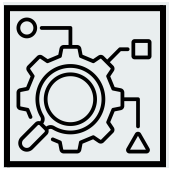
In the past week, ZeroFox observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in technology, software development, and critical infrastructure. CISA added four new vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on November 10 and November 12, 2025. Researchers have found that threat actors exploited a now-patched vulnerability (CVE-2025-12480) in Gladinet's Triofox file-sharing and remote access platform as a zero-day before a patch was released. A vulnerability in a popular expr-eval JavaScript library enables remote code execution (RCE) through malicious inputs. Multiple vulnerabilities have been patched in Runc container runtime that is used by Kubernetes, Docker, and other platforms to design and run containers. Researchers have discovered a flaw in OpenAI's video generator Sora 2 model that leaks the system prompt through audio transcripts. Ivanti has released patches for three high vulnerabilities in its Endpoint Manager that could enable a local authenticated attacker to write arbitrary files anywhere on disk. Microsoft has patched more than 60 vulnerabilities in its November Patch Tuesday security updates, including an actively exploited Windows Kernel zero-day (CVE-2025-62215) that enables attackers to gain system privileges via a race condition. Google Chrome version 142 has patched five vulnerabilities, including three high-severity flaws such as an out-of-bounds write in the WebGPU API (CVE-2025-12725) and memory-corruption bugs in the V8 engine and Views framework.

CRITICAL

CVE-2025-34299

What happened: A critical pre-authentication RCE bug in Monsta FTP allows attackers to force the application to download and write malicious payloads anywhere on the host, enabling full server takeover. Approximately 5,000 exposed instances were discovered, and Monsta FTP released a patch in v2.11.3.

- **What this means:** If left unpatched, unauthenticated code execution is likely to cause rapid escalation and lateral movement that could expose sensitive data and enable ransomware or supply-chain attacks.
- **Affected products:**
  - Monsta FTP versions 2.11 and earlier



CRITICAL

CVE-2025-21042

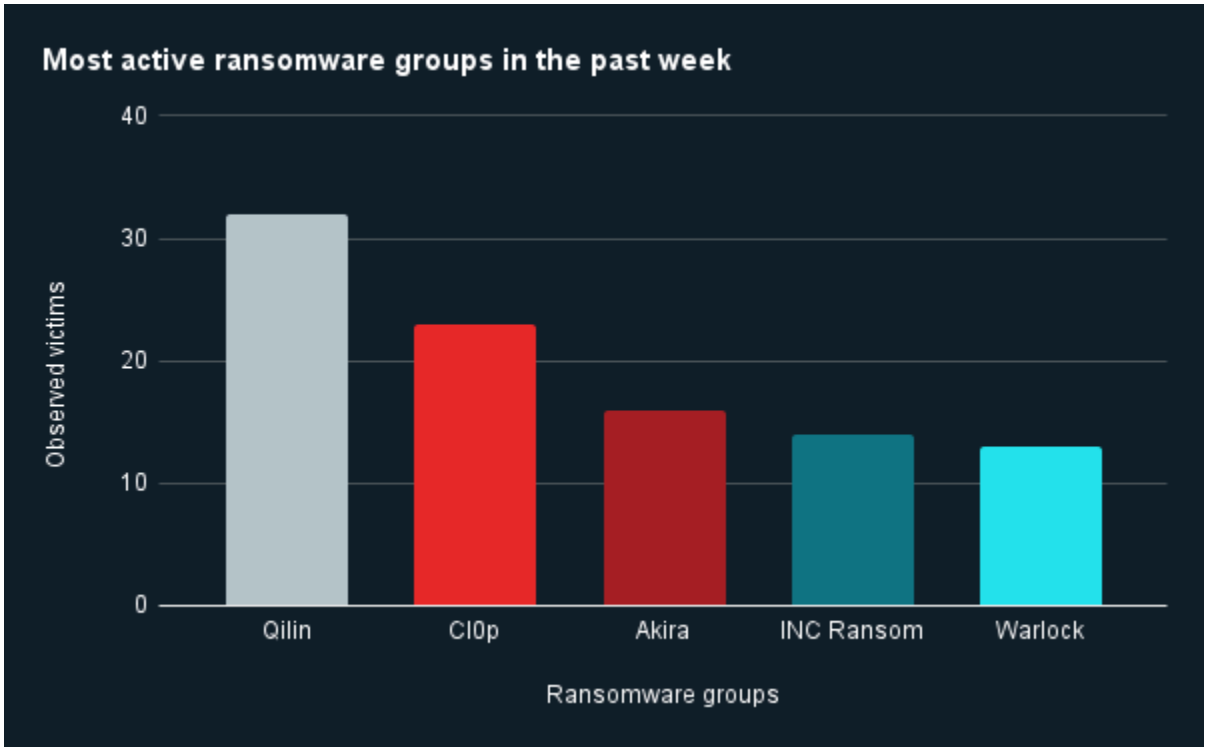
What happened: This already-patched zero-day vulnerability in Samsung's Android image processing library was reportedly exploited to deploy a commercial grade spyware tool, dubbed "Landfall," targeting Samsung Galaxy users in Iraq, Iran, Turkey, and Morocco. The campaign operated from mid-2024 to April 2025.

- **What this means:** The spyware enables operators to record conversations, collect contacts and call logs, track device locations, capture photos, and perform other surveillance without detection. Similar iOS attacks around the same time likely suggest a broader, coordinated surveillance campaign exploiting image-processing flaws across mobile devices.
- **Affected products:**
  - Android 13, 14, 15

Ransomware and Breach Intelligence

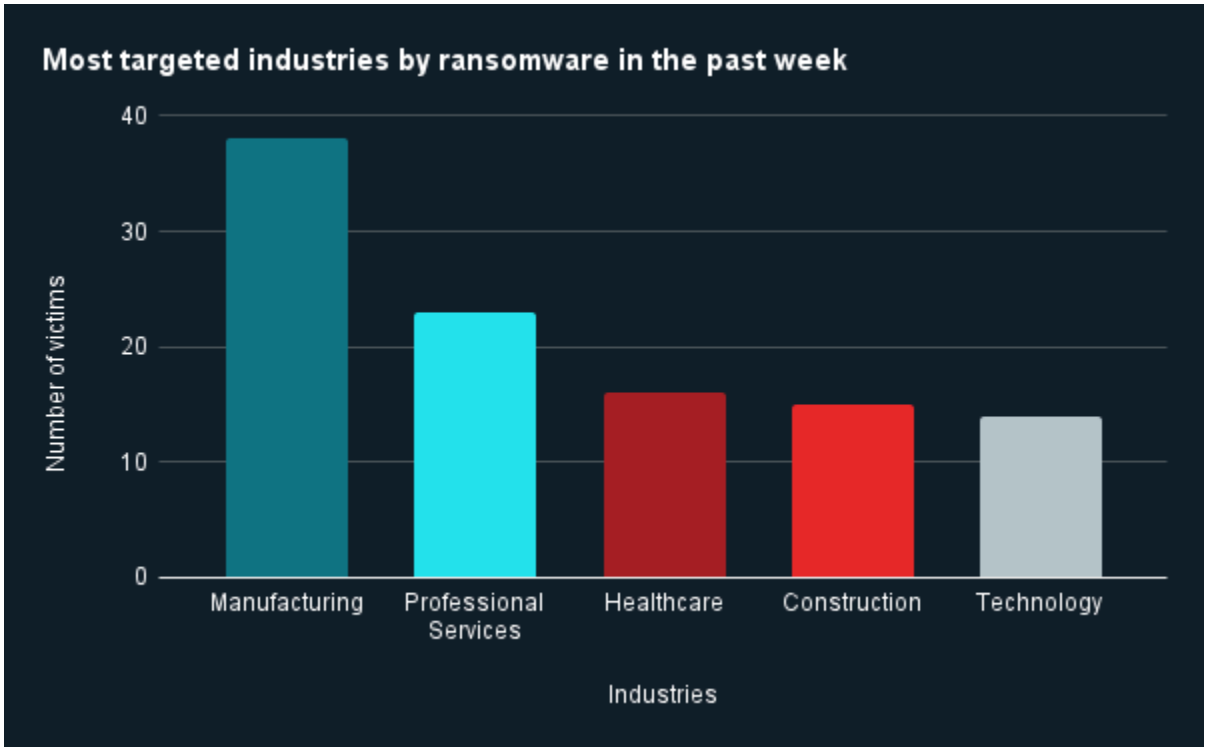
Ransomware and Breach Intelligence Key Findings

Ransomware Trends and Victims



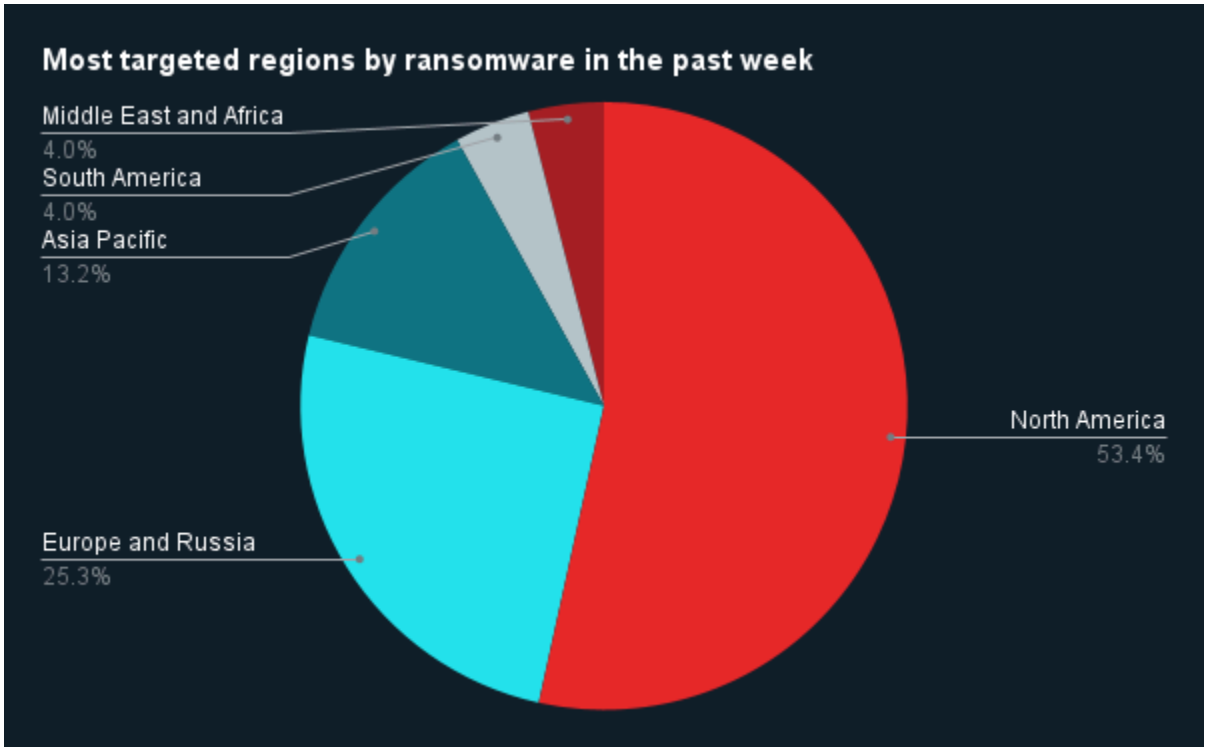
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Qilin, Cl0p, Akira, INC Ransom, and Warlock were the most active ransomware groups. ZeroFox observed close to 165 ransomware victims disclosed, most of whom were located in North America. The Qilin ransomware group accounted for the largest number of attacks, followed by Cl0p.



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 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 93 ransomware attacks observed in North America, while Europe and Russia accounted for 44, Asia-Pacific (APAC) for 23, South America for seven, and Middle East and Africa for seven.

Major Data Breaches Spanning Global Industries and Targets

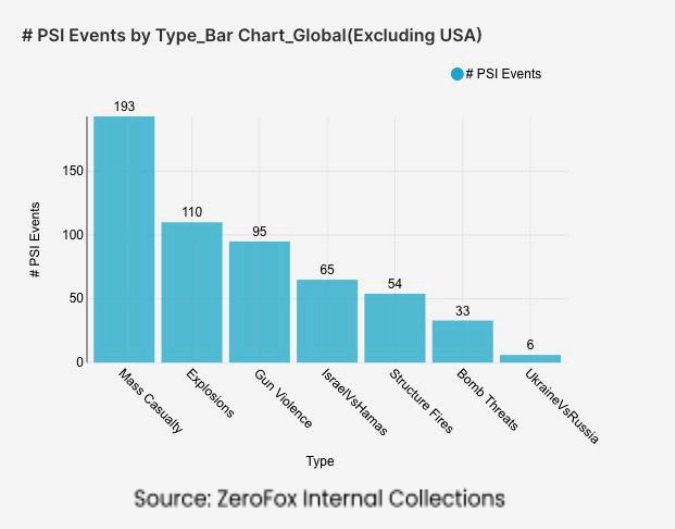
Targeted Entity	Hyundai AutoEver America (HAEA)	Doctor Alliance	Knownsec
Compromised Entities/victims	Unconfirmed number of Hyundai, Kia, and Genesis customers in North America	Allegedly, 1,240,640 files of patient data amounting to 353 GB	Data of the Indian government and LG Uplus Corp. (South Korea), as well as Taiwan's road planning data and plans of other global
Compromised Data Fields	Full name, Social Security number, driver's license information	Patient names, dates of birth, addresses, phone numbers, email addresses, Medicare numbers, medical record numbers, diagnoses, treatment plans, medications and dosages, provider information, and other protected health information	Classified cyberweapon documents, internal tools, global target lists, Remote Access Trojan (RAT) code, 95 GB of Indian immigration data, 3 TB of call records, and more
Suspected Threat Actor	Unconfirmed	Kazu	Unconfirmed
Country/Region	United States	Texas	China
Industry	Technology	Healthcare	Government
Possible Repercussions	Phishing, financial fraud, physical stalking, doxxing, credential theft, and account takeover	Social engineering attacks (such as phishing), identity theft and fraud, extortion, physical stalking, financial scams, doxxing, and sale of compromised data on dark web market places	Exposure of Chinese cyber operations and tools, intelligence gathering opportunities for adversaries, operational disruption for affected entities, increased risk of cyberattacks using leaked tools

Three major breaches observed in the past week

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

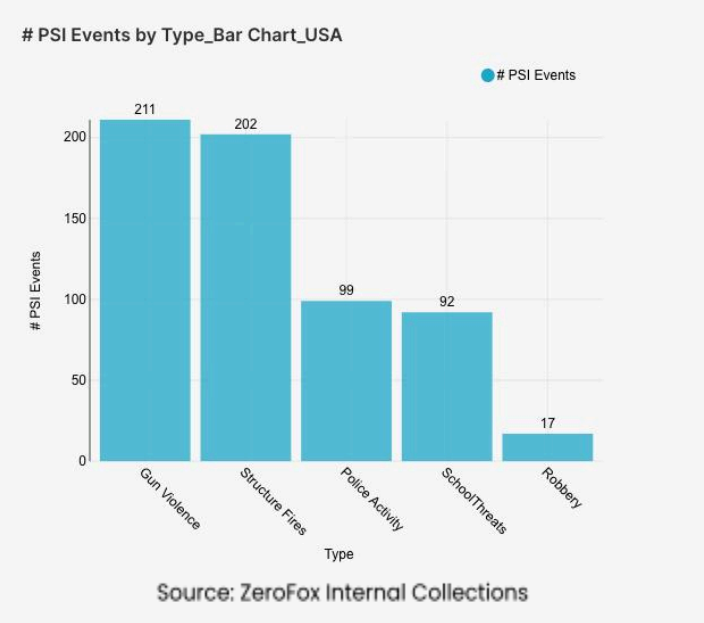


Source: ZeroFox Internal Collections

What happened: Excluding the United States, there was a 25 percent increase in mass casualty events this week from the previous week, with the top contributing countries or territories being India, Pakistan, and Lebanon, in that order. Approximately 57 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 32 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict (including raids and attacks) increased by 16 percent from the previous week. Events related to Russia's war in Ukraine decreased by 57 percent. The top three most-alerted subtypes were explosions, which saw a 7 percent increase from the previous week; gun violence, which decreased by 2 percent; and structure fires, which decreased by 17 percent. Notably, bomb threats increased by 175 percent from the previous week.

- **What this means:** With an overall increase across several threat subtypes, this week's data underscores a heightened global climate of instability. The significant increase in bomb threats correlates with a recent pattern of security alerts across India, one of the top contributing countries to global mass casualty events. Specifically, the Indira Gandhi International Airport (IGIA) in Delhi received a bomb threat email on November 12, which also mentioned other airports in Delhi, Mumbai, Chennai, Goa, and Hyderabad. Israel and Hamas have been in ongoing negotiations and exchanges of deceased hostages, and the recent ceasefire deal has been tested by renewed Israeli strikes in Gaza following accusations of Hamas violations. Additionally, the Israeli military carried out a series of airstrikes on Southern Lebanon on November 13, violating the terms of a November 2024 ceasefire agreement. Finally, in Pakistan, at least 12 people were killed and 27 others wounded on November 11 in a suicide bombing in Islamabad; the incident comes as the country is facing a resurgence of assaults by several insurgencies. Overall, global physical security is currently characterized by a volatile threat landscape, marked by persistent conflicts and elevated mass casualty risks.

Physical Security Intelligence: United States



Source: ZeroFox Internal Collections

What happened: In the past week, the top three most-alerted incident subtypes were gun violence, structure fires, 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 20 percent of this week's nationwide total. Gun violence across the United States overall decreased by 2 percent from the week prior. Police activity alerts increased by 19 percent, and the top contributing states were Florida and Texas. Structure fires increased by 24 percent, and the top two states for this subtype were New York and California. Notably, robberies increased by 31 percent.

- **What this means:** This week's domestic security landscape reflects an escalating and complex security environment. Structure fires saw a significant increase, driven by incidents in New York and California; for instance, an apartment building fire in New York City on November 12 killed one person and injured seven others. The increased use of heating devices during colder months, as well as persistent hazards associated with dense, multi-story urban residential buildings, may have contributed to the overall increase. Another notable increase this week was robberies, a trend that some officials have directly linked to economic instability. Specifically, the removal of Supplemental Nutrition Assistance Program (SNAP) benefits due to the federal government shutdown has been cited by officials, such as the Harris County District Attorney in Texas, as a potential driver for a rise in property crimes, suggesting a correlation between a decrease in food security and increased crime rates. Police activity rose this week as well, which may have been in response to the increase in crime. Overall, the U.S. physical security situation is currently defined by elevated domestic crime and man-made incident alerts.

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%