ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

November 22, 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 20, 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 Flash Report - Series of UK Cyberattacks Inspires New Cybersecurity Law

On November 12, 2025, the Labour Party proposed a Cyber Security and Resilience Bill to the UK Parliament to enhance the United Kingdom's existing cybersecurity law and improve defenses against cyberattacks that are increasingly targeting European Union (EU) critical infrastructure. A series of recent cyberattacks against UK-based organizations and critical infrastructure underpin how captive the UK economy is to its industry leaders and the depth of vulnerabilities stemming from cybersecurity gaps impacting them. Western political priorities have demonstrated an increased focus on protecting critical infrastructure, as evidenced by U.S. and UK policies targeting the intersection of cybersecurity and national security vulnerabilities.

ZeroFox Intelligence Flash Report - New DanaBot Malware Variant Emerges After Takedown

On November 10, 2025, security researchers observed a new variant of DanaBot malware—six months after a law enforcement operation removed 300 servers and 650 domains that were used as part of the DanaBot network infrastructure. Unlike previous iterations of DanaBot, the new variant reportedly harnesses standard IP-based command and control (C2) domains and dark web addresses to facilitate delivery of other modules and configuration files, enabling enhanced persistence and continuous execution. The re-emergence of DanaBot indicates that disrupted cybercrime networks are very likely to reorganize under recognizable branding to reignite their criminal enterprises as long as financial incentives persist.

ZeroFox Intelligence Brief - Underground Economist: Volume 5, Issue 23

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

BPH Providers Sanctioned and Disrupted

What we know:

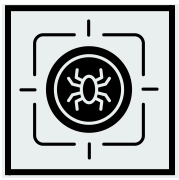
- The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), along with other agencies, has sanctioned Media Land, a Russia-based bulletproof hosting (BPH) provider, for supporting ransomware and cybercrime operations.
- The sanctions also designate Media Land's leadership, sister companies, and affiliates for evading previous sanctions.
- By offering resilient hosting and payment facilitation, Media Land facilitated global cybercriminal activity, increasing operational efficiency and anonymity for threat actors.

Background:

- This action follows a separate law enforcement action in which Dutch investigators seized roughly 250 physical servers and thousands of virtual servers from a BPH provider that was reportedly used exclusively to support criminal activity.
- The provider's infrastructure was also leveraged to launch distributed denial-of-service (DDoS) attacks against several companies and critical infrastructure, disrupting services and creating leverage for extortion.
- Additionally, affiliates were used to relocate IP infrastructure, establish front companies, and obscure connections to previously sanctioned entities.

What is next:

- These law enforcement actions are likely to further expand efforts in identifying other BPH providers and cybercrime enablers.
- Additionally, in the near term, these sanctions are expected to reduce the operational capacity of ransomware groups and DDoS actors that rely on resilient hosting services.
- Threat actors dependent on such platforms are likely to find other alternatives such as Virtual Private Server (VPS) and less well-known BPH services.



Europol Dismantles Rhadamanthys, VenomRAT, and Elysium in Operation Endgame

What we know:

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

Background:

- The alleged main suspect behind VenomRAT, who reportedly had access to over 100,000 victims' crypto wallets worth millions, was arrested in Greece on November 3, 2025. 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.

WhatsApp Vulnerability Enabled Global Phone Number Harvesting

What we know:

- Researchers have uncovered a major privacy flaw in WhatsApp's contact discovery feature that enabled anyone to rapidly enumerate billions of phone numbers due to weak rate limiting and the platform's reliance on predictable phone numbers as account identifiers.

Background:

- By automating lookup requests through WhatsApp Web, researchers collected 3.5 billion registered numbers, many with publicly exposed profile photos and "About" text.
- The issue had been known since 2017 but remained exploitable until Meta implemented stricter rate limits in October 2025.

Analyst note:

- The research shows systemic risks in phone number-based identity systems that threat actors could leverage for large-scale scraping to sell on dark web forums and carry out spear phishing attacks.
- The vulnerability is also likely to be used by authoritarian governments to identify and track users.

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 two vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog (CVE-2025-58034 and CVE-2025-13223) and released six industrial control advisories (ICS). CVE-2025-58034 is an OS Command Injection vulnerability in FortiWeb that could enable an authenticated attacker to execute unauthorized code on the underlying system via crafted HTTP requests or Command Line Interface (CLI) commands. Fortinet has observed this to be exploited in the wild. An unauthenticated command injection vulnerability (CVE-2025-9501) in the W3 Total Cache (W3TC) WordPress plugin, affecting versions before 2.8.13, enables remote PHP command execution via a malicious comment payload. Operation WrtHug has hijacked thousands of mostly end-of-life or outdated ASUS WRT routers globally, exploiting six vulnerabilities, including a critical bug (CVE-2025-2492). Google issued an emergency security update for Chrome to fix CVE-2025-13223, the seventh zero-day vulnerability exploited this year. Threat actors are actively exploiting CVE-2025-11001, a recently disclosed 7-Zip flaw that enables remote code execution through malicious ZIP file symlinks. The EchoGram flaw identified in early 2025 can bypass safety guardrails in major LLMs, including GPT-5.1, Claude, and Gemini, using simple, specially crafted words or code sequences.

MEDIUM

CVE-2025-58034

What happened: Fortinet has disclosed a second zero-day vulnerability in its FortiWeb web application firewall (WAF) line shortly after disclosing another exploited flaw (CVE-2025-64446) earlier. CVE-2025-58034 is a command injection flaw that enables an authenticated attacker to execute code via crafted HTTP requests and commands.
What this means: Attackers could run arbitrary commands on affected FortiWeb devices, gaining control of the WAF and pivoting to internal networks.

- **Affected products:**
  - The affected products are listed in this advisory.

HIGH

CVE-2025-13223

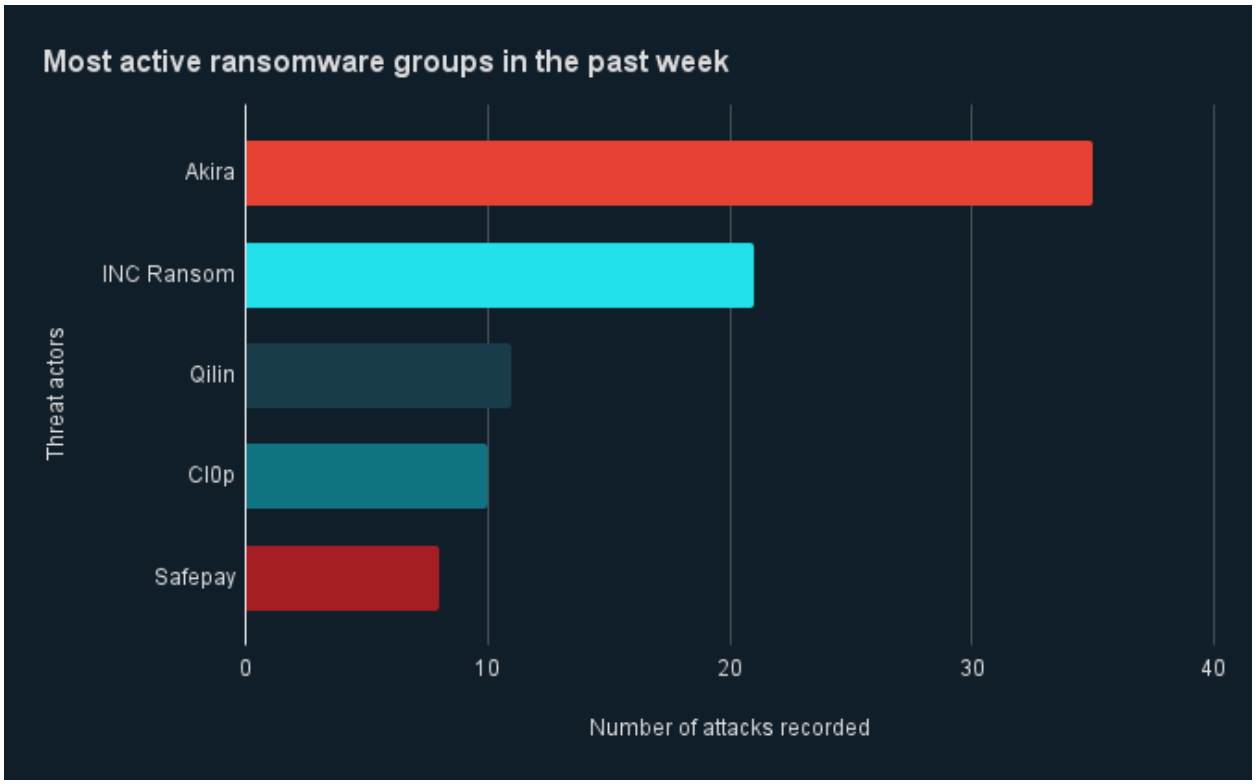
What happened: Google has released a patch for this type confusion vulnerability in the V8 JavaScript engine. The bug could enable arbitrary code execution and system crashes.

- **What this means:** Successful exploitation is likely to lead to full system compromise via a crafted HTML page. Threat actors are likely to steal credentials, cookies, and other data stored on Chrome web browser in case of a successful exploit.
- **Affected products:**
  - The affected products are listed in this advisory.

Ransomware and Breach Intelligence

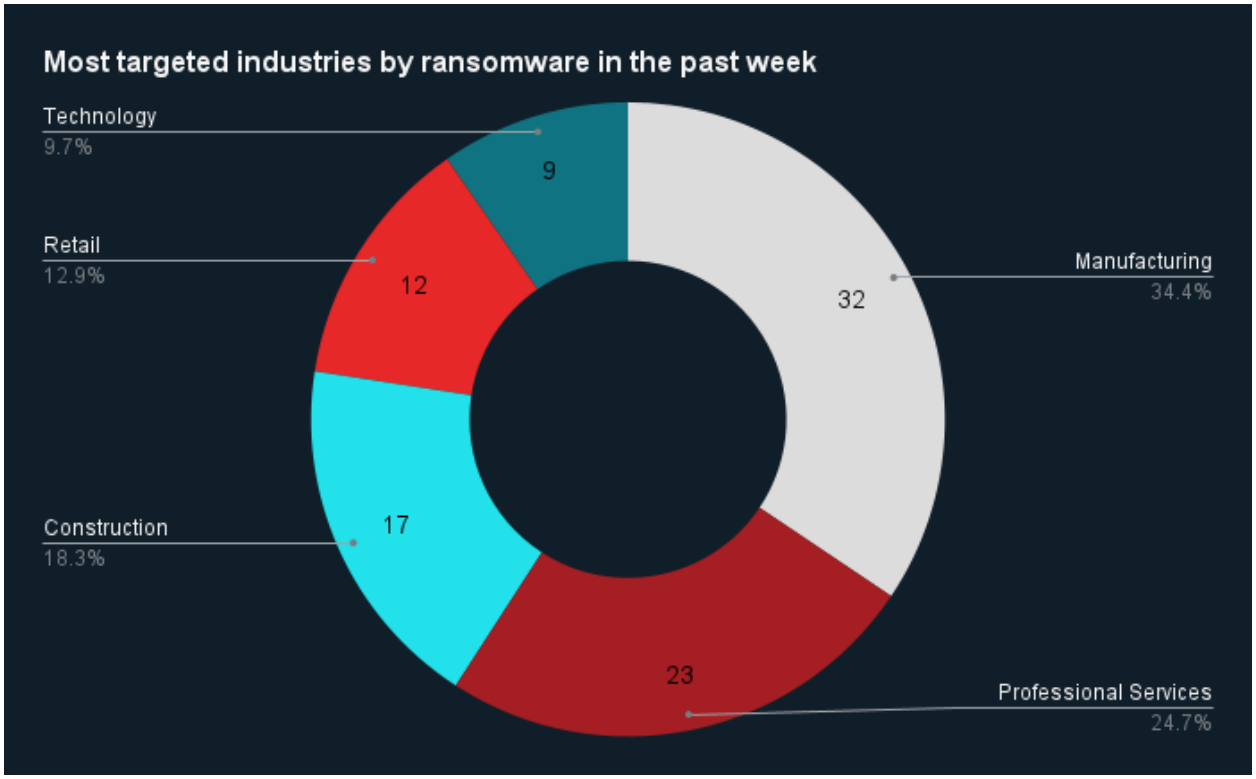
Ransomware and Breach Intelligence Key Findings

Ransomware Actors, Industry, and Region Trends



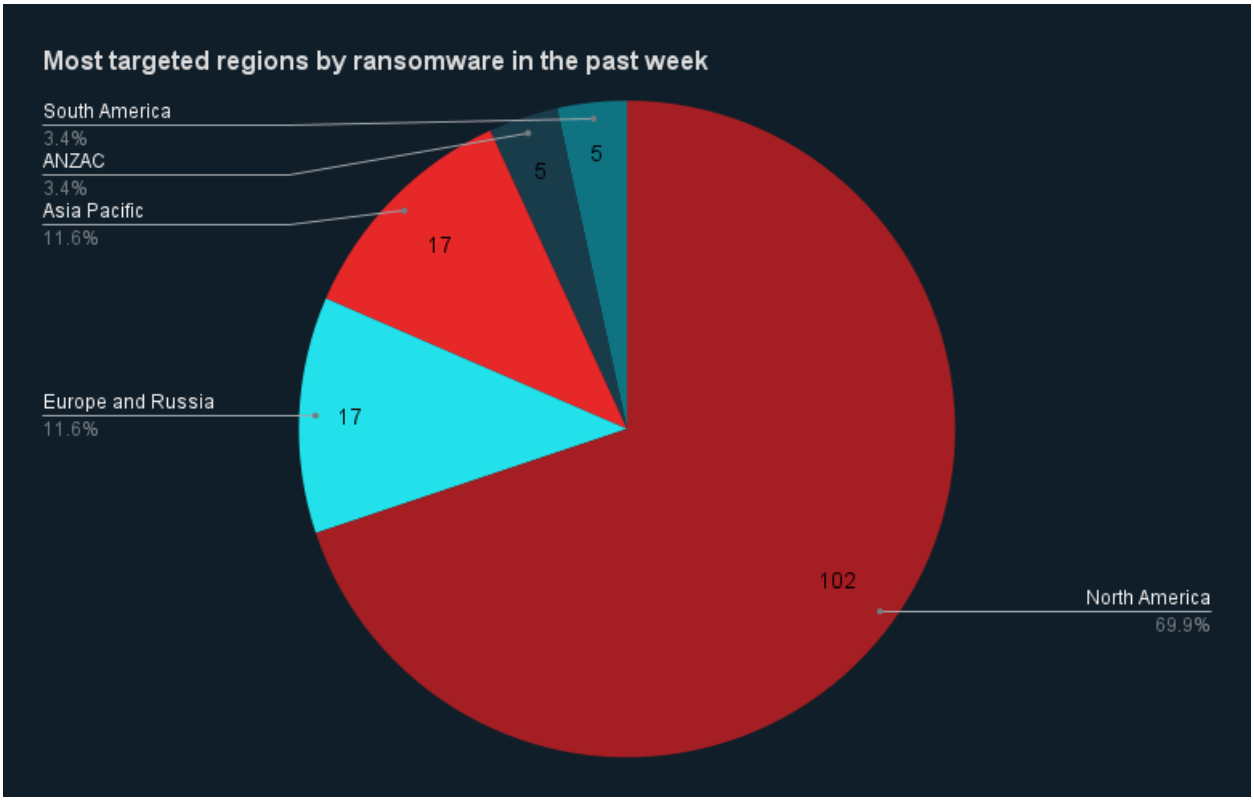
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Akira, INC Ransom, Qilin, Cl0p, and SafePay were the most active ransomware groups. ZeroFox observed close to 128 ransomware victims disclosed, most of whom were located in North America. The Akira ransomware group accounted for the largest number of attacks, followed by INC Ransom.



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 and Asia Pacific (APAC) regions. There were at least 102 ransomware attacks observed in North America, while Europe and Russia and APAC accounted for 17 each, and Australia and New Zealand (ANZAC) and South America accounted for five each.

Significant Data Breaches Reported in the Past Week

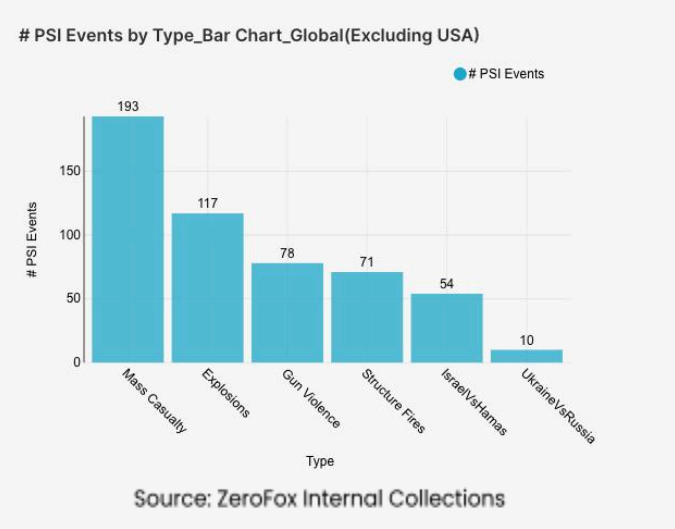
Targeted Entity	Protei	Pajemploi	Samsung Medison
Compromised Entities/victims	N/A	1.2 million employees and employers in France	N/A
Compromised Data Fields	Protei's web server includes around 182 GB of files and emails dating back years	Names, birth details, addresses, Social Security numbers (SSNs), bank names, and Pajemploi numbers	SQL tables, user and employee records, names, emails, country details, internal logs, and exported cloud directories
Suspected Threat Actor	N/A	N/A	DarkForums user 888
Country/Region	Russia, Italy, Mexico, Bahrain, Jordan, central Africa, Kazakhstan, and Pakistan	France	South Korea
Industry	Communication	Professional Services	Healthcare
Possible Repercussions	Data likely to be leveraged by defense and security entities to map surveillance infrastructure, clients, supply chains, and potential state-linked operations.	Ransom demands, phishing, impersonation, and social engineering attacks	Phishing, social engineering, follow-on attacks targeting downstream entities, including disruption to services and operations

Three major breaches observed in the past week

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

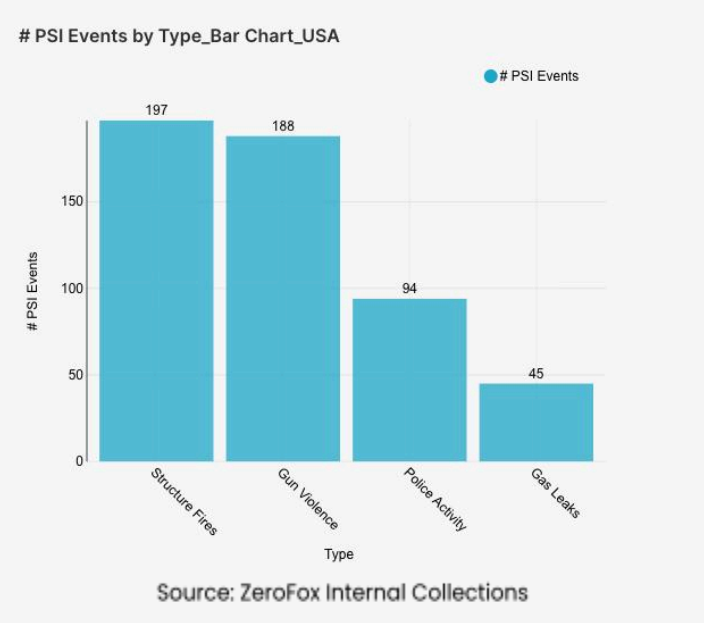


Source: ZeroFox Internal Collections

What happened: Excluding the United States, there was no increase or decrease in mass casualty events this week from the previous week, with the top contributing countries or territories being India, the Palestinian territories, and Lebanon, in that order. Approximately 61 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) decreased by 17 percent from the previous week. Events related to Russia's war in Ukraine increased by 67 percent. The top three most-alerted subtypes were explosions, which saw a 6 percent increase from the previous week; gun violence, which decreased by 18 percent; and structure fires, which increased by 31 percent.

- **What this means:** This week's data continues to underscore a heightened global climate of instability. The Russia-Ukraine war showed the greatest escalation, reflected in continued intensified Russian attacks, such as the numerous missile and drone strikes that killed at least 26 civilians and wounded at least 139 in Kharkiv on November 18–19. Notably, there are speculations that a peace plan has been devised between the United States and Russia, which allegedly contains proposals for Ukraine to cede territory and weaponry. Whether or not this will solidify into a lasting truce is yet to be determined. The data on the Israel-Hamas conflict indicates a decrease in general alerts, corresponding with the holding of a fragile ceasefire in Gaza since early October 2025. However, the Palestinian territories and Lebanon remain critical hotbeds of violence. For instance, on November 18, Israeli forces conducted strikes in Lebanon that killed at least 13 people in a Palestinian refugee camp. Further, on November 19 and 20, Israeli strikes in Gaza killed at least 32 Palestinians, demonstrating that, while broad conflict alerts may have lessened, mass casualty incidents are still highly frequent.

Physical Security Intelligence: United States



Source: ZeroFox Internal Collections

What happened: In the past week, the top three most-alerted incident subtypes in the United States 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 35 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 9 percent, and the top contributing states were California and Ohio. Structure fires increased by 32, and the top two states for this subtype were New York and California. Notably, gas leaks increased by 24 percent.

- **What this means:** While overall criminal and police activity decreased this past week, the United States saw a sharp rise in man-made disaster and accident alerts, driven primarily by an increase in structure fires and gas leaks. The highest concentration of these structural risks was in New York and California. Corroborating this trend, the Los Angeles Fire Department reported multiple structure fire knockdowns in California, including one on November 19 that took 66 firefighters nearly an hour to contain. Furthermore, the risk of explosions from gas leaks was highlighted by a recent incident on November 16, in which nine people were injured in an explosion caused by a gas leak in Chino Hills, California. The National Fire Protection Association consistently reports that winter months see a higher number of home fires; heating equipment is the second leading cause of house fires, and unvented combustion heating appliances lead to possible gas leaks. The decrease in gun violence and police activity also correlates with research showing that violent crime tends to fall during the winter months.

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%