



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

May 17, 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 (EDT) on May 15, 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	2
ZeroFox Intelligence Brief – Underground Economist: Volume 5, Issue 9	2
 Cyber and Dark Web Intelligence Key Findings	4
Scammers Target Job Seekers on Popular Messaging Application	4
New Info-Stealer Malware Disguised as Fake AI Generation Tool	5
FBI Warns of End-of-Life Routers Abused for Cybercrime	5
 Exploit and Vulnerability Intelligence Key Findings	7
CVE-2025-4632	7
CVE-2025-3711	8
 Ransomware and Breach Intelligence Key Findings	10
Ransomware Roundup: Most Active Actors, Affected Regions, Industries, and More	10
Major Data Breaches Observed This Week	13
 Physical and Geopolitical Intelligence Key Findings	15
Physical Security Intelligence: Global	15
Physical Security Intelligence: United States	16
 Appendix A: Traffic Light Protocol for Information Dissemination	17
 Appendix B: ZeroFox Intelligence Probability Scale	18

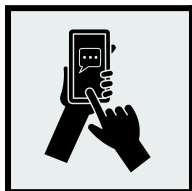
| This Week's ZeroFox Intelligence Reports

[ZeroFox Intelligence Brief – Underground Economist: Volume 5, Issue 9](#)

The Underground Economist is an intelligence-focused series illuminating dark web findings from our ZeroFox Dark Ops intelligence team.

| Cyber and Dark Web Intelligence |

| Cyber and Dark Web Intelligence Key Findings



Scammers Target Job Seekers on Popular Messaging Application

What we know:

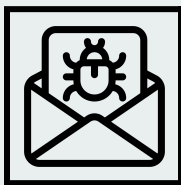
- Threat actors are conducting sophisticated recruitment scams targeting job seekers globally.
- Tactics used by threat actors include impersonating reputable tech firms, logistics recruiters, and even the government of Singapore.
- Victims are lured via platforms like WhatsApp and Telegram and directed to fake websites that mimic legitimate operations.
- The scams are designed to extract upfront payments, steal personal information, and gain unauthorized access to victims' financial assets or sensitive data.

Background:

- Tech employer impersonation scams often use small initial credits to gain trust, then demand escalating deposits in USD Tether (USDT) for fake task completions.
- Logistics agency impersonation shows a high volume of geo-targeting—especially towards U.S.-based job seekers, with at least 63,000 targeted.
- Government impersonation relies on phishing through fake Telegram groups, requesting personal IDs and phone verification codes.
- At least 45 fake websites (nine tech-related, 36 logistics-related) have been identified as part of these ongoing operations.

What is next:

- Threat actors could exploit stolen data for identity theft, account takeovers, and financial fraud to create synthetic identities, bypass security measures, or sell on the dark web. They could also leverage victims' data in follow-up scams or extortion attempts.
- These scams are becoming increasingly sophisticated, with attackers using social engineering, fake job portals, artificial intelligence (AI)-generated content, and geo-targeted campaigns to build trust and deceive victims. More impersonation scams—via Telegram, fake websites, and “verification” platforms—are likely to grow in scale and complexity.



New Info-Stealer Malware Disguised as Fake AI Generation Tool

What we know:

- Threat actors are using fake AI-powered video-making tools and Facebook ads to distribute a new information-stealing malware known as Noodlophile.

Background:

- Noodlophile is being sold on dark web forums, usually along with "Get Cookie+Pass" services, a malware-as-a-service (MaaS) operation linked to Vietnamese-speaking actors. The malware targets data stored on web browsers, including crypto wallets and account credentials.

Analyst note:

- Financially motivated threat actors are likely to exploit any new AI content trend to deploy malware by claiming to offer free AI tools. This can result in financial losses and takeover of victims' accounts, which can be further misused for social-engineering attacks.



FBI Warns of End-of-Life Routers Abused for Cybercrime

What we know:

- The Federal Bureau of Investigation (FBI) has been warning of threat actors exploiting outdated routers with known vulnerabilities to install malware and convert them into proxies.

Background:

- These compromised devices, often infected with variants of TheMoon malware, are used to obfuscate cybercriminal activity, including espionage and crypto theft.

Analyst note:

- Threat actors are likely to exploit these functioning and unsecured end-of-life routers to launch large-scale attacks while evading detection through proxy networks. These attacks could include network infiltration, account hijacking, distributed denial-of-service attacks, and remote code execution.

| **Exploit and Vulnerability Intelligence** |

| Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox has 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 a total of six new vulnerabilities on [May 13](#) and [May 14](#) to its Known Exploited Vulnerabilities Catalog. Microsoft's [May 2025 Patch Tuesday](#) has addressed 72 flaws, including five actively exploited and two publicly disclosed zero-days. Six critical bugs were fixed, with the majority involving remote code execution and privilege escalation. [Apple has released](#) a series of updates for its multiple software versions to address various security vulnerabilities. Ivanti has released updates for Endpoint Manager Mobile (EPMM) to address two security flaws: [CVE-2025-4427 and CVE-2025-4428](#). A Fortinet vulnerability ([CVE-2025-32756](#)) enables a remote unauthenticated attacker to execute arbitrary code or commands by sending HTTP requests. [SAP released a patch](#) for a zero-day (CVE-2025-42999) exploited in recent attacks on NetWeaver servers, which were discovered during an earlier investigation into CVE-2025-31324.



CRITICAL

CVE-2025-4632

What happened: This improper limitation of a pathname to a restricted directory vulnerability that enables attackers to write arbitrary files as system authority has been [exploited in the wild](#).

- **What this means:** If devices are not updated, threat actors could bypass device security by rewriting arbitrary files to install malware, lock systems, and cause operational disruptions.
- **Affected products:**
 - Samsung Electronics MagicINFO 9 Server versions 0 to 21.1052

**CRITICAL****CVE-2025-3711**

What happened: This is a stack-based buffer overflow vulnerability in IP-based CL5708IM LCD KVM Switch. It enables remote attackers to execute arbitrary code on a targeted device.

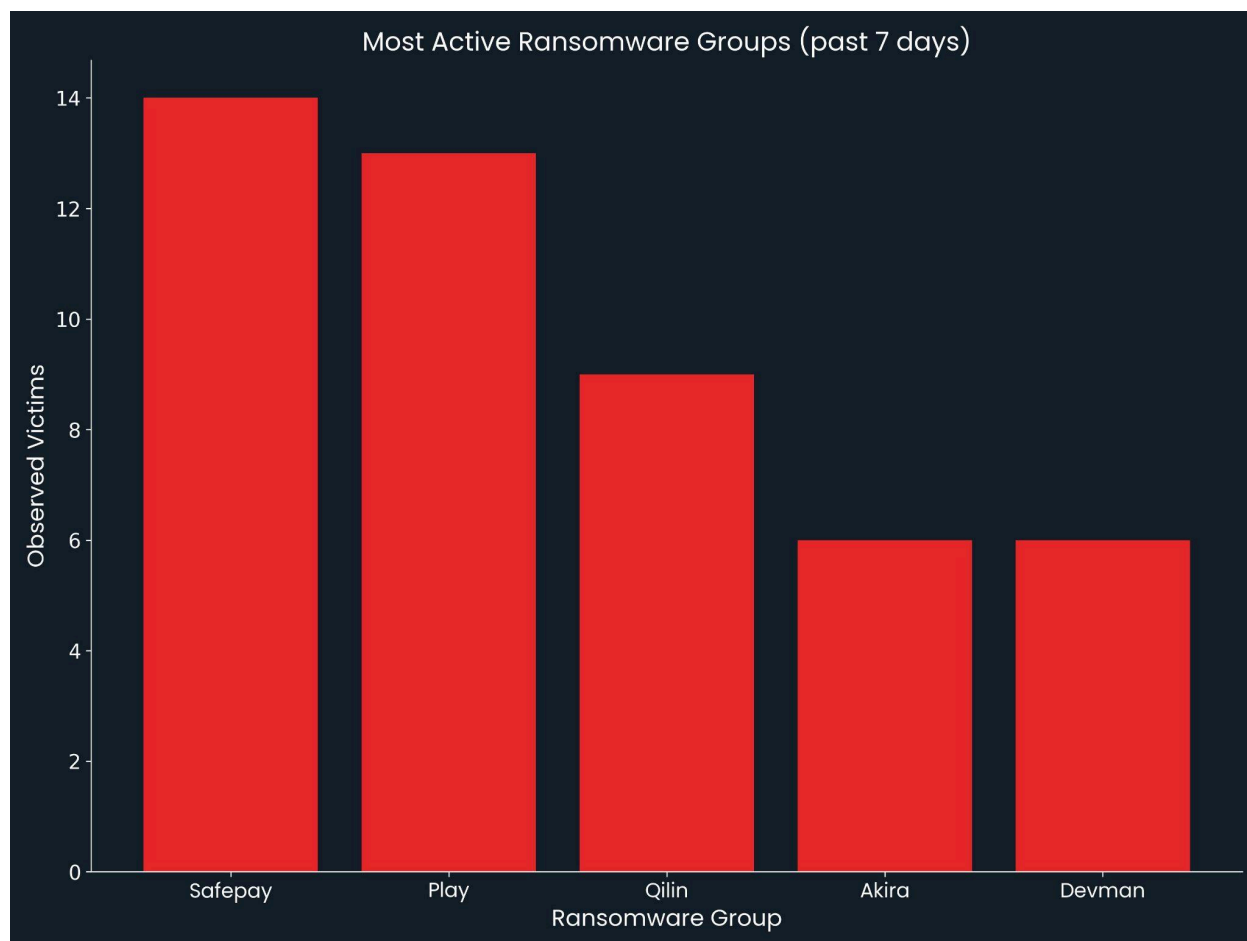
- **What this means:** This vulnerability likely enables threat actors to disrupt operations on a device or steal information. Government, education, transport, and broadcasting and media sectors using affected devices are likely to be targeted by either financially or politically motivated threat actors.
- **Affected products:**
 - CL5708IM LCD KVM Switch

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

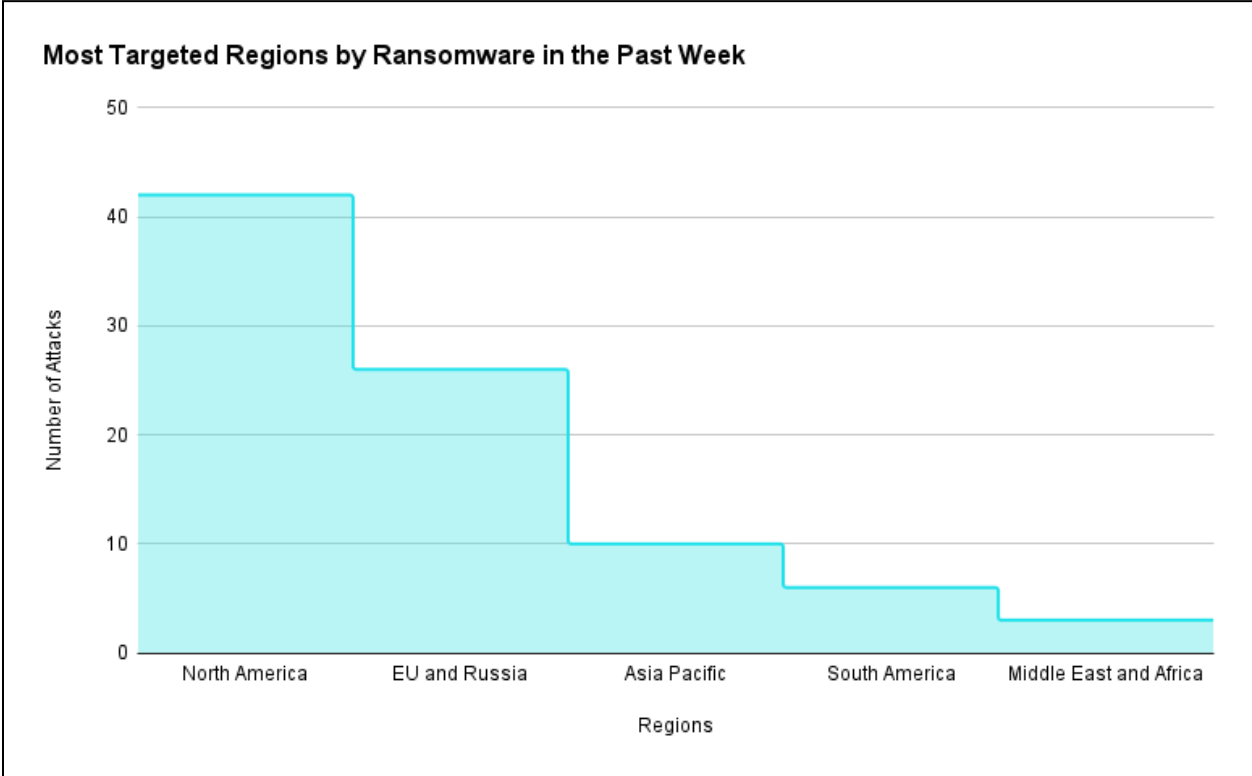


Ransomware Roundup: Most Active Actors, Affected Regions, Industries, and More



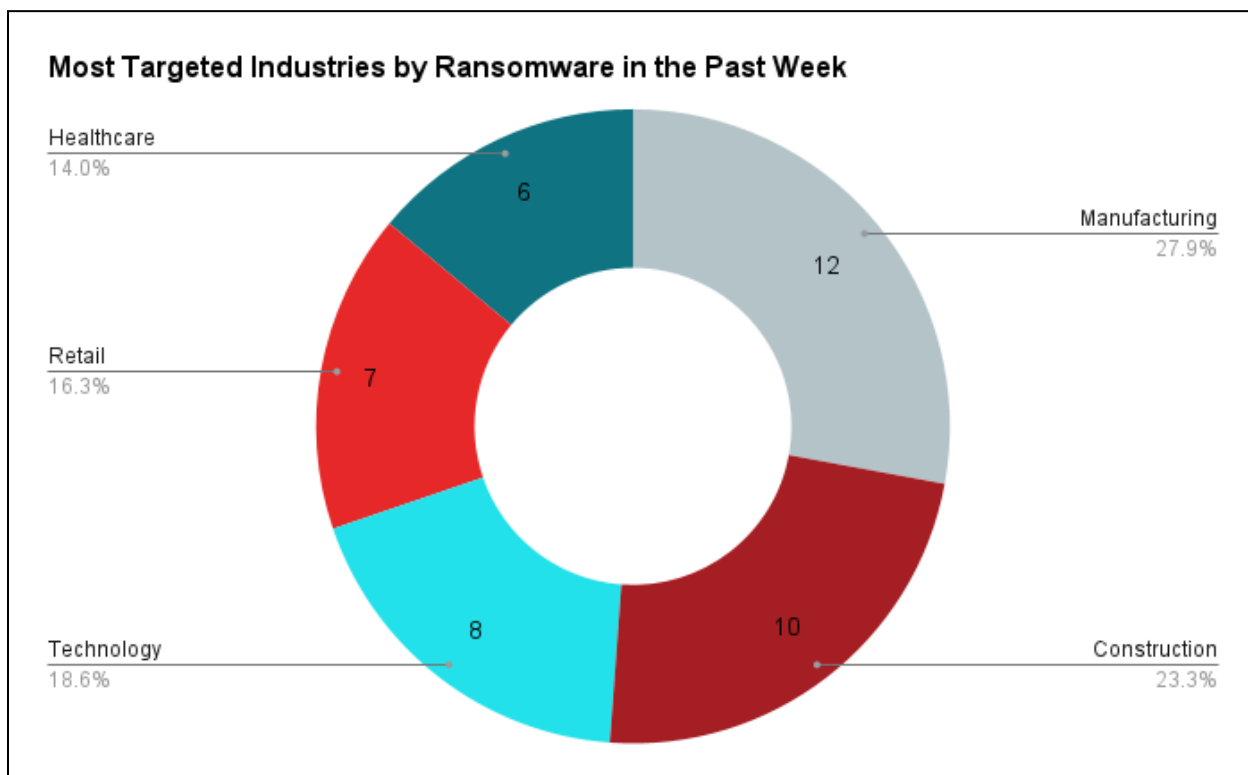
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Safepay, Play, Qilin, Akira, and Devman were the most active ransomware groups. ZeroFox observed at least 48 ransomware victims disclosed, most of which are located in North America. Safepay and Play accounted for the largest number of attacks.



Source: ZeroFox Internal Collections

Regional ransomware trends: In the past seven days, ZeroFox has observed that North America was the most targeted region by ransomware attacks, followed by EU-Russia.



Source: ZeroFox Internal Collections

Industry ransomware trend: In the past week, ZeroFox observed that manufacturing, construction, technology, retail, and healthcare were the industries most targeted by ransomware attacks. The graph above shows the number of ransomware attacks suffered by these industries in the last week. The manufacturing and construction industries were the most targeted, with 12 and 10 attacks, respectively.



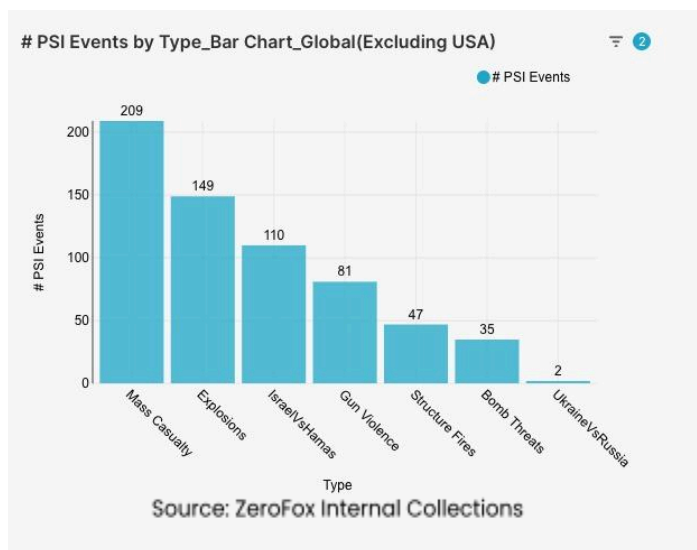
Major Data Breaches Observed This Week

Targeted Entity	<u>Marks & Spencer</u>	<u>Pearson</u>	<u>House of Dior</u>
Impacted Entities	Customer information	N/A	Customer information
Compromised Data and Infrastructure	Personally identifiable information (PII) of customers, including contact numbers, home addresses, and dates of birth	Customer information, support tickets, financials, and source code reportedly stolen, along with credentials to cloud platforms	PII of customers, including contact numbers, purchase amounts, mailing addresses, and purchase and preferences data but excluding financial information like bank account details or credentials
Suspected Threat Actor	DragonForce or Scattered Spider Ransomware groups	N/A	N/A
Country/Region	United Kingdom	UK-based company working with schools, universities, and individuals in over 70 countries	South Korea and China confirmed so far, other regions possibly affected
Industry	Retail	Education	Luxury
Possible Repercussions	Identity theft, social engineering and phishing attacks, double extortion, financial fraud	Double extortion, content manipulation, copyright infringement, intellectual property theft, financial fraud, phishing, social engineering	Phishing, social engineering, impersonation attacks, financial fraud, ransomware, data resale on dark web forums

Three major breaches observed in the past week

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings



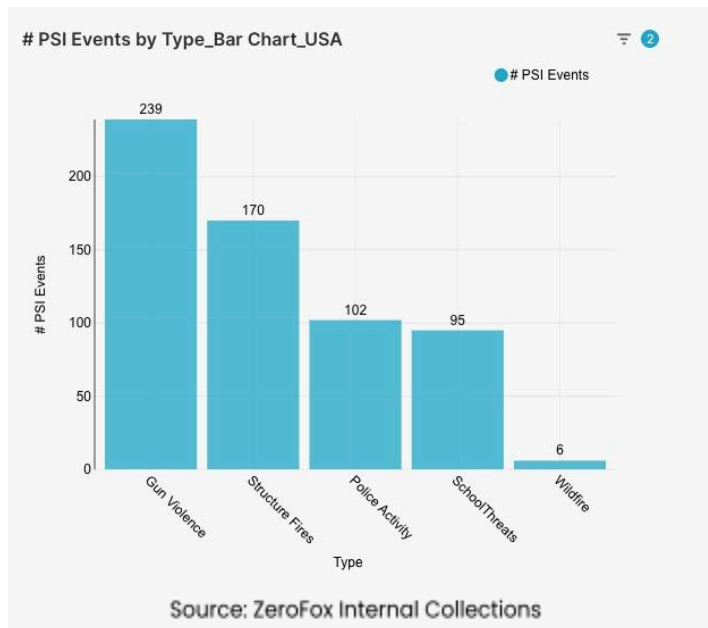
Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 33 percent increase in mass casualty events this week from the previous week, with the top contributing countries being India, Pakistan, and Palestine, in that order. Approximately 71 percent of these events were explosions, and the three aforementioned countries accounted for about 64 percent of all mass casualty alerts. General alerts related to the

Israel-Hamas War (including protests, raids, and involvement in neighboring countries) increased by 67 percent from the previous week. Events related to Russia's war in Ukraine decreased by 86 percent. The top three most-alerted subtypes were explosions, which saw a 32 percent increase from the previous week; gun violence, which increased by 14 percent; and structure fires, which increased by 27 percent. Global protest activity decreased by 6 percent. Notably, bomb threats increased by 338 percent from the previous week, and India was the largest contributor to this number.

- **What this means:** The India-Pakistan conflict has sharply escalated this week, as the two countries have cut diplomatic ties and launched [retaliatory actions](#), including Indian airstrikes and reported Pakistani countermeasures. Tensions remain high, with sporadic clashes contributing to both the rise of mass casualty events and explosion alerts. Additionally, this conflict—as well as [bomb threats](#) against transportation infrastructure—have caused Indian airports to ramp up security measures. The significant rise in alerts related to the Israel-Hamas conflict this week points to continued military operations, civilian unrest, and cross-border tensions involving neighboring states. On May 13, Israel allegedly targeted a hospital in which Hamas leader [Mohammed Sinwar](#) was located, although it is unclear if this resulted in his death. As for the Russia-Ukraine war, the decrease in alerts this week may have been due to the May 8-11 [ceasefire](#) implemented by Russia. Furthermore, [peace talks](#) have been scheduled between Russian President Putin

and Ukrainian President Zelenskyy on May 15, although it is unclear whether Putin himself intends to appear.



Physical Security

Intelligence: United States

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 that had the most gun violence alerts were California and New York,

which together made up 18 percent of this week's nationwide total. Gun violence across the United States overall decreased by 7 percent from the week prior. Police activity alerts increased by 1 percent, and the top contributing states were California and Texas. Structure fires also increased by 1 percent, and the top two states for this subtype were California and New York. Notably, there were six times as many wildfire alerts this week compared to the week prior.

- > **What this means:** The most significant increase this week was the wildfires subtype, with a ["Red Flag Warning"](#) issued for Arizona, New Mexico, Montana, Nebraska, South Dakota, North Dakota, Minnesota, Iowa, and Wisconsin. Critical fire conditions occurred in both Minnesota, which experienced three major wildfires this week, and [Arizona](#), where a wildfire consumed thousands of acres and mass-evacuations ensued. The slight increase in structure fire alerts may be due to seasonal weather changes, such as warmer temperatures or drier air in some regions, which can elevate fire risk. The decrease in gun violence alerts across the country may be attributed to several factors, including improved law enforcement strategies, recent community intervention efforts, or short-term shifts in public behavior due to schools beginning their summer holidays. Meanwhile, the small rise in police activity alerts could reflect heightened security responses to ongoing public safety concerns or increased reporting of suspicious behavior, especially in large, populous states like California and Texas.

| 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%