ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

May 9, 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 May 7, 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

Fragile Ceasefire – SITREP #37: May 6, 2026

On May 3, the U.S. military launched "Project Freedom" to restart commercial shipping in the Strait of Hormuz (SoH), enabling two vessels to exit. Iran retaliated with attacks against nearby United Arab Emirates (UAE), commercial vessels, and U.S. ships. Iran's response reaffirms its commitment to restricting commercial shipping in the SoH, making a significant increase in transits highly unlikely. Despite recent setbacks, the April 8 ceasefire continues to hold, likely because the episodes demonstrated that renewed fighting will not resolve the conflict. To this end, Project Freedom was paused after one day amid reports that a memorandum of understanding (MOU) to end the war was circulating. Major stock indices surged and oil prices dropped in response to reports of the MOU. This is likely a reflection of the higher likelihood the MOU will lead to an agreement because it represents the United States moving a step closer to accepting certain Iranian demands in the short term. However, neither the United States nor Iran has tangibly altered its long-term negotiating positions, which could resurface in future talks.

ZeroFox Intelligence Flash Report - SITREP #36 - Pro-Iran Terrorism in Europe - May 5, 2026

Since March 9, 2026, a group claiming to support Iran in its war against the United States and Israel has reportedly conducted a campaign of attacks against Jewish targets in Europe. Harakat Ashab al-Yamin al-Islamia (HAYI) has claimed 17 attacks against Jewish communities, Israeli diplomatic missions, and Iranian dissident journalists across Europe—the most recent of which was the April 29, 2026, stabbing of two Jewish individuals in the Golders Green area of London. In the case of at least one claimed attack, HAYI likely recruited and paid criminal actors to conduct attacks on its behalf. Following an attack on a French branch of a U.S. bank, the detained suspect reportedly claimed to have been paid EUR 600 by an unidentified individual online to conduct the attack. While there is no direct connection to the Iranian government, it is likely that HAYI is operating as a Europe-based proxy for the Islamic Revolutionary Guard Corps-Quds Force (IRGC-QF). Initially, HAYI made posts claiming responsibility on Telegram channels likely under its control; however, Telegram closed down several channels associated with HAYI after March 9, leaving the group to post claims on channels associated with IRGC-QF controlled Iraqi Shia militias. HAYI is likely an identifiable group only online. HAYI likely operates as a function of Iranian hybrid warfare and recruits criminals and radicalized individuals via online forums to conduct attacks—almost certainly due to a combination of financial motives and ideological alignment with Iranian war aims.

Monthly Geopolitical Assessment – May 2026

Measured military responses to setbacks in U.S.-Iran talks signal that both sides are likely reluctant to return to armed conflict and instead prefer to utilize economic coercion to increase ceasefire pressure. The United States and Iran will likely resume talks, but escalatory risks remain—especially as both countries maintain dual blockades of the Strait of Hormuz (SoH). Since the terms of the ceasefire require the SoH to remain closed, all of the negative economic consequences seen during the period of all-out war in Iran will very likely worsen. The United Arab Emirates (UAE)'s decision to leave OPEC very likely signals its intent to increase oil production once the SoH is reopened and reflects concern that the war in Iran has quickened the transition away from fossil fuels. Few other states have the UAE's competitive advantages, and the UAE is very likely moving to maximize output while oil demand remains. Other states are likely to make this decision as well, which is expected to lead to a temporary increase in fossil fuel production before demand slumps. The chaos surrounding Peru's elections has been the norm in recent regional elections. The losing side will very likely claim electoral fraud, increasing the risk of social unrest. Similar outcomes are likely in the major upcoming elections in Colombia and Brazil. U.S. President Donald Trump and Chinese President Xi Jinping are scheduled to attend a high-profile summit in mid-May 2026. If the war in Iran is not settled by that time but does not delay their meeting again, Trump is likely to be on weaker footing for the summit; Xi will likely pressure the United States to make a public commitment to downgrading its ties with Taiwan. However, overall U.S.-China tensions are likely to improve throughout 2026. A definitive resolution to the U.S. blockade of Cuba remains unlikely while the Trump administration remains preoccupied with Iran. Growing Australia–Japan defense ties are likely a model of how U.S. allies will develop alternative security pacts.

ZeroFox Intelligence Brief - Underground Economist: Volume 6, Issue 10

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

ZeroFox Intelligence Profile - The Gentlemen

The Gentlemen is a ransomware-as–service (RaaS) collective active since at least September 2025 that publishes victim data on its dark web-hosted blog. As of April 2026, The Gentlemen has conducted at least 346 attacks, averaging 43 per month. The Gentlemen is almost certainly financially motivated; neither its dark web leak site nor its public statements on dark web forums, social media, or covert communication channels indicate any political stance, ideological messaging, or affiliation with a specific cause.

The Gentlemen employs a double extortion model with a silent encryption mode, as indicated by the file encryptions and ransom notes in confirmed attacks. The group actively solicits initial access brokers (IABs) for Virtual Private Networks (VPNs) and botnets and purchases targets' data from infostealer logs. The collective's target pool has included a national human rights institute, a university, and the healthcare sector, suggesting the group or its affiliates do not exclude public sector organizations despite their typically lower ransom-paying capacity. ZeroFox assesses that The Gentlemen is likely a technically mature threat actor group based on its observable Operations Security (OPSEC) posture, which presents a mixture of defensive security measures and credibility-driven self-exposure.

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

Critical cPanel Zero-Day

What we know:

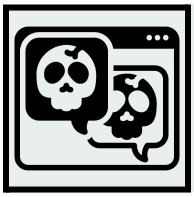
- A critical authentication bypass vulnerability (CVE-2026-41940) affecting web server management software cPanel is being actively exploited.
- Approximately 1.5 million cPanel instances are exposed online, with over 40,000 servers compromised worldwide.
- Since the initial patch release on April 28, 2026, attackers have ramped up efforts, targeting government and military entities in Southeast Asia using public proofs of concept.

Background:

- CVE-2026-41940 can enable attackers to fully hijack servers running cPanel, impacting millions of websites globally, with users urged to patch all affected versions.
- Meanwhile, ZeroFox has observed threat actor “NormalLeVrai” advertising a "second cPanel" information disclosure vulnerability that allegedly exposes website login credentials, including panel links, usernames, and passwords.
- The flaw has allegedly affected 13,522 instances across 94 countries.

Analyst note:

- Given the widespread use of cPanel across hosting environments, exploitation of CVE-2026-41940 is likely to enable attackers to compromise large numbers of websites from a single vulnerable server.
- Unpatched hosting providers are likely to expose multiple tenants, scaling the initial compromise extensively.
- Providers must urgently rotate credentials, scan Indicators of Compromise (IOCs), and block ports 2083 and 2087.



DAEMON Tools Compromised in Supply Chain Attack

What we know:

- Threat actors have compromised installers for the popular DAEMON Tools virtual drive software, embedding a backdoor that has infected thousands of systems across more than 100 countries.
- The attack targets versions 12.5.0.2421 through 12.5.0.2434, with infections reported since April 8.

Background:

- The infection chain initially used an infostealer to identify high-value targets, including government and scientific organizations.
- Threat actors then deployed a more advanced backdoor capable of executing commands or injecting malicious code directly into the target system's memory.

Analyst note:

- Threat actors are likely to act as initial access brokers or move laterally to map the location of the most valuable data, including source code.
- They are also likely to install keyloggers capable of recording typed information and capturing periodic screenshots for real-time victim monitoring.

Fragmented Botnet Infrastructure Fuels Stealthy DDoS Campaign

What we know:

- In mid-April, threat actors launched 2.45 billion malicious requests against a major platform within five hours, in a “low and slow” distributed denial-of-service (DDoS) campaign.
- The attack reportedly peaked at 205,344 requests per second, while evading standard rate-limiting defenses.

Background:

- The campaign leveraged a fragmented infrastructure, distributing traffic across more than 1.2 million IP addresses and 16,402 autonomous system numbers (ASNs), with no single network contributing more than 3 percent of the total traffic volume.
- Attackers reportedly used a “pulsed cadence” technique to evade rate limits, keeping requests per IP low while sustaining a continuous high-volume flood.

Analyst note:

- The campaign likely reflects an evolution in DDoS tradecraft, with attackers using adaptive techniques to evade conventional detection and rate-limiting controls.

- Similar attacks are likely to increase as threat actors adopt infrastructure fragmentation and behavioral evasion tactics that reduce the effectiveness of traditional network defenses.

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 two vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue on May 1 and May 6, 2026. Additionally, on May 5, 2026, CISA released six Industrial Control Systems (ICS) advisories, including CVE-2026-21661, CVE-2025-11043, CVE-2025-11044, CVE-2026-0936, CVE-2026-0936, and CVE-2018-1002208. WhatsApp has disclosed two medium-severity vulnerabilities (CVE-2026-23863 and CVE-2026-23866) that can enable attachment spoofing via Null Byte manipulation and arbitrary URL scheme redirection through flawed artificial intelligence (AI) rich response validation. Progress Software released patches for two vulnerabilities in MOVEit Automation, including a critical authentication bypass flaw (CVE-2026-4670) and a privilege escalation bug (CVE-2026-5174). CVE-2026-31431 (or "Copy Fail") is a local privilege escalation flaw that enables an unprivileged user to gain root access due to a logic bug in the Linux kernel's cryptographic authentication template. Threat actors are exploiting CVE-2026-29014, a remote code execution (RCE) vulnerability in the open-source MetInfo CMS. Apache Software Foundation released security updates for HTTP Server and MINA, patching multiple critical and high-severity vulnerabilities that could enable RCE, denial-of-service (DoS), information disclosure, and authentication bypass. An unauthenticated RCE vulnerability (CVE-2026-22679) is being actively exploited in Weaver E-cology enterprise collaboration platforms.

CRITICAL

CVE-2026-0300

What happened: CVE-2026-0300 is a buffer overflow vulnerability affecting internet-exposed Palo Alto Network's PAN-OS User-ID Authentication Portals. Palo Alto Networks stated that exploitation has been limited so far and mainly affects organizations exposing the User-ID Authentication Portal to untrusted or public networks.

- **What this means:** The flaw is being actively exploited in the wild, with over 5,800 exposed VM-Series firewalls reportedly reachable online, primarily in Asia and North America.
  - **Affected products** are included in Palo Alto's advisory.

CRITICAL

CVE-2026-26956

What happened: CVE-2026-26956 is a sandbox escape vulnerability disclosed in the widely used Node.js sandboxing library vm2 that enables attackers to execute arbitrary code on the host system.

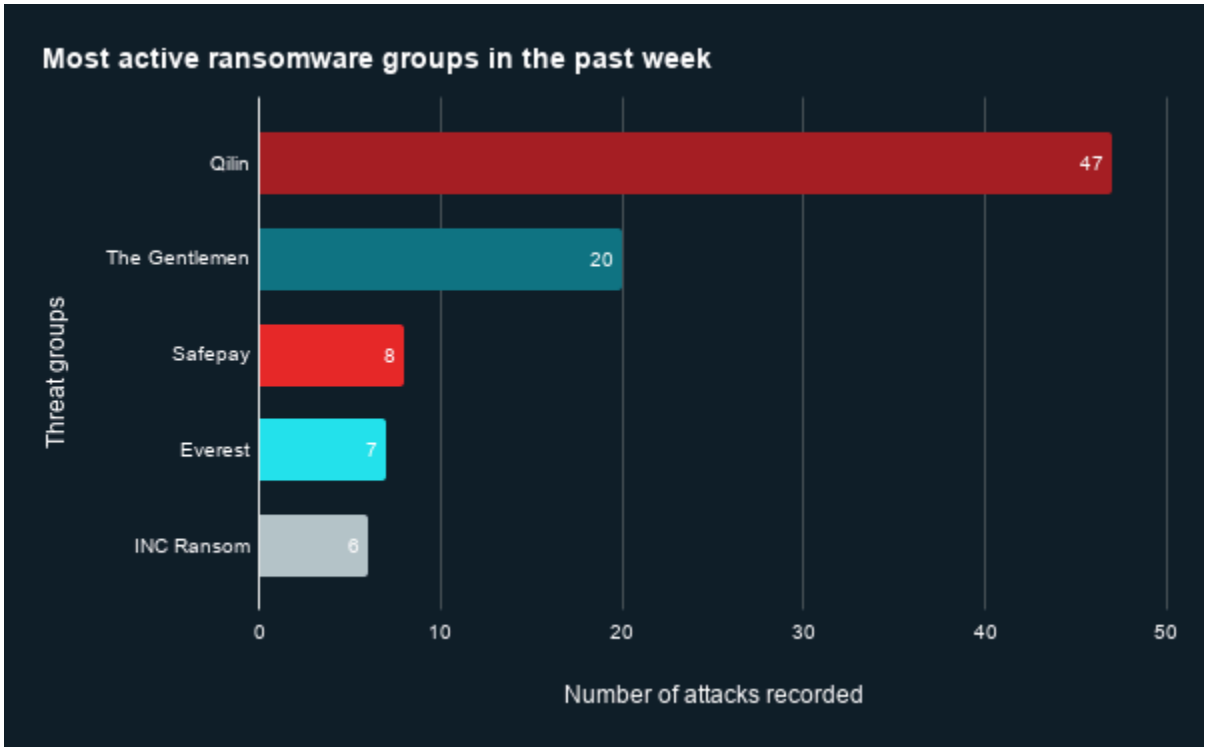
- **What this means:** The flaw abuses WebAssembly exception handling in Node.js 25 to bypass vm2's JavaScript-based protections, leak host-side objects into the sandbox, and regain access to sensitive Node.js internals such as the process object.
  - **Affected products:** Node.js library vm2 version 3.10.4

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

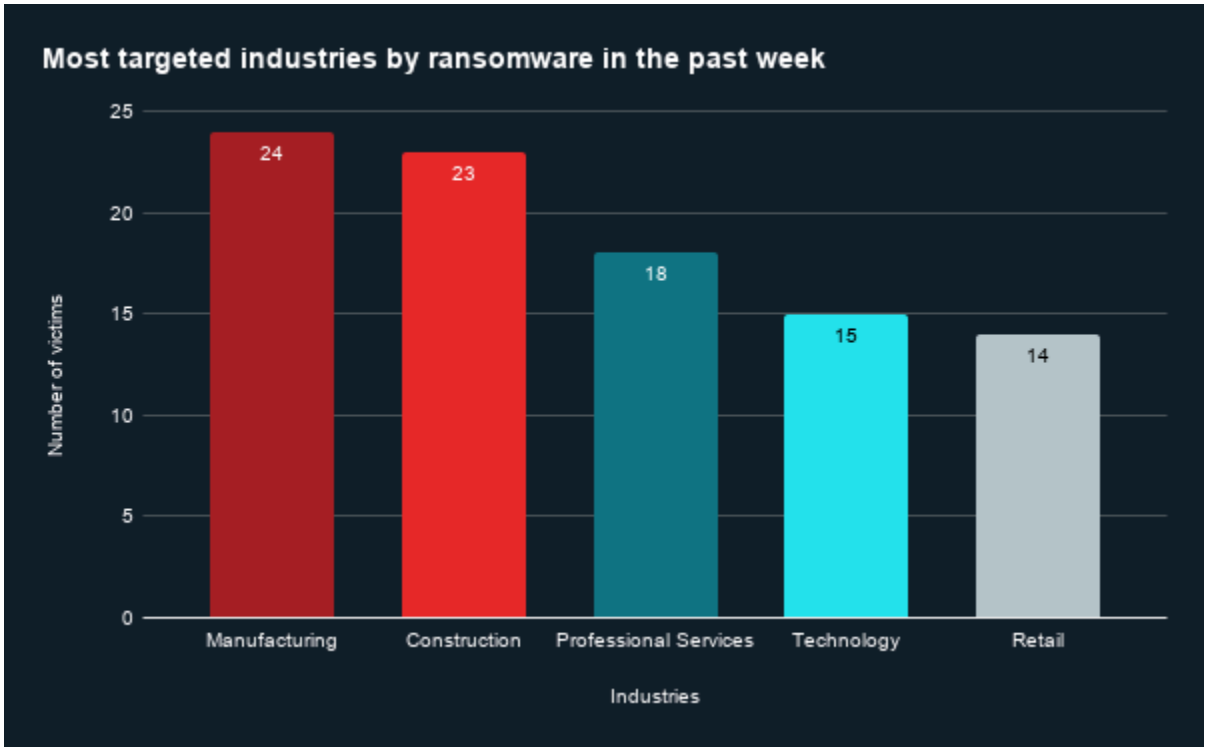
Ransomware Group, Industry, and Regional Trends

Last week in ransomware: In the past week, Qilin, The Gentlemen, SafePay, Everest, and INC Ransom were the most active ransomware groups. ZeroFox observed close to 137 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.



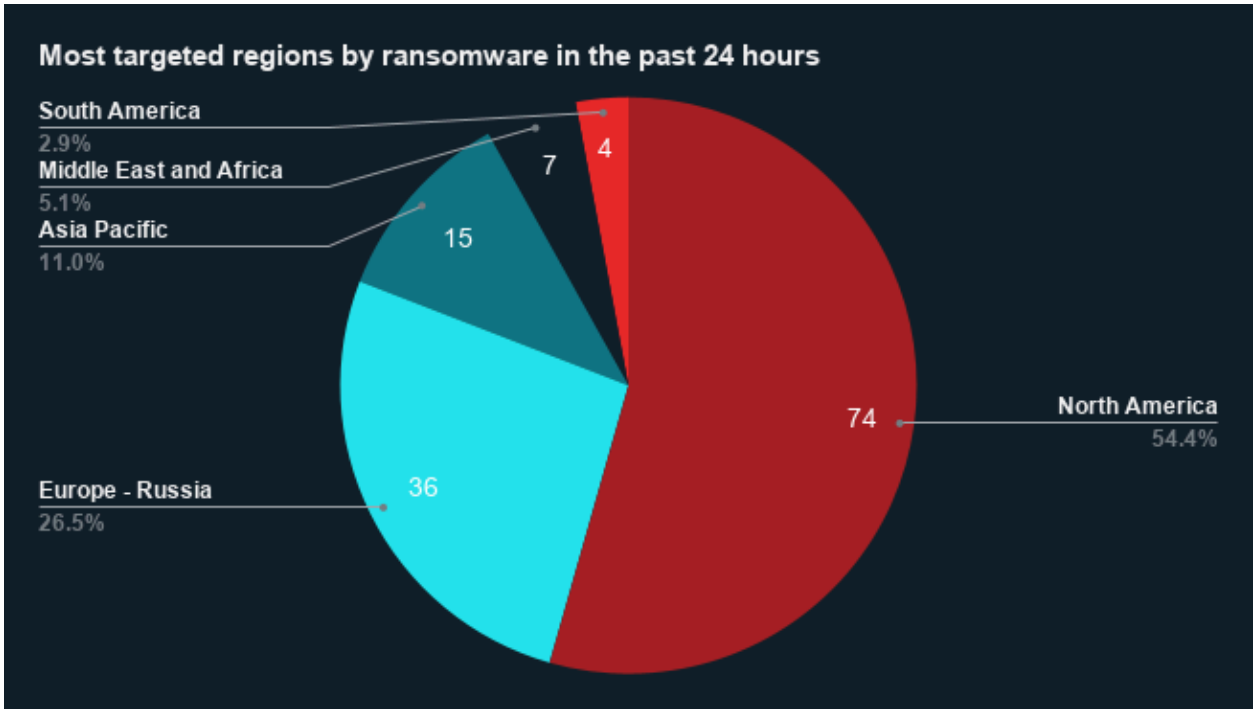
Source: ZeroFox Internal Collections

Industry ransomware trends: In the past week, ZeroFox observed that manufacturing was the industry most targeted by ransomware attacks, followed by 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 74 ransomware attacks observed in North America, while Europe and Russia accounted for 36, Asia-Pacific (APAC) for 15, Middle East and Africa for seven, and South America for Four.



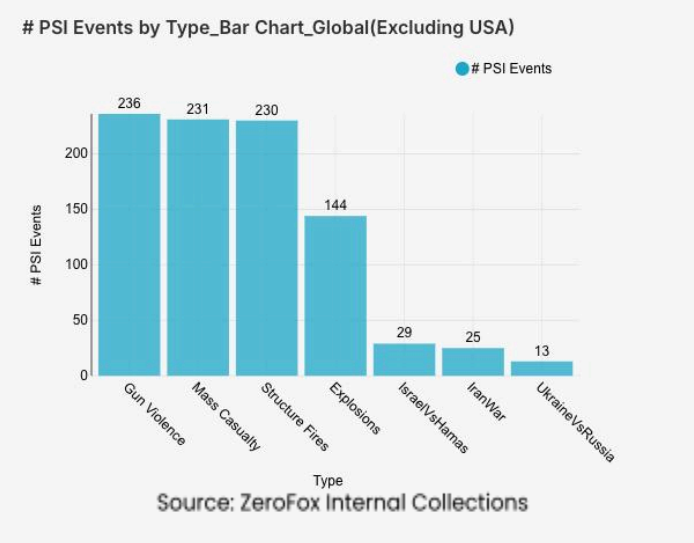
Source: ZeroFox Internal Collections

Significant Data Breaches Reported over the Past Week

Targeted Entity	Ahorramas	Braintrust	Vimeo
Compromised Entities/Victims	Ahorramas employees	Braintrust customers	Approximately 119,200 Vimeo users and customers
Compromised Data Fields	Employees' National Identity Card (Documento Nacional de Identidad (DNI)), financial records, and store blueprints	Application Programming Interface (API) keys used by customers to access cloud-based AI models	Email addresses, names, video titles, technical data, and metadata
Suspected Threat Actor	Qilin	N/A	ShinyHunters
Country/Region	Spain	United States	United States
Industry	Retail	Technology	Media/Entertainment
Possible Repercussions	Financial fraud using DNIs of exposed employees, physical security risks, and disruption in order fulfillment	Unauthorized access to AI model environments impersonating legitimate users, credential abuse across connected cloud services, and supply chain risk to AI development pipelines	Phishing emails impersonating Vimeo targeting exposed users, as well as account takeover attempts

Three major breaches observed in the past week

Physical and Geopolitical Intelligence Key Findings

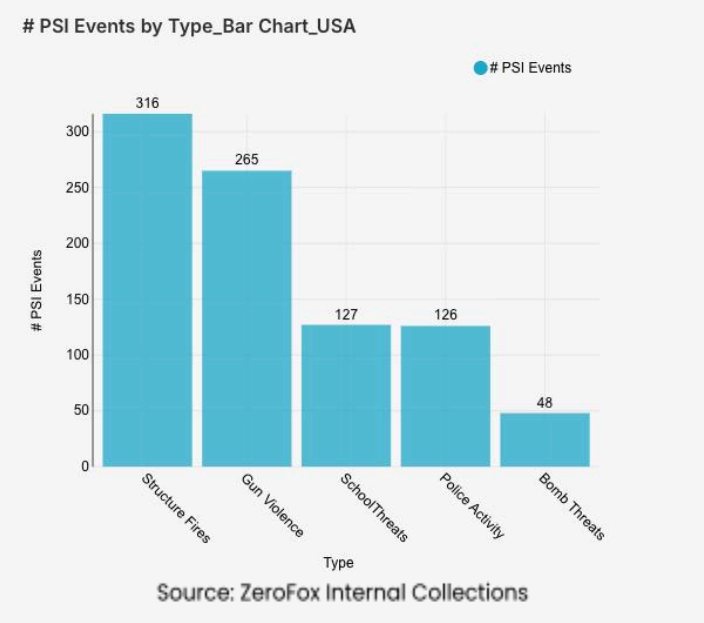


Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 10 percent decrease in mass casualty events this week from the previous week, with the top contributing countries or territories being Mexico, India, and Lebanon, in that order. Approximately 62 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 increased by 12 percent from the previous week, whereas alerts related to the war in Iran decreased by 14 percent. Events related to Russia's war in Ukraine increased by 63 percent. The top three most-alerted subtypes were gun violence, which saw an 11 percent decrease from the previous week; structure fires, which increased by 33 percent; and explosions, which increased by 6 percent.

- **What this means:** This week's data reveals a complex global landscape, wherein regional escalations continue to drive significant instability despite a slight decrease in overall mass casualty events. The most dramatic surge in alerts was related to Russia's war in Ukraine; the United Nations Human Rights Monitoring Mission in Ukraine (HRMMU) reported that, on May 5 alone, a wave of Russian strikes killed 28 people and injured 194 others, marking one of the deadliest single-day surges of the year. Lebanon has seen a resurgence of violence as well, as Israel conducted its first airstrike in Beirut in nearly a month on May 6, killing a top Hezbollah commander. In India, the threat landscape spiked on May 7, as multiple schools in Punjab's Jalandhar and Faridkot were evacuated following coordinated bomb threats; on May 5, there was a confirmed explosion near the Army Cantonment area in Khasa. Mexico, which remains a primary driver of global gun violence alerts due to cartel activity, is also grappling with security instability ahead of the 2026 FIFA World Cup, for which it has deployed almost 100,000 security personnel. Overall, global physical security remains unstable, characterized by both localized civil unrest and high-intensity regional warfare.

Physical Security Intelligence: United States



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 California and Illinois, which together made up 15 percent of this week's nationwide total. Gun violence across the United States overall decreased by 5 percent from the week prior. Police activity alerts increased by 8 percent, and the top contributing states were California and Texas. Structure fires increased by 37 percent, and the top two states for this subtype were New York and California. Notably, bomb threats across the nation increased by 55 percent.

- **What this means:** This week's data highlights a volatile shift in domestic security concerns. There has been a significant surge in structure fires, exemplified by a multi-building fire in New York City, on May 6 which injured three firefighters and displaced several people from their homes. While gun violence overall saw a slight decrease, the lethality of individual incidents remained severe; for instance, a shooting at a party in Edmond, Oklahoma, on May 3 injured 22 and killed one. Overall, 10 mass shootings occurred within the last week in the United States. Meanwhile, police activity increased across the country due to large-scale group gatherings nationwide that were scheduled at the beginning of the month. Notably, there was a significant spike in bomb threats this week, highlighted by a wave of coordinated threats against Kentucky schools on May 5, which state police suspect to be part of an illegal robocall scheme, forcing multiple lockdowns and investigations. Ultimately, the dramatic surge in threats to infrastructure and generalized public disorder suggests a shifting landscape for emergency responders and urban safety.

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%