ZEROFOX

Weekly Intelligence Brief

Classification: TLP:GREEN

March 7, 2026

ZEROFOX®
Weekly Intelligence Brief

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 March 5, 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

ZeroFox Intelligence Flash Report - SITREP #9 - Military Strikes on Iran - March 5, 2026

Major economic indicators such as oil prices and global stock markets have only shifted moderately since declining on March 2, the first day of open trading. This data is consistent with belief that the Iran conflict will be short in duration or Iranian offensive military capabilities will be eliminated. Data on targeting of Iran's offensive weapons systems and the steep decline in Iranian attacks support this narrative. However, if Iran maintains enough offensive firepower for escalation and spreading the conflict, economic optimism will prove misplaced, and there will almost certainly be dramatic economic declines. Iran can likely maintain its capabilities to dissuade commercial aviation and shipping for weeks, whereas economic optimism is based on the assumption that it will not. Iran will likely reject maximalist demands from Israel in favor of concessions that appeal to a U.S. priority for normalcy in the region. U.S. President Donald Trump has reportedly offered support to Kurdish ground forces in Iran, staging from areas in Iraq. Such attacks will further strain Iranian defenses, which are struggling to combat airstrikes against its political and military establishment, and will almost certainly result in an escalation of Iranian targeting in Iraq while motivating Iran to escalate the conflict in the short term. To know more about how the conflict has progressed, read previous SITREPs here: SITREP #1, SITREP #2, SITREP #3, SITREP #4, SITREP #5, SITREP #6, SITREP #7, and SITREP #8.

ZeroFox Intelligence Flash Report - Cyber SITREP #1 - Military Strikes on Iran - March 5, 2026

The United States and Canada have issued warnings that Iran-aligned cyber threat actors are very likely to target Western critical infrastructure and financial institutions in retaliation for the ongoing U.S.-led attacks in Iran. Threat actors and hacktivist collectives—primarily those who self-describe as pro-Iranian, pro-Islamic, pro-Palestinian, or pro-Russian—are employing a combination of distributed denial-of-service (DDoS) attacks, website defacements, data exfiltration, and claimed intrusions into Industrial Control Systems (ICS). Since February 26, 2026, at least 241 separate cyber incidents have likely been linked to the ongoing military campaign against Iran. These incidents include ransomware attacks, initial access broker (IAB) sales, and vulnerabilities/exploits affecting multiple regions and industries. The notable increase in cyber activity is likely intended to support Iran and retaliate against nations perceived as backing U.S. military operations.

ZeroFox Intelligence Flash Report - North Korean Threat Actor Revealed as Medusa Affiliate

On February 24, 2026, North Korean threat actor "Lazarus Group" reportedly widely deployed Medusa ransomware in a series of attempted attacks against healthcare organizations. These attacks indicate that state-sponsored threat actors are almost certainly using cybercrime infrastructure to generate revenue for the North Korean government. By combining with Medusa, Lazarus Group has likely gained access to an established ransomware infrastructure with which to conduct financially motivated attacks. However, Medusa is an independent threat actor, and not all Medusa ransomware-as-as-service (RaaS) attacks should be attributed to Lazarus Group. Lazarus Group's deployment of Medusa RaaS likely indicates the collective is seeking to improve the operational security of its financially motivated attacks by concealing its activities behind the established brand of the Medusa RaaS operation. Given the group's history of conducting state-sponsored attacks that advance North Korean government objectives, it is very likely their financially motivated operations are intended to generate revenue for the communist regime in Pyongyang.

Monthly Geopolitical Assessment: March 2026

The growing U.S. military presence in the Middle East makes it likely that there will be some form of military action against Iran. In turn, Iran has made it clear that it will target the region's energy supply. Following the successful Mexican special forces operation that killed Mexico's top cartel leader, El Mencho, retaliatory acts of cartel violence are likely to dissuade further counter-narcotics operations. Mexico's residents are the primary victims of cartel-related crime, and deliberate targeting of Westerners is rare; however, retaliatory cartel violence in major Mexican cities will likely injure or kill innocent bystanders. Trade uncertainty will very likely be driven by whether firms will aggressively seek tariff refunds and if U.S. authorities will impose new tariffs to counter the U.S. Supreme Court's recent ruling that country-specific U.S. tariff rates are illegal. Continued terror attacks in Pakistan make cross-border fighting with Afghanistan almost certain, while also increasing the probability of renewed hostilities with India. There is a likely chance of renewed fighting involving Ethiopia before elections in June 2026. Conflict in Ethiopia will likely have a wider impact due to East Africa's complex web of alliances and rivalries.

ZeroFox Intelligence Brief - Underground Economist: Volume 6, Issue 5

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

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

Authorities Take Down LeakBase, Seize Domains and Data

What we know:

- The United States and allies have shut down the illicit forum LeakBase, seizing its data and two domains used to operate the platform.
- Authorities have also taken "measures" against 37 most active users of the platform.

Background:

- The forum's landing page has been replaced with a law enforcement seizure banner stating that users' accounts, posts, credit details, private messages, and IP logs have been secured.
- Active since 2021 and backed by the ARES threat group, LeakBase grew to have over 142,000 members, operating as a free-to-join cybercrime forum and marketplace offering leaked databases, exploits, and other illicit services.

Analyst note:

- Following the takedown, displaced members are likely to migrate to established data leak and credential trading communities such as BreachForums, Exploit[.]In, and XSS.
- Former members are likely to visit discussion forums such as Dread to share updates and possible alternatives, verify arrests, warn others, and strategize where to regroup.

LastPass Warns of New Phishing Campaign

What we know:

- Password manager app LastPass is warning users of a phishing campaign designed to steal login credentials.
- This is the second such warning in 2026, with the last one reported in January 2026. LastPass added that its infrastructure has not been compromised and that there has been no impact on its systems.

Background:

- The phishing emails urge users to respond to suspicious activity with urgency by clicking on malicious links.
- The links redirect to a domain mimicking LastPass's login page (verify-lastpass[.]com). Indicators of compromise (IoCs) are detailed in this advisory.

Analyst note:

- Two-factor authentication (2FA) is likely to prevent less advanced phishing campaigns from being successful.
- LastPass account compromise likely risks account takeover attempts of other platforms and theft of sensitive files.
- Clicking on malicious links is also likely to lead to malware installation, which can further result in system-level compromise.

Pakistani News Channels Hit by Transmission Hijack; Retaliatory Attacks Target Indian Broadcaster

What we know:

- Several major Pakistani television channels have experienced a significant broadcast disruption after unknown actors of unconfirmed allegiance allegedly hijacked satellite transmissions.
- Following the incident, threat group Pakistan Cyber Force allegedly carried out retaliatory cyber activity, targeting major Indian broadcaster ABP News, defacing a website, and launching distributed denial-of-service (DDoS) attacks.

Background:

- The breach occurred during peak Ramadan viewing hours, when hackers allegedly interfered with transmissions carried via PAKSAT satellite, displaying unauthorized on-screen messages criticizing the Pakistan Armed Forces and urging opposition to the military.

Analyst note:

- The politically charged hijacked messages indicate an influence-driven operation that aligns with broader regional conflicts.

- Given Pakistan's long-standing conflict with India and now Afghanistan, the incident likely involves nationalist hacktivist collectives, proxy actors, and false-flag efforts aimed at intimidation or provoking escalation against factions belonging to these countries.

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 seven vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on March 3, 2026 and March 5. It also added nine Industrial Control System (ICS) advisories on March 3 and March 5. An already-patched insufficient policy enforcement vulnerability in Google Chrome's WebView tag, tracked as CVE-2026-0628, was found to enable privilege escalation. Cisco has patched two critical-severity vulnerabilities (CVE-2026-20079 and CVE-2026-20131) that can be remotely exploited by threat actors. CVE-2026-20079 is an authentication bypass flaw that enables attackers to gain root access to the operating system, while CVE-2026-20131 is a remote code execution (RCE) flaw.

HIGH

CVE-2026-21385

What happened: This is a high-severity zero-day vulnerability in a Qualcomm display component that was actively exploited and has now been patched. It is an integer overflow vulnerability that can further trigger memory corruption and escalate privileges on the system.

- **What this means:** The vulnerability is likely to be used to launch targeted attacks to compromise Android devices.
    - **Affected products**: 235 Qualcomm chipsets

CRITICAL

CVE-2026-28289

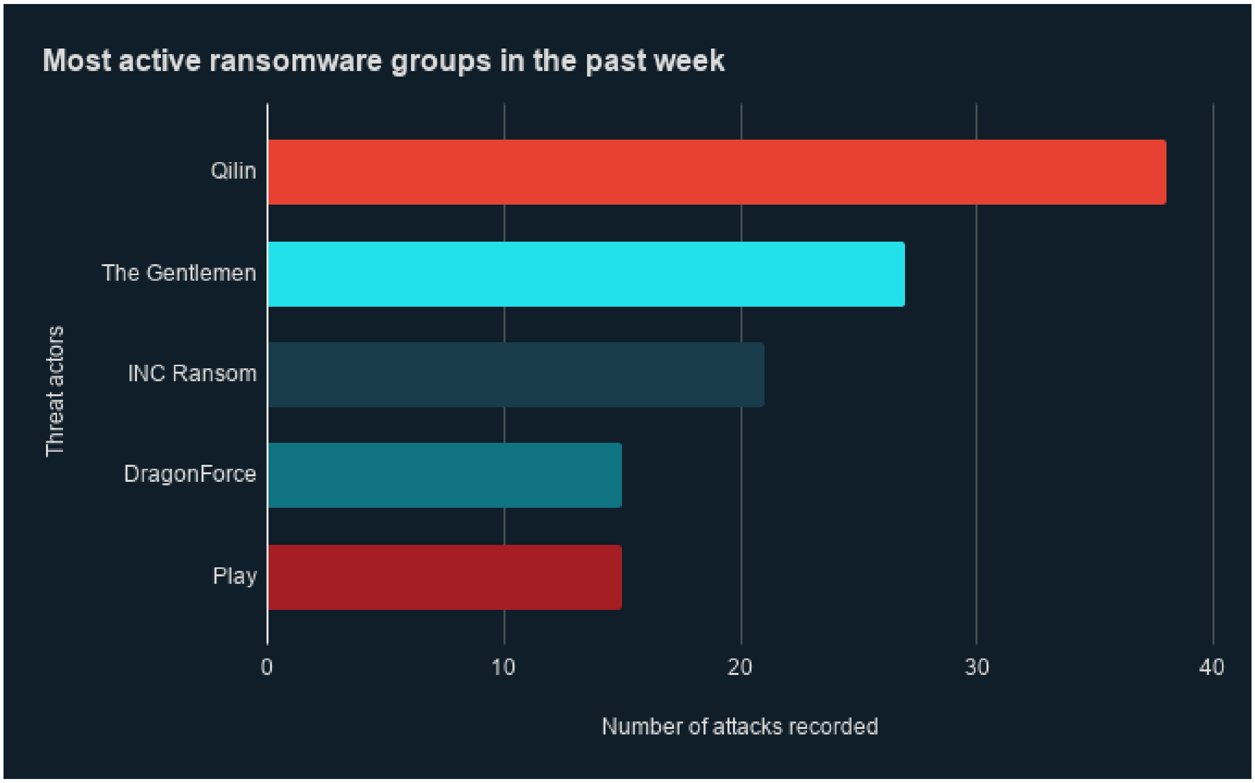
What happened: This is a zero-click RCE vulnerability in FreeScout, an open-source help desk and shared inbox. The flaw bypasses a prior patch using a zero-width space to upload a malicious file to evade validation and be saved as a valid dotfile. By sending a crafted email to a mailbox configured in FreeScout, attackers can write the payload to disk without authentication or user interaction and then access it to execute remote commands on the server.

- **What this means:** If exploited, this vulnerability is likely to enable attackers to gain full control of vulnerable FreeScout servers, leading to theft of helpdesk tickets, mailbox data, and other sensitive information handled by the platform.
    - **Affected products** All FreeScout 1.8.206 installations running on Apache with AllowOverride All enabled

Ransomware and Breach Intelligence

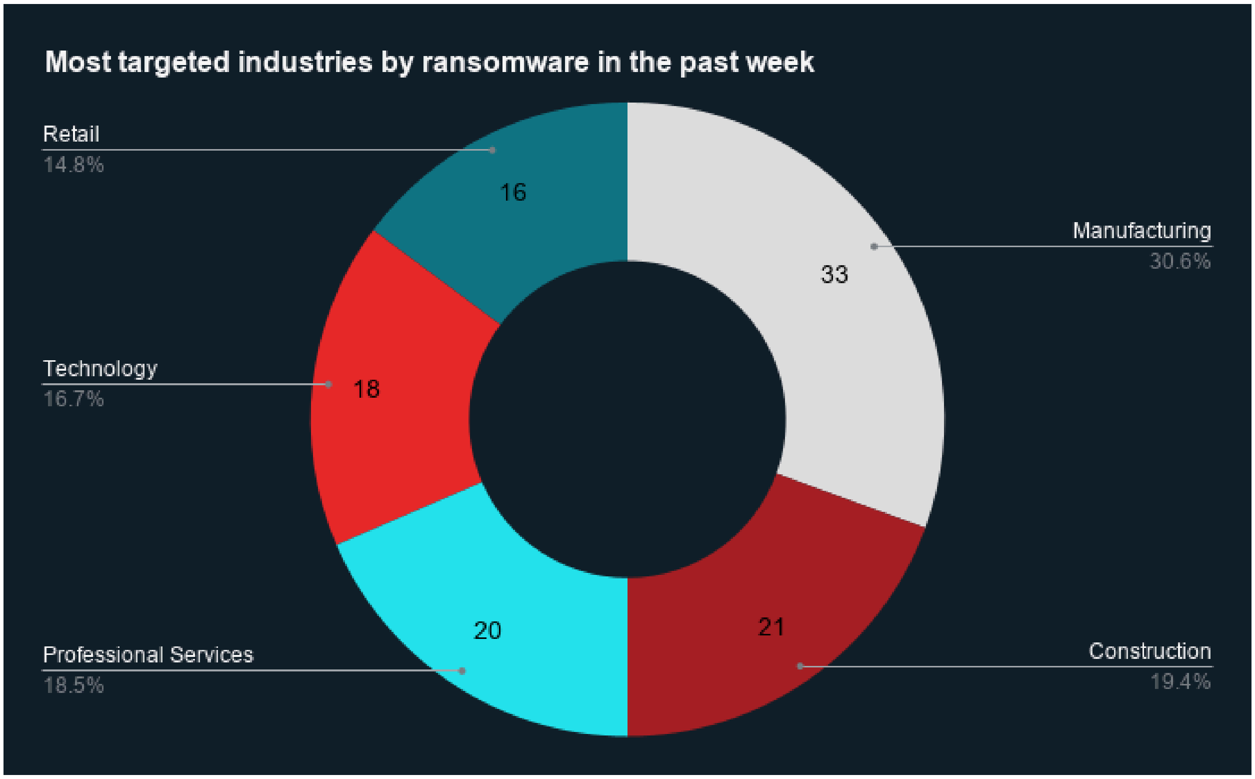
Ransomware and Breach Intelligence Key Findings

Ransomware Groups, Activities, and Trends



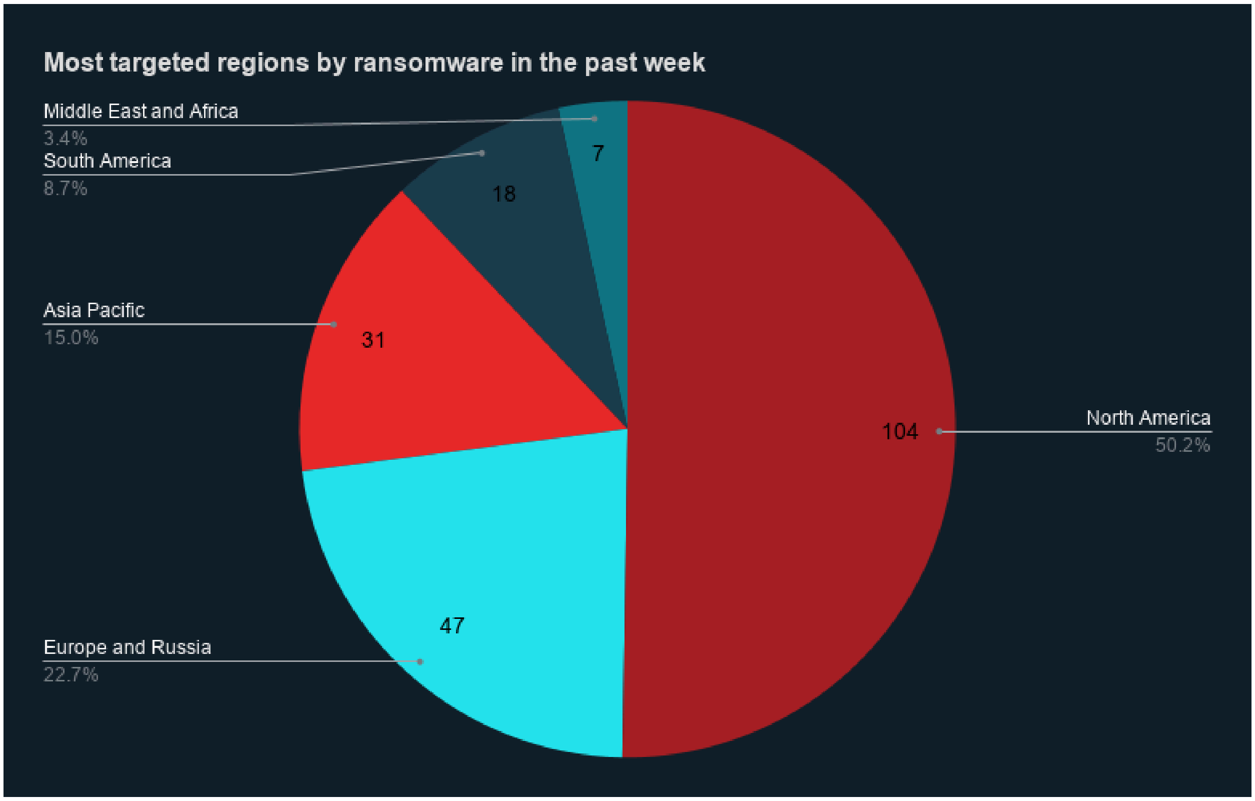
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Qilin, The Gentlemen, INC Ransom, DragonForce, and Play were the most active ransomware groups. ZeroFox observed close to 178 ransomware victims disclosed on the deep and dark web, 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, manufacturing was the industry most targeted by ransomware attacks, followed by construction, professional services, technology, and retail.



Source: ZeroFox Internal Collections

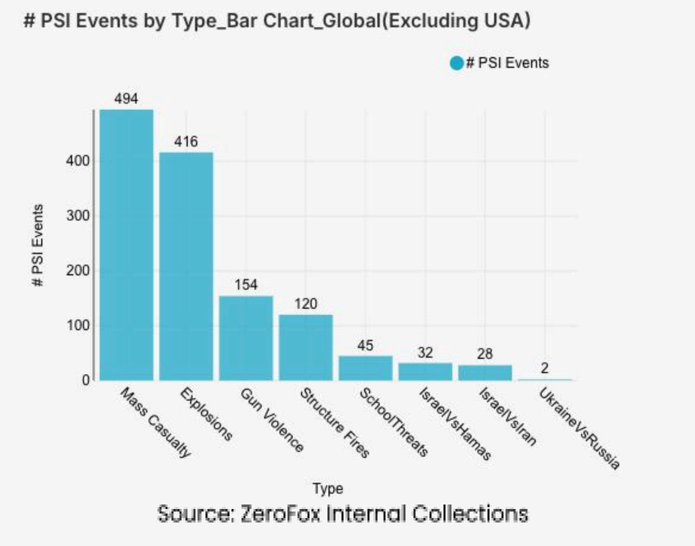
Regional ransomware trends: In the past week, ZeroFox observed that North America was the region most targeted by ransomware attacks, followed by Europe and Russia. North America recorded 104 attacks, Europe and Russia recorded 47, Asia Pacific noted 31, South America saw 18, and Middle East and Africa recorded seven.

Notable Data Breaches Reported in the Past Week

Targeted Entity	**LexisNexis**	**Cloud Imperium Games (CIG)**	**Cegedim Santé**
Compromised Entities/Victims	2 GB of customer and business information	Users	15.8 million administrative records of French residents, allegedly including senior political figures
Compromised Data Fields	Customer names, user IDs, business contact information, products used, customer surveys with respondent IP addresses, and support tickets	Metadata, contact details, username, date of birth, and name	165,000 files, including physician notes, highly sensitive health information such as HIV status and sexual orientation, and personally identifiable information (PII)
Suspected Threat Actor	FulcrumSec	N/A	DumpSec
Country/Region	United States	Multiple	France
Industry	Professional Services	Hospitality	Healthcare
Possible Repercussions	Brute force attacks. Exposed individuals and entities are also likely to be targeted in phishing and social engineering attacks	Financially motivated phishing and social engineering attacks	Blackmail, insurance fraud, political targeting, and phishing attacks

Three major breaches observed in the past week

Physical and Geopolitical Intelligence Key Findings



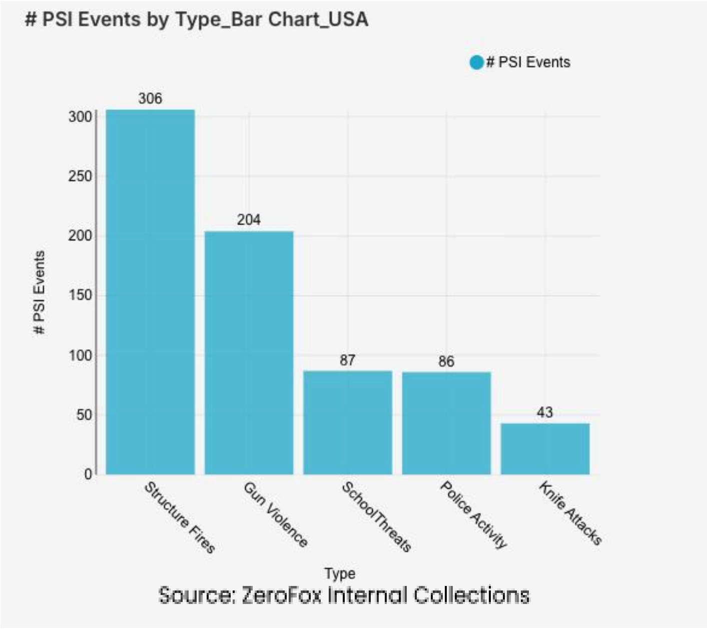
Source: ZeroFox Internal Collections

Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 100 percent increase in mass casualty events this week from the previous week, with the top contributing countries or territories being Iran, Israel, and Iraq in that order. Approximately 84 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 39 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict (including raids and attacks) decreased by 3 percent from the previous week, and alerts related to the recent Iran conflict increased by 28 instances. Events related to Russia's war in Ukraine decreased by 89 percent. The top three most-alerted subtypes were explosions, which saw a 187 percent increase from the previous week; gun violence, which decreased by 15 percent; and structure fires, which also decreased by 15 percent.

- **What this means:** The global landscape of conflict has undergone a seismic shift this week, marked by a sharp increase in mass casualty events primarily driven by the sudden escalation in the Middle East. As of March 5, the direct military confrontation between a U.S.-Israeli coalition and Iran has made Iran, Israel, and Iraq the top contributors to global violence, with explosions spiking dramatically. Notable incidents include the reported strike on the Shajareh Tayyebeh school in Minab that killed nearly 170 children, and the killing of Supreme Leader Ali Khamenei during the opening salvos of Operation Epic Fury (also known as Operation Roaring Lion). Conversely, events related to Russia's war in Ukraine saw a significant decrease; this "lull" may be attributed to Russia's strategic pivot as its primary military partner, Iran, comes under direct attack. The overall state of global physical security this week is currently characterized by a volatile and rapid geographic pivot, where a surge in high-intensity kinetic events in the Middle East has indirectly de-escalated or overshadowed traditional conflict theaters, leading to an unstable and highly unpredictable international security environment.

Physical Security Intelligence: United States

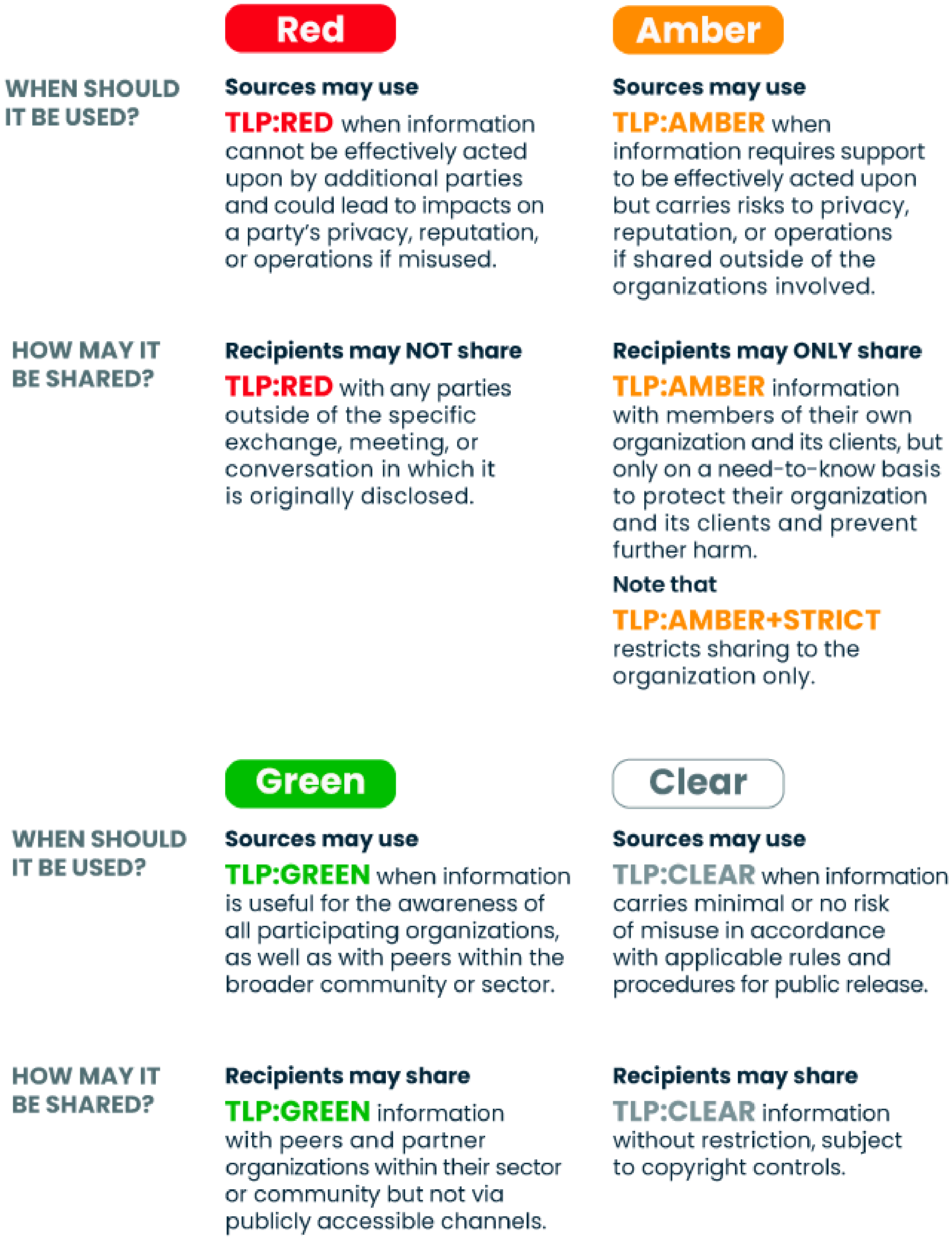


Source: ZeroFox Internal Collections

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 California and Illinois, which together made up 21 percent of this week's nationwide total. Gun violence across the United States overall increased by 34 percent from the week prior. Police activity alerts decreased by 31 percent, and the top contributing states were California and Texas. Structure fires increased by 15 percent, and the top two states for this subtype were California and New York. Notably, knife attacks increased by 48 percent nationwide.

- **What this means:** In the past week, the United States has experienced a volatile shift in domestic security, characterized by a surge in gun violence and epitomized by a mass casualty event in Austin, Texas, on March 1: a lone shooter opened fire at Buford's Backyard Beer Garden on West Sixth Street, resulting in four deaths and 16 injuries. This is currently being investigated by the FBI as a potential act of terrorism due to ideological indicators related to Iran found at the scene. Six mass shootings occurred within the last week, two of which came from California, one of the top contributing states to overall gun violence alerts. Amidst these kinetic events, the nation also observed a variety of large-scale collective gatherings and civic expressions in major cities. Knife attacks saw a sharp rise this week as well, with instances including a "road rage" mass stabbing in Virginia on March 3 which resulted in four victims and a deceased pet, with the State Department later confirming the suspect was a Foreign Service Officer. Overall, the current state of domestic physical security for this week is defined by a volatile surge in high-intensity individualized violence and targeted mass-casualty events.

Appendix A: Traffic Light Protocol for Information Dissemination

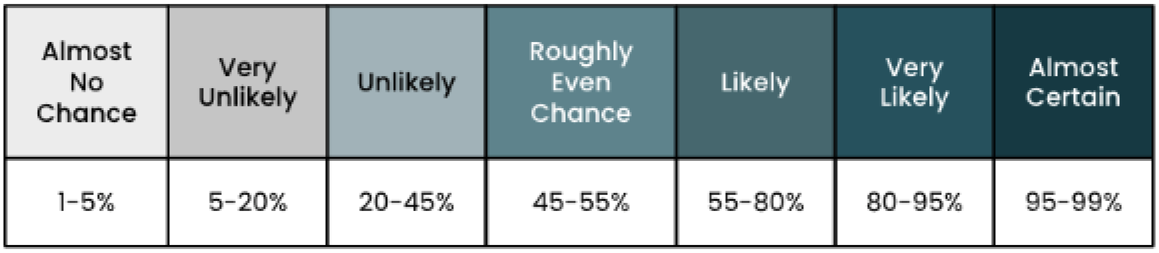


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** **TLP:AMBER** when information requires support to be effectively 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%