ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

March 28, 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 (EST) on March 27, 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 #29 - Military Strikes on Iran - March 27, 2026

On March 26, 2026, U.S. President Donald Trump issued a statement extending the deadline for Iran to open the Strait of Hormuz (SoH) by an additional 10 days; the new deadline is April 6, 2026. Iran rejected a 15-point U.S. proposal to end the conflict and countered with five conditions. Despite these proposals, the risk of escalation remains high. The U.S. Department of War ordered thousands of additional troops to the region, likely for potential ground operations or to challenge Iran's control of the SoH, while Iran has begun charging transit fees for passage to solidify its control. Earlier, on March 21, 2026, President Trump threatened attacks on Iran's energy infrastructure. Iran is expected to retaliate against facilities across the Gulf, which would almost certainly worsen the global energy crisis while ensuring it feeds into other sectors (led by global food trade). The Handala Hack Team posted purported personal information about U.S. citizens, threatening to physically target U.S. employees of Lockheed Martin in Israel and their families if they did not cease their work supporting the war.. To know more about how the conflict has progressed, read previous SITREPs.

ZeroFox Intelligence Brief - Underground Economist: Volume 6, Issue 7

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

TeamPCP Expands Trivy Campaign; Iranian Systems Under Target

What we know:

- Threat group TeamPCP is continuing to expand the Trivy supply chain attack by pushing malicious Docker images, hijacking Aqua Security's GitHub repositories, wiping Iran-specific Kubernetes clusters, and compromising the popular "LiteLLM" Python package on PyPI.
- TeamPCP has also been linked to compromising Checkmarx AST/KICS and over 10,000 GitHub workflows using trivy-action.
- The cloud environments of thousands of organizations have reportedly been infected in the attack.
- TeamPCP is also suspected of working with notorious extortion crews such as Lapsus$.

Background:

- Aqua Security's Trivy vulnerability scanner was compromised in a supply chain attack, which distributed credential-stealing malware through official releases and GitHub Actions.
- The same threat group is reportedly targeting Iranian systems with a wiper malware, while installing the CanisterWorm backdoor on other non-Iranian systems.

Analyst note:

- The Trivy supply chain attack is likely to enable the threat actors to compromise downstream entities and move deeper into corporate networks.
- The wiper attack against Iranian systems likely indicates state-aligned or geopolitically motivated operations disguised as cybercriminal activity to obscure attribution.
- TeamPCP is likely to be able to maintain a foothold in compromised networks if there is an incomplete revocation of Continuous Integration/Continuous Delivery (CI/CD) tokens and GitHub secrets. This makes full-scope credential rotation critical for defenders.

United States, Australia Issue Cybersecurity Outline for Satellite Communications Systems

What we know:

- U.S. and Australian space agencies have released a report outlining cybersecurity risks and mitigation strategies for Low Earth Orbit (LEO) satellite communication (SATCOM) systems across space, ground, user, and communication and supply chain segments.

Background:

- In the space segment, satellites' reliance on radio frequency links makes them vulnerable to jamming, spoofing, and command injection.
- Ground segment hubs are exposed to malware, credential theft, and denial-of-service (DoS) attacks, while user devices can be exploited via phishing or misconfigurations.

Analyst note:

- LEO SATCOM systems are almost certainly to be targets of kinetic and cyberattacks during geopolitical flashpoints, as adversarial nations aim to sever emergency communications across government, military, and private sectors.
- For advanced non-state cybercriminals, satellite communications systems are high-value targets for extortion.

Authorities Seize Key Infrastructure Powering Large-Scale Global DDoS Campaigns

What we know:

- Law enforcement has disrupted Aisuru, KimWolf, JackSkid, and Mossad botnets, which were used to launch large-scale distributed denial-of-services (DDoS) attacks against global victims.
- Authorities also executed seizure warrants targeting domains, servers, and infrastructure, aiming to cut off botnet communications and prevent further attacks.

Background:

- The four botnets infected over three million devices globally, primarily Internet of Things (IoT) devices such as routers, webcams, and digital video recorders, many of which were hijacked despite being behind firewalls.

- The operators of these illicit infrastructure monetized access through a cybercrime-as-a-service model, using compromised devices to launch hundreds of thousands of DDoS attacks worldwide.

Analyst note:

- This operation will likely see an increase in demand and pricing for other botnet accesses on underground markets, as supply is temporarily constrained.
- There is also likely to be a shift toward exploiting new devices and vulnerabilities as attackers look to build new infrastructure.

Exploit and Vulnerability Intelligence

Exploit and Vulnerability Intelligence Key Findings

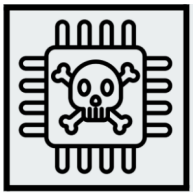
In the past week, ZeroFox observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in technology, software development, and critical infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA) added six new vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue on March 20 and March 25, 2026. Additionally, on March 24, 2026, CISA released seven Industrial Control Systems (ICS) advisories featuring a total of seven vulnerabilities, including CVE-2026-3650, CVE-2026-2417, CVE-2026-1286, and CVE-2025-46819. Meanwhile, Apple has released updates fixing more than 80 vulnerabilities across iOS, macOS, and other platforms, including high-severity flaws in WebKit and the kernel that could enable data leaks, sandbox escapes, and remote attacks. Google released a Chrome 146 update fixing eight high-severity vulnerabilities, including memory safety issues such as buffer overflows and use-after-free bugs. Citrix has released patches for two vulnerabilities (CVE-2026-3055 and CVE-2026-4368) in NetScaler ADC and Gateway. CVE-2026-20963 is an already-patched deserialization vulnerability in SharePoint servers that is under active exploitation by unknown threat actors. Exploitation enables unauthenticated threat actors to remotely execute code on the server without any user interaction. Internet Systems Consortium (ICS) has released updates for BIND 9 to patch multiple vulnerabilities, including high-severity flaws. Cisco has released patches for multiple vulnerabilities in Cisco IOS and Cisco IOS XE.

CRITICAL

CVE-2026-21992

What happened: Oracle has released emergency patches for a critical vulnerability in Oracle Identity Manager and Oracle Web Services Manager.

- **What this means:** The flaw enables unauthenticated remote code execution (RCE) via HTTP, giving attackers full control of the affected systems without user interaction. Threat actors are likely to exploit this flaw to escalate privileges, move laterally within corporate networks, and access sensitive data in unpatched environments.
    - **Affected products**: Oracle Identity Manager versions 12.2.1.4.0 and 14.1.2.1.0 and Oracle Web Services Manager versions 12.2.1.4.0 and 14.1.2.1.0



CRITICAL

CVE-2026-33017

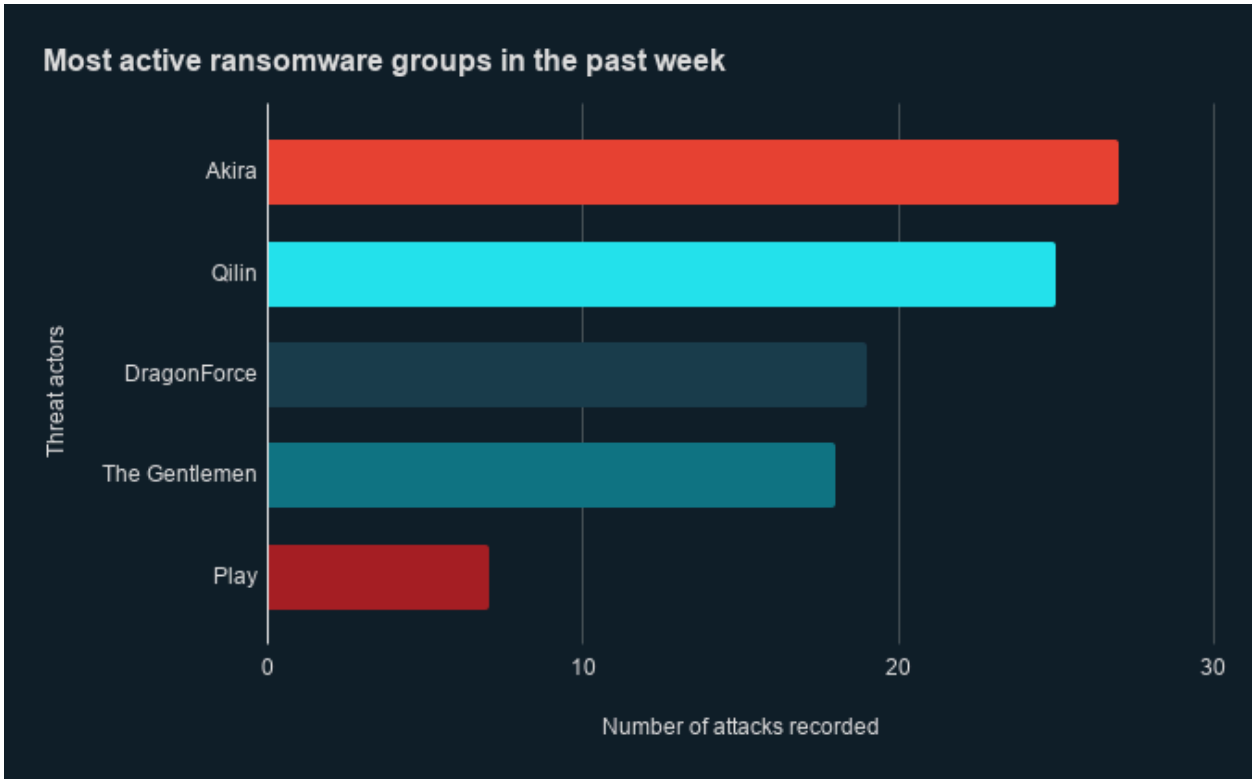
What happened: This vulnerability in Langflow enables unauthenticated RCE via code injection, enabling attackers to run arbitrary Python code with full server privileges.

- **What this means:** The flaw has reportedly already been exploited in the wild within 20 hours of disclosure, with attackers conducting credential harvesting, data exfiltration, and deploying follow-on payloads on vulnerable systems. The short window between disclosure and exploitation likely suggests that threat actors are weaponizing vulnerabilities faster than most organizations have time to patch, increasing the risk of immediate widespread compromise.
  - **Affected products:** Langflow version prior to and including 1.8.1

Ransomware and Breach Intelligence

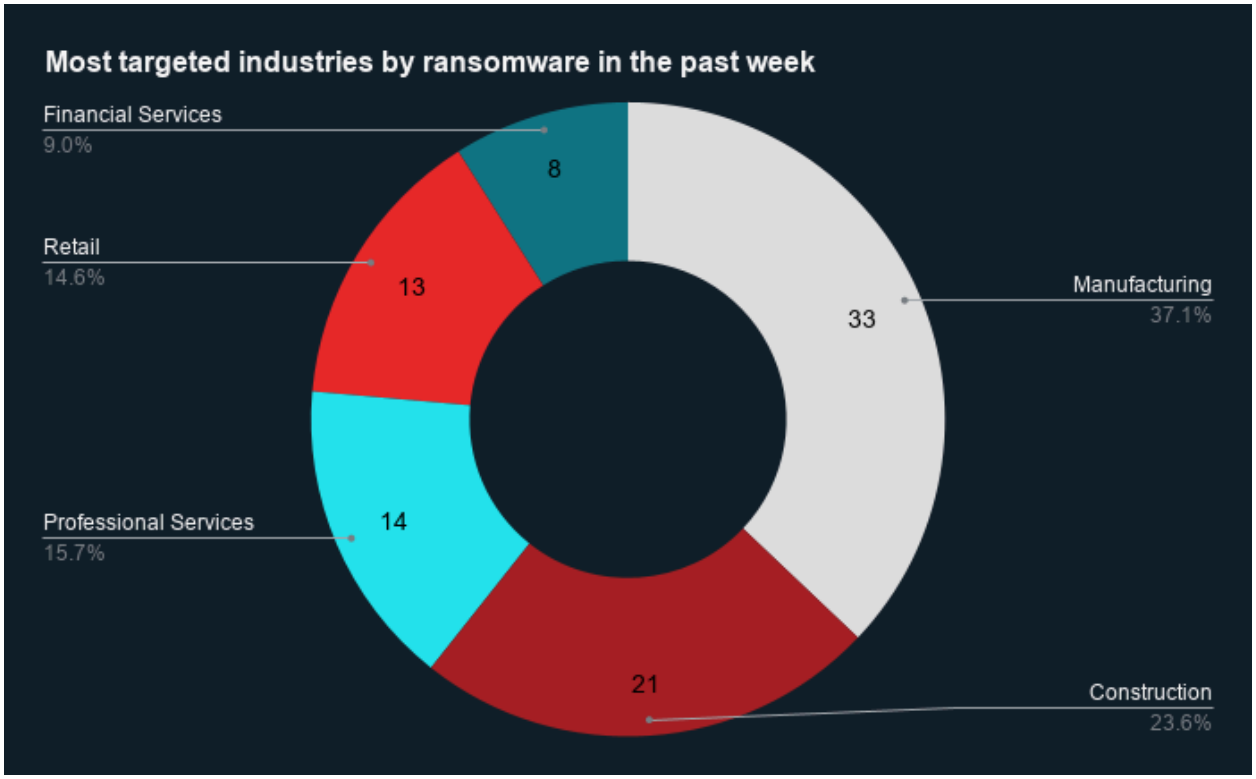
Ransomware and Breach Intelligence Key Findings

Ransomware Group, Industry, and Region Trends



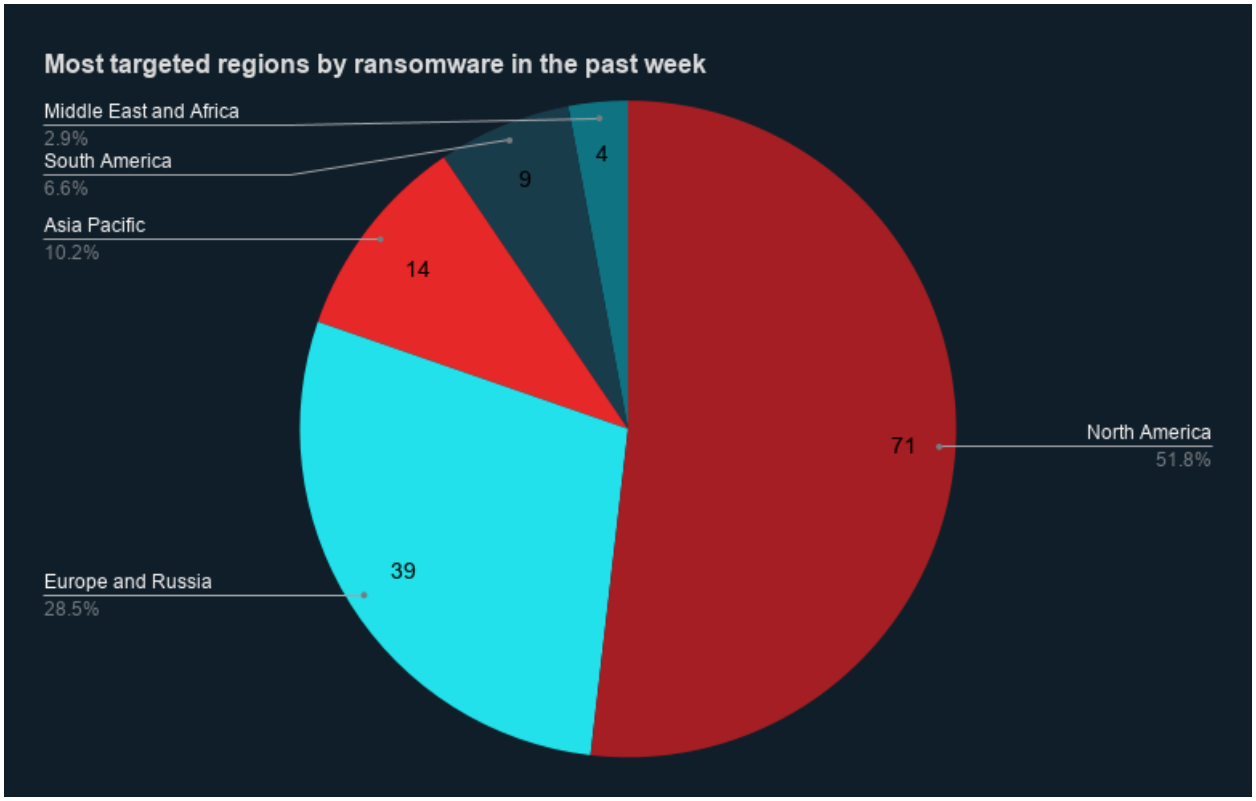
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Akira, Qilin, DragonForce, The Gentlemen, and Play were the most active ransomware groups. ZeroFox observed close to 138 ransomware victims disclosed, most of whom were located in North America. The Akira ransomware group accounted for the largest number of attacks, followed by Qilin.



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 71 ransomware attacks observed in North America, while Europe and Russia accounted for 39, Asia-Pacific (APAC) for 14, South America for nine, and Middle East and Africa for four.

Recap of major ransomware events observed in the past week: An exposed server has reportedly revealed the entire toolset of a member of the Beast ransomware group, exposing the threat actor's tactics, techniques, and procedures (TTPs). Semiconductor testing company Trio-Tech International confirmed a ransomware attack at its Singapore subsidiary following a claim by the Gunra ransomware group on March 17, 2026. The Interlock ransomware group is reportedly exploiting a vulnerability, tracked as CVE-2026-20131, in Cisco's Secure Firewall Management Center.

Significant Data Breaches Reported in the Past Week

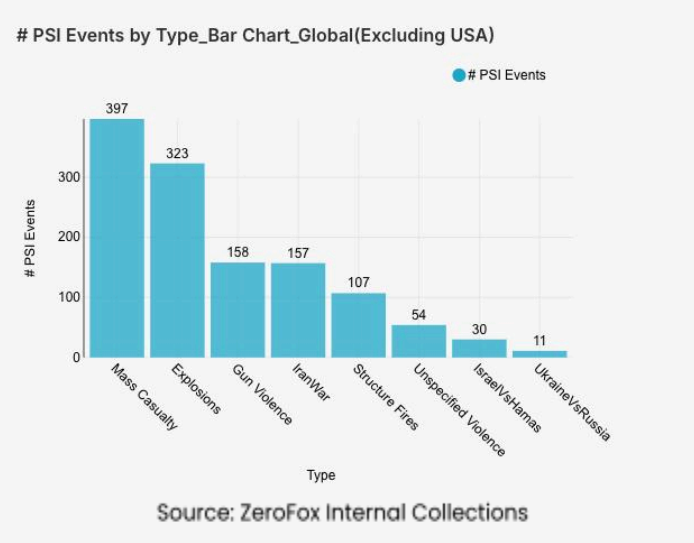
Targeted Entity	Mazda	Navia Benefit Solutions	OpenLoop Health Inc
Compromised Entities/Victims	Employees and business partners	2.7 million individuals	1.6 million patients
Compromised Data Fields	Personal information, including company-issued user IDs, names, email addresses, company names, and business partner IDs	Full name, date of birth, Social Security number (SSN), phone number, email address, Health Reimbursement Arrangement (HRA) participation, Flexible Spending Account (FSA) information, and Consolidated Omnibus Budget Reconciliation Act (COBRA) enrollment information	Names, email addresses, phone numbers, physical addresses, dates of birth, medical information, IP addresses, FedEx tracking numbers, and additional personal data
Suspected Threat Actor	N/A	N/A	BreachForums user Stuckin2019
Country/Region	Japan, Thailand	United States	United States
Industry	Transportation	Healthcare	Healthcare
Possible Repercussions	Phishing and social engineering scams or spam emails	Insurance fraud, identity theft, phishing, and social engineering attacks	Insurance fraud, FedEx package theft, identity theft, phishing, and social engineering attacks

Three major breaches observed in the past week

Other major data breaches observed in the past week: About 300 HackerOne employees have reportedly been impacted by the breach at Navia Benefit Solutions. Student management software provider Infinite Campus acknowledged a cyber incident without naming the threat actor. The acknowledgement comes as the ShinyHunters extortion group claimed a data breach at the firm. Healthcare management services company QualDerm Partners disclosed a data breach involving personally identifiable information (PII) and protected health information (PHI) of

at least 3.1 million individuals. Personal information of roughly 243,000 public education employees, most of them teachers, has reportedly been leaked in a cyberattack on a French Education Ministry HR system. NYC Health + Hospitals has disclosed a data breach where attackers accessed its network via a third-party vendor and remained undetected for over two months, exfiltrating sensitive data, including PII and PHI.

Physical and Geopolitical Intelligence Key Findings

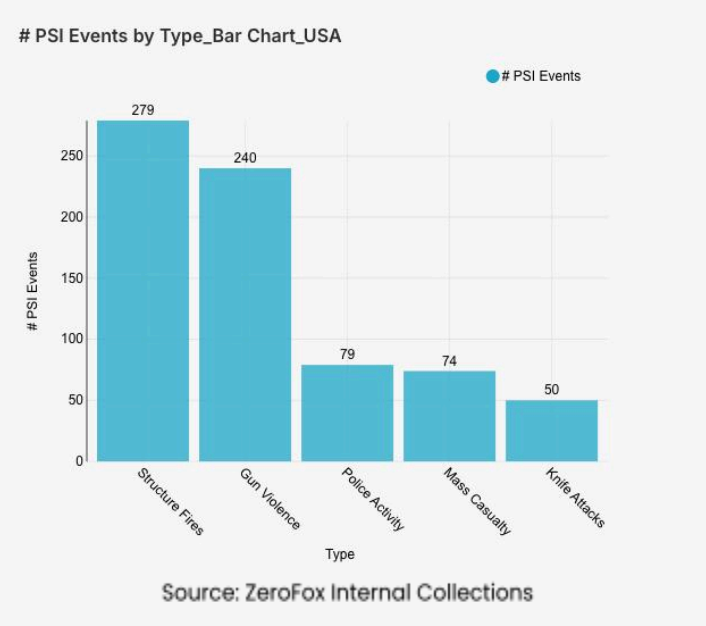


Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 16 percent decrease 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 81 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 41 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict decreased by 17 percent from the previous week, and alerts related to the war in Iran decreased by 25 percent. Events related to Russia's war in Ukraine increased by 32 percent. The top three most-alerted subtypes were explosions, which saw a 12 percent decrease from the previous week; gun violence, which decreased by 1 percent; and structure fires, which decreased by 13 percent. Unspecified violence, which includes attacks and raids of unknown nature, increased by 32 percent, and the top contributing country for this subtype was Mexico.

- **What this means:** While mass casualty events saw a decrease this week, the conflict involving Iran, Israel, and Iraq remains the primary driver. For instance, as of March 24, the Israel Defense Forces (IDF) reported an extensive wave of strikes targeting Iranian missile production sites in Isfahan province, while retaliatory cluster munition fire from Iran continues to target Israeli civilian centers. Conversely, Russia's war in Ukraine has seen a surge in activity as Moscow launched its Spring-Summer 2026 offensive; recent reports from March 23 indicate Russian forces conducted over 600 assaults in just four days, resulting in nearly 9,000 combined casualties. Meanwhile, the rise in "unspecified violence" is highlighted by Mexican gang violence; the February 2026 death of Cártel de Jalisco Nueva Generación (CJNG) leader El Mencho has triggered a sustained wave of retaliatory armed raids across several states. Overall, the current landscape of global security reflects a volatile shift, characterized by a slight dip in mass casualty frequency across the Middle East contrasted by a sharp escalation in Eastern Europe.

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 Illinois and Ohio, which together made up 21 percent of this week's nationwide total. Gun violence across the United States overall increased by 85 percent from the week prior. Police activity alerts increased by 36 percent, and the top contributing states were California and Texas. Structure fires increased by 8 percent, and the top two states for this subtype were New York and Florida. Notably, knife attacks increased by 61 percent.

- **What this means:** The United States has seen a significant surge in public safety incidents this week, with gun violence alerts increasing sharply; 16 mass shootings occurred within the last seven days, with 10 of them occurring on March 22. In Illinois, a mass shooting in Normal on March 22 injured six people; Virginia saw a mass shooting on March 23 at Virginia Beach that resulted in seven victims. Additionally, the surge in knife-related violence has been particularly stark in metropolitan areas this week. In Los Angeles, California, a confrontation at a bar on March 22 escalated into a mass stabbing that left six people injured. This week's data aligns with a well-documented phenomenon in criminology: as temperatures rise, so does violent crime. According to a 2024 Rutgers University study, sudden upward swings in temperature, like those experienced within the past week, can disrupt daily routines and lead to a significant uptick in aggravated crimes. With a large number of people gathering nationwide this weekend to express common grievances, the risks for opportunistic violence increases as well.

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%