ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

April 11, 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 April 9, 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 #33 - Military Strikes on Iran - April 9, 2026

On April 7, 2026, the United States and Iran agreed to a two-week ceasefire. However, just hours later, Iran closed the Strait of Hormuz (SoH) over Israeli targeting of Hezbollah, creating confusion as to whether the ceasefire remains in place and if both sides are even negotiating from the same framework. Markets have almost certainly determined that the ceasefire marks the end of the conflict. However, such early setbacks have reduced the probability the truce will hold, and there is only a roughly even chance the agreed-upon ceasefire holds for the two-week duration and that a longer-term agreement can be reached in that time. Israel's willingness to abide by the terms agreed upon by the United States and Iran is one of several uncertainties regarding the ceasefire's success. Other uncertainties include the continued buildup of U.S. forces in the region, how willing the United States and its Gulf allies are to tolerate an Iranian-controlled SoH, assurances made to Iran against future aggression, and historical concerns over Iran's nuclear and missile programs and support for regional proxies. One certainty is that the ceasefire's success very likely depends on the free flow of tanker traffic through the SoH. To know more about how the conflict has progressed, read previous SITREPs.

ZeroFox Intelligence Brief - Underground Economist: Volume 6, Issue 8

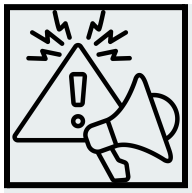
The Underground Economist is an intelligence-focused series illuminating Dark Web findings in digestible tidbits from our ZeroFox Dark Ops intelligence team.

ZEROFOX

Weekly Intelligence Brief

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings



BlueHammer Exploit Targets Windows SAM Database Through LPE Vulnerability

What we know:

- Exploit code for an unpatched Windows local privilege exploitation (LPE) flaw has been released. This flaw could enable attackers to gain SYSTEM/admin privileges via a time-of-check to time-of-use (TOCTOU) race condition and path confusion issue.
- Researchers noted the flaw is difficult to exploit but can grant local attackers access to the Security Account Manager (SAM) database containing password hashes.

Background:

- BlueHammer is the proof-of-concept exploit demonstrating this vulnerability, which was publicly disclosed by a researcher called "Chaotic Eclipse."
- Additionally, researchers tested this exploit and found that it was buggy, unreliable, and does not work on Windows Server systems.

Analyst note:

- This flaw, being a local privilege issue, enables low-privileged users to gain a foothold into affected devices.
- Therefore, threat actors are likely to try to gain access by stealing credentials from users through targeted social engineering tactics, such as phishing, deepfakes, and business email compromise.
- Users are advised to be aware of suspicious messages and rotate their credentials or set new passwords so that threat actors do not use credential stuffing attacks to gain privileges.

Russian APT Fancy Bear Exploiting Routers in DNS Hijacking Campaign

What we know:

- Russian military-linked threat group APT28 (Fancy Bear) has been carrying out a Domain Name System (DNS) hijacking campaign by exploiting MicroTik and TP-Link routers (mainly

small office/home office [SOHO] routers) to steal credentials and other sensitive information.
- The Federal Bureau of Investigation (FBI) said that it has cut off access to the compromised routers in the United States.

Background:
- The campaign has been used to specifically target military, government, and critical infrastructure entities by filtering down a wide pool of impacted users worldwide.
- Recently, the United States banned the foreign-made routers over national security concerns.

Analyst note:
- Employees and contractors in government, military-industrial, and critical infrastructure sectors are very likely to be high-value initial targets.
- Such compromised access is likely to enable attackers to establish persistent presence in larger networks, monitor communications, access sensitive data, and carry out phishing using compromised legitimate email domains.

Token Theft Breach Hits Snowflake Customers via Suspected Third-Party Compromise

What we know:
- Over a dozen companies were hit by data theft attacks after a third-party software as-a-service (SaaS) company was breached, and authentication tokens were stolen.
- The attacks primarily targeted Snowflake customers, though the platform itself was not compromised.

Background:
- The incident is linked to a suspected breach at an artificial intelligence (AI)-based anomaly detection company called Anodot, enabling attackers to access customer accounts via stolen tokens.
- ShinyHunters has reportedly claimed responsibility and is now extorting affected companies with threats of data leaks.

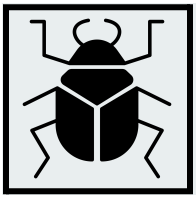
Analyst note:
- ShinyHunters is likely to leverage stolen data to extort its victims, failing which, compromised data, such as authentication tokens, will be sold in dark web marketplaces.
- Stolen authentication tokens are likely to enable threat actors to further compromise victims by bypassing their password and multi-factor authentication (MFA) requirements.

- This is likely to enable them to gain unauthorized access to SaaS applications and access downstream communications.

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 new vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue on April 6 and April 8, 2026. Additionally, on April 7, 2026, CISA released one Industrial Control System (ICS) advisory, which features two Mitsubishi vulnerabilities (CVE-2025-14815 and CVE-2025-14816). CVE-2026-2699 and CVE-2026-2701 are two critical vulnerabilities in Progress Software's ShareFile service that can reportedly be chained together in an exploit to unauthorized make configuration changes and achieve remote code execution (RCE). CVE-2026-34197 is an improper input validation and "code injection" vulnerability in Apache ActiveMQ Broker and Apache ActiveMQ. The flaw reportedly existed for 13 years and can be exploited in a chain attack using an older bug to bypass authentication. Hackers are actively exploiting CVE-2025-59528, a critical flaw in Flowise that enables arbitrary JavaScript injection, leading to RCE and file system access. CVE-2026-0740 is a flaw in the Ninja Forms File Upload add-on for WordPress that enables unauthenticated attackers to upload malicious files. Android's latest security update patches two flaws, a critical denial-of-service (DoS) bug (CVE-2026-0049) in the Framework component that can be triggered locally without privileges or user interaction and fixes a high-severity StrongBox vulnerability (CVE-2025-48651) that can potentially impact secure key storage across multiple vendors, though its exact impact remains undisclosed. A vulnerability dubbed "GrafanaGhost" in Grafana AI components could enable attackers to bypass safeguards and exfiltrate enterprise data via prompt injection and malicious image rendering. OpenSSL has patched seven vulnerabilities, including CVE-2026-31790, wherein improper verification in RSASVE key exchange can leak sensitive data from uninitialized memory. Other low-severity flaws mainly cause DoS, while rare scenarios could enable code execution, with fixes available across affected OpenSSL 3.x versions.



HIGH

CVE-2026-34040

What happened: This high-severity vulnerability in Moby, created by Docker Engine, can enable threat actors to bypass authorization plugins using specially crafted Application Programming Interface (API) requests.

- **What this means:** This flaw could enable creation of privileged containers with host access, risking full system compromise and credential theft. If threat actors bypass authorization plugins, they are likely to escalate from limited API access to full host compromise, which could expose a user's assets, including credentials, and Kubernetes configs.
    - **Affected products**: Docker's Moby versions prior to 29.3.1

CRITICAL

CVE-2026-35616

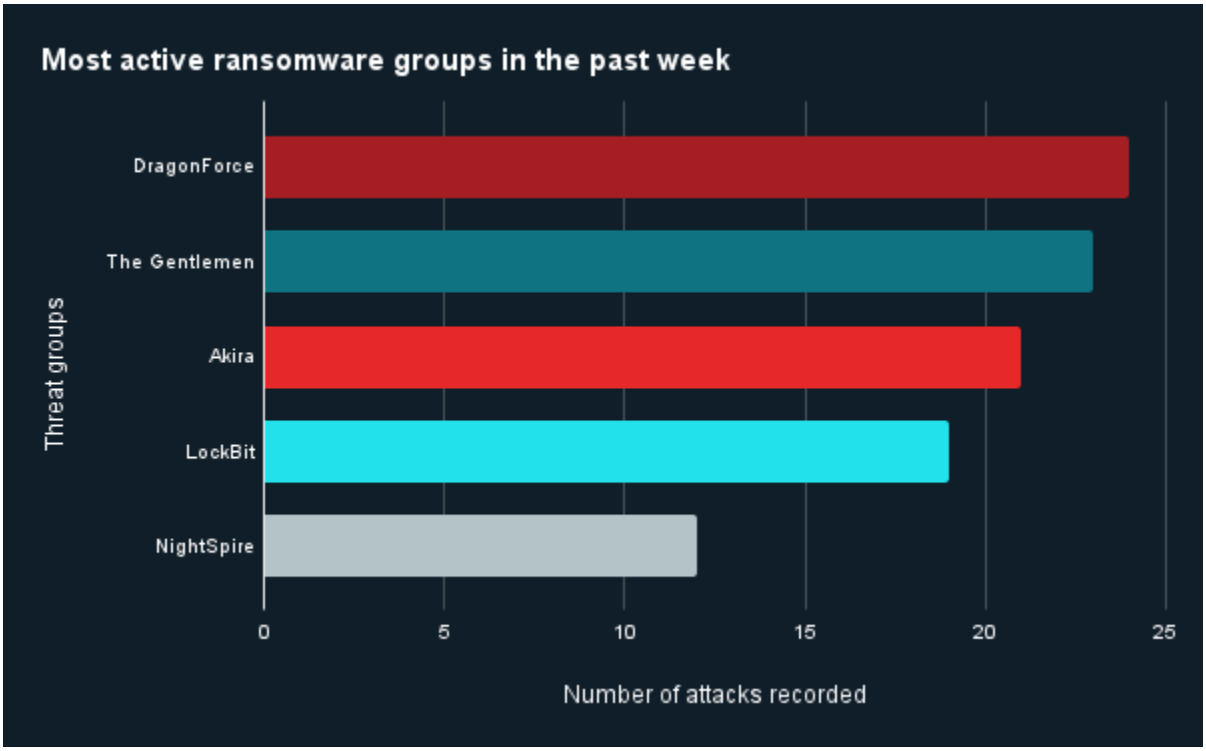
What happened: This is an Improper Access Control vulnerability in FortiClient EMS that may enable an unauthenticated attacker to execute unauthorized code or commands via crafted requests. Fortinet has observed this to be exploited in the wild. There are reportedly over 2,000 exposed FortiClient EMS instances online, with the majority located in the United States and Germany.

- **What this means:** Successful exploitation of the vulnerability is likely to lead to malware deployment and/or further intrusion into a corporate network.
    - **Affected products:** FortiClientEMS versions 7.4.5 through 7.4.6

Ransomware and Breach Intelligence

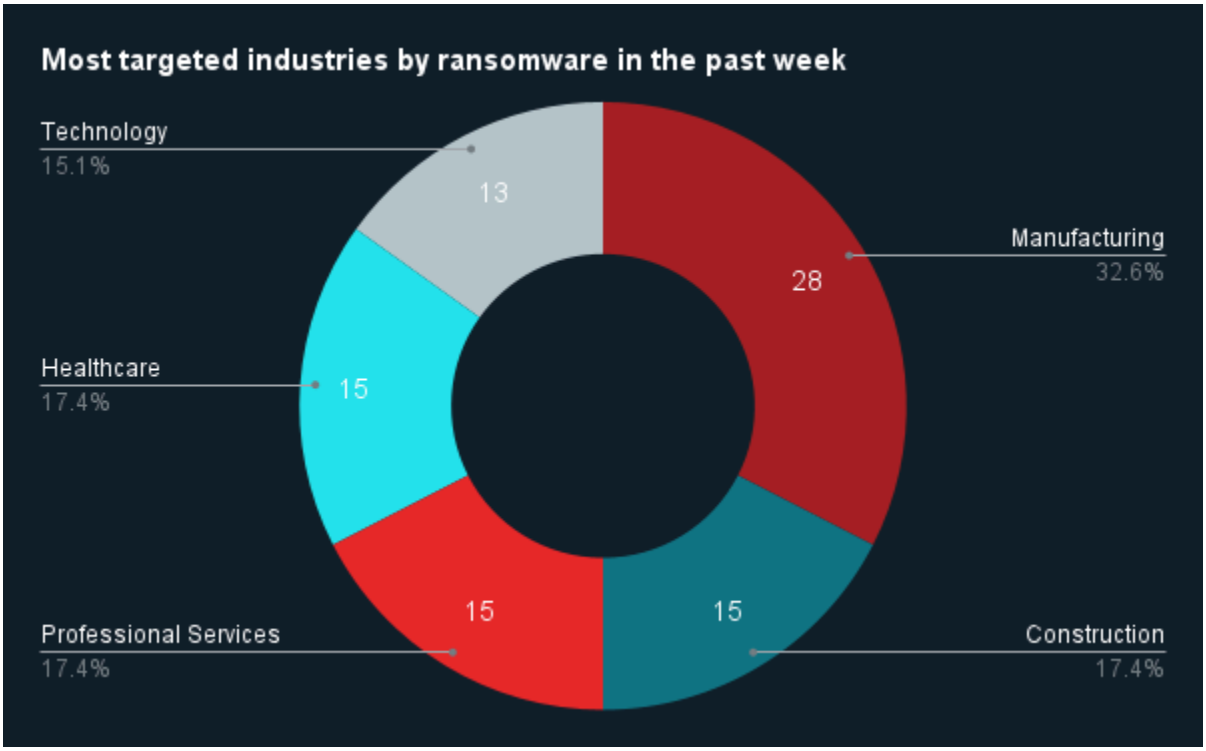
Ransomware and Breach Intelligence Key Findings

Ransomware Group, Industry, and Region Trends



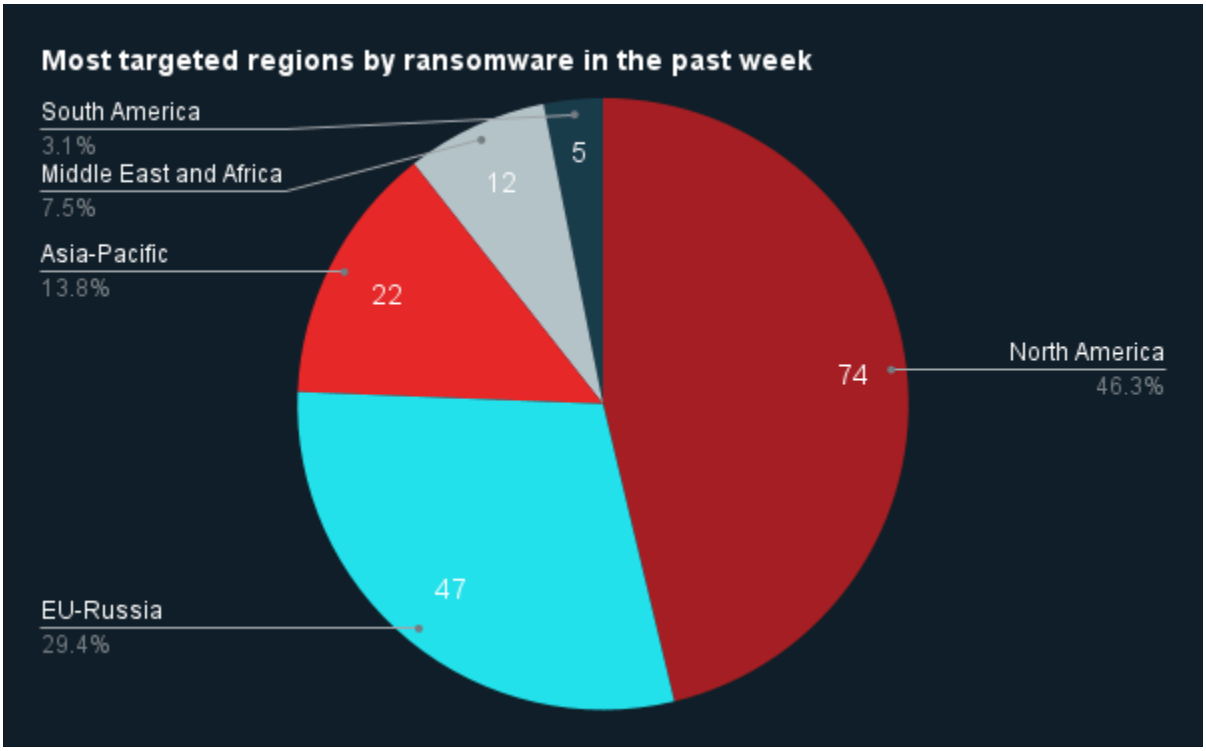
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, DragonForce, The Gentlemen, Akira, LockBit and NightSpire were the most active ransomware groups. ZeroFox observed nearly 163 leaked ransomware victims, most of whom were located in North America. The Dragoforce 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, professional services, and healthcare.



Source: ZeroFox Internal Collections

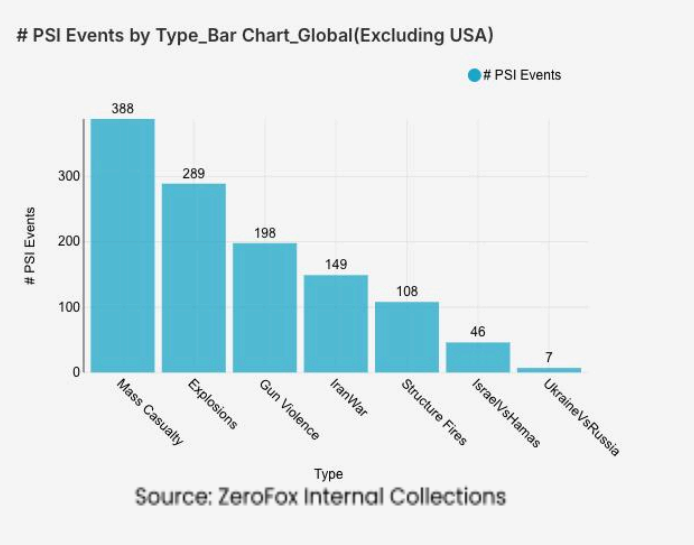
Regional ransomware trends: Over the past seven days, ZeroFox observed that North America was the region most targeted by ransomware attacks, followed by Europe and Russia. There were at least 74 ransomware attacks observed in North America, while Europe and Russia accounted for 47, Asia-Pacific (APAC) for 22, Middle East and Africa for 12, and South America for five.

Significant Data Breaches Reported in the Past Week

Targeted Entity	LA City Attorney's Office	ProxyCare LLC	The National Supercomputer Center (NSCC) in Tianjin
Compromised Entities/Victims	337,000 files totaling 7.7 TB affecting the Los Angeles Police Department, witnesses, and individuals named in court filings	Over 150 ProxyCare's patients; total affected individuals yet to be determined	Over 10 PB of sensitive information affecting more than 6000 clients, including defense agencies
Compromised Data Fields	Settled civil litigation files, personnel files, and Internal Affairs investigations, witness names, and unredacted criminal complaints.	Personally identifiable information (PII) of patients, including their Social Security numbers and driver's license numbers	Defense documents marked as "secret" in Chinese, visual simulations and renderings of defense equipment, including bombs and other research data
Suspected Threat Actor	WorldLeaks ransomware group	Unknown	Telegram user FlamingChina
Country/Region	United States	United States	China
Industry	Government	Healthcare	Critical Infrastructure
Possible Repercussions	Physical security risk to exposed individuals (such as witnesses and complainants) and operational disruptions	Identity theft risk, financial and insurance fraud, social engineering, and phishing attacks	National security compromise, strategic upper hand for adversarial nations, and intellectual property theft

Three major breaches observed in the past week

Physical and Geopolitical Intelligence Key Findings

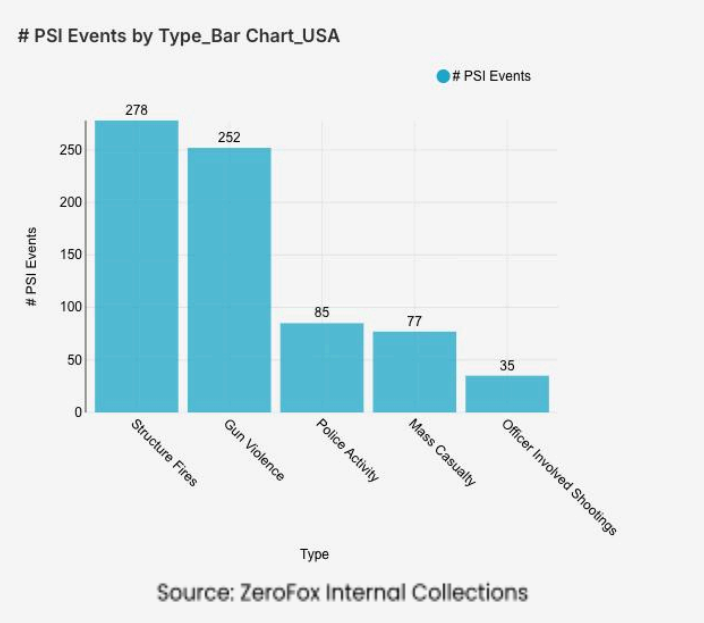


Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 4 percent decrease in mass casualty events this week from the previous week, with the top contributing countries or territories being Iran, Israel, and Lebanon, in that order. Approximately 74 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 38 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict decreased by 36 percent from the previous week, whereas alerts related to the war in Iran increased by 12 percent. Events related to Russia's war in Ukraine decreased by 30 percent. The top three most-alerted subtypes were explosions, which saw a 10 percent decrease from the previous week; gun violence, which decreased by 10 percent; and structure fires, which decreased by 15 percent.

- **What this means:** While overall mass casualty events saw a slight decrease this past week, the Middle East remains the primary driver of these statistics. Iran, Israel, and Lebanon emerged as the top contributors, largely due to the fracturing of a fragile U.S.-Iran ceasefire and Israel's subsequent escalation against Hezbollah. For instance, on April 8, Israel launched "Operation Eternal Darkness," a series of over 100 airstrikes across Lebanon that killed several hundreds of people and injured over a thousand, illustrating why explosions accounted for the majority of recent mass casualty events. Although alerts related to the Israel-Hamas conflict dropped somewhat, the war in Iran saw a rise in alerts as paramilitary forces reportedly placed sea mines in the Strait of Hormuz following the collapse of diplomatic trust. Conversely, the decrease in alerts regarding Russia's war in Ukraine reflects a momentary shift toward localized drone strikes on energy infrastructure rather than large-scale troop movements, as evidenced by recent drone attacks on civilian buses near Nikopol, Ukraine, on April 7. Ultimately, the data from this week confirms that regional volatility remains the primary driver of international mass casualty trends.

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 Georgia and Ohio, which together made up 17 percent of this week's nationwide total. Gun violence across the United States overall increased by 10 percent from the week prior. Police activity alerts increased by 29 percent, and the top contributing states were California and Florida. Structure fires decreased by 14 percent, and the top two states for this subtype were New York and California. Notably, officer involved shootings increased by 84 percent, with California as the top contributing state.

- **What this means:** The past week across the United States has been characterized by a significant surge in high-intensity incidents, specifically regarding law enforcement engagements and violent crime. The significant increase in officer-involved shootings specifically is exemplified by a high-profile incident in Patterson, California, on April 7, where ICE agents were involved in a shooting during an attempted traffic stop of a suspect. Nationally, gun violence remains a critical concern, with four mass shootings occurring within the last week. Two of those incidents took place in Georgia, with the one in Atlanta on April 5 resulting in four teenage victims. Furthermore, the week's data highlights how mass gatherings for holidays and festivals can inadvertently create environments prone to mass casualty events. On April 4, a vehicle plowed into a Lao New Year parade in New Iberia, Louisiana, injuring approximately 15 people. Overall, this data reveals a challenging week for domestic public safety, where seasonal gatherings were frequently overshadowed by a significant increase in violent incidents and generalized law enforcement activity.

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%