# ZEROFOX®

## *Weekly Intelligence Brief*

**Classification: TLP:GREEN**

**April 4, 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 2, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

# Weekly Intelligence Brief



© 2026 ZeroFox, Inc. All rights reserved.

# This Week's ZeroFox Intelligence Reports

## ZeroFox Intelligence Flash Report - SITREP #31 - Military Strikes on Iran - April 2, 2026

U.S. President Donald Trump has continued vacillating between threatening to escalate the Iran conflict and winding it down. Iran made its most significant acknowledgement to date that it is open to talks, without conceding on previous demands. There is now a roughly even chance the U.S. military will scale back its operations after meeting only some of its stated goals, such as removing layers of Iran's leadership and debilitating its weapons program. This would very likely leave Iran in control of the Strait of Hormuz (SoH), which Trump has suggested is possible. Although additional reinforcements for ground operations are anticipated, the U.S. military likely possesses enough existing capabilities to launch such operations now. There is a roughly even chance the United States winds down the conflict after pursuing military goals such as seizing Iran's enriched uranium, conducting operations against Iranian nuclear facilities and critical infrastructure, or further reducing Iran's ability to control the SoH. On March 31, 2026, the Islamic Revolutionary Guard Corps (IRGC) issued a warning to 18 companies (including 16 U.S. and two Dubai-based companies), threatening them with attack for their alleged support of U.S. and Israeli war efforts. The IRGC suggested that employees stay away from their places of work in order to "preserve their own lives." To know more about how the conflict has progressed, read previous SITREPs.

## Monthly Geopolitical Assessment April 2026

Iran is expected to leverage its influence over energy markets to ensure that any ceasefire-driven stabilization does not leave the country vulnerable to future targeting. Therefore, the United States is likely to pursue a diplomatic de-escalation before a multinational effort to contest Iran's control over the SoH. Israel will likely cease its strikes in concert with the United States if U.S. President Donald Trump declares a ceasefire, but operations in Lebanon will very likely continue regardless. It is likely that concessions from Cuba will begin in the coming months as the government attempts to reduce U.S. pressure. U.S. military action similar to that seen in Venezuela does not appear likely in Cuba, especially while the United States is focused on Iran. The delay of a high-profile summit between President Trump and Chinese President Xi Jinping is unlikely to change the outcome, and U.S-China tensions are likely to improve throughout 2026. The conflict in Iran is providing a significant economic benefit to Russia, marked by a revenue windfall from spiking global oil prices. However, this economic success is offset by Russia's poor performance on the battlefield, where Ukrainian forces have gained territory and nearly liberated Dnipropetrovsk Oblast. Additionally, key European elections in April, led by those in Hungary, are likely to expose Russia's lack of political support in Europe.

© 2026 ZeroFox, Inc. All rights reserved.

ZEROFOX®
*Weekly Intelligence Brief*

# Cyber and Dark Web Intelligence

© 2026 ZeroFox, Inc. All rights reserved.

# Cyber and Dark Web Intelligence Key Findings

## North Korea-Linked Threat Actors Target Axios

**What we know:**

- The Axios JavaScript NPM package was recently compromised by North Korean threat actors UNC1069.
- The actors hijacked Axios's npm account to publish trojanized versions of Axios (1.14.1 and 0.30.4), embedding a malicious dependency ("plain-crypto-js") that delivers a cross-platform backdoor across Windows, macOS, and Linux.

**Background:**

- Axios is an open source software development tool with 400 million downloads per month on npm.
- During the attack, the dependency executed a hidden postinstall script, deploying the SILKBELL dropper and WAVESHAPER.V2 backdoor across Windows, macOS, and Linux systems.
- The malware was observed to establish persistence, contact command-and-control (C2) infrastructure, execute commands, and then remove traces, indicating a highly planned and scalable attack targeting developers.
- The indicators of compromise (IOCs) are available here.

**Analyst note:**

- The breach of Axios on npm exposes millions of downstream applications, enabling large-scale compromise of developer environments and production systems.
- Compromised dependencies can propagate malware into Continuous Integration/Continuous Delivery (CI/CD) pipelines and enterprise software, increasing the risk of widespread, cascading breaches across organizations.

## Meta Accuses Italian Spyware Maker of Pushing Fake WhatsApp Versions

**What we know:**

© 2026 ZeroFox, Inc. All rights reserved.

- Meta has accused Italian spyware maker SIO of tricking some 200 iPhone users in Italy into downloading a fake version of WhatsApp that contained spyware. Meta did not specify who the victims were but said it has alerted them.

**Background:**

- SIO was previously found to be behind a series of spyware Android apps. The firm's website describes it as a provider of cyber intelligence solutions partnering with governments.
- In January 2025, Meta alerted 90 users in Italy, including journalists and pro-immigration activists, that they were targeted by spyware from U.S.-Israeli firm Paragon Solutions.

**Analyst note:**

- Ongoing spyware scandals suggest Italian government bodies may still be targeting critics with surveillance despite cutting ties with Paragon a year earlier.
- Instances of governments deploying spyware across Europe stand in stark contrast to the European Union's stringent data protection and privacy framework under the General Data Protection Regulation (GDPR).

## Canada Imprisons Individual Linked to Online Extremist Group Terrorgram Collective

**What we know:**

- The Canadian Public Prosecution Service sentenced an individual to 20 years in prison for producing and disseminating violent extremist propaganda as part of the online network known as the "Terrorgram Collective" that inspired multiple terrorist attacks.

**Background:**

- Europol has also been involved in the investigation since 2022, mapping the Terrorgram network and identifying individuals linked to it across Europe and beyond.

**Analyst note:**

- In the short term, international law enforcement will likely disrupt the group's activity and recruitment. However, it is unlikely to eliminate online extremism in the long term, as deeper factors such as governance, education, and economic conditions continue to sustain it.

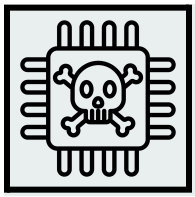
© 2026 ZeroFox, Inc. All rights reserved.

# Exploit and Vulnerability Intelligence

© 2026 ZeroFox, Inc. All rights reserved.

# 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 three new vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue on March 27, March 30, and April 2, 2026. CISA also added two Industrial Control Systems (ICS) advisories on March 31. Google has released security patches for its Chrome web browser, addressing 21 vulnerabilities. An already-patched integrity verification bypass vulnerability in TrueConf client video conferencing software , tracked as CVE-20 26-3502, has reportedly been exploited as a zero-day in a campaign targeting government entities in Southeast Asia. Apple has released iOS 18.7.7 and iPadOS 18.7.7 updates to protect older devices against the DarkSword exploit, a web-based attack capable of stealing sensitive data such as messages, location, and cryptocurrency. The move follows the public leak of the DarkSword toolkit, which has already been used in targeted attacks and can now be widely exploited against users running unpatched iOS 18 versions. A critical remote code execution (RCE) vulnerability in PTC Windchill and FlexPLM, tracked as CVE-2026-4681, has triggered an unprecedented response in Germany, where police physically visited companies at night to warn of imminent risk. A vulnerability in Trivy security scanner, tracked as CVE-2026-33634, has been exploited, allegedly by TeamPCP hackers, in a supply chain attack, enabling credential theft.



**HIGH**

## CVE-2026-5281

**What happened:** This is an actively exploited zero-day tracked CVE-2026-5281. It is a use-after-free flaw that enables RCE.

- **What this means:** Successful exploitation is likely to be chained with other flaws to escalate privileges, establish persistence, and exfiltrate data.
  - **Affected products**: Google Chrome prior to 146.0.7680.178

© 2026 ZeroFox, Inc. All rights reserved.

**CRITICAL**

## CVE-2025-53521

**What happened:** F5 Networks has reclassified this vulnerability in its BIG-IP Access Policy Manager (APM) from a denial-of-service flaw to an RCE issue after confirming active exploitation. Attackers are exploiting the flaw to deploy webshells on unpatched systems.

- **What this means:** Sustained exploitation of this vulnerability is likely to enable threat actors to access networks, cloud services, applications, and Application Program Interfaces (APIs) controlled by BIG-IP APM.
  - **Affected products:** The affected products are listed in this advisory.

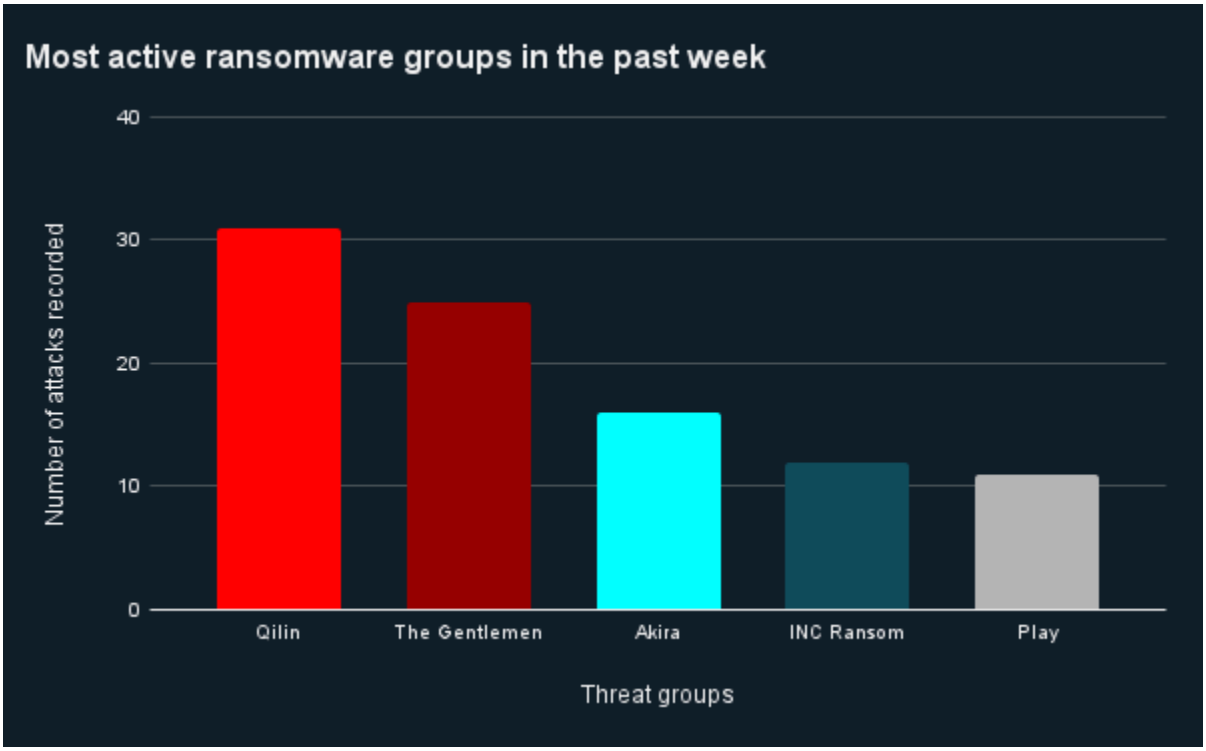
© 2026 ZeroFox, Inc. All rights reserved.

# Ransomware and Breach Intelligence

© 2026 ZeroFox, Inc. All rights reserved.

# Ransomware and Breach Intelligence Key Findings

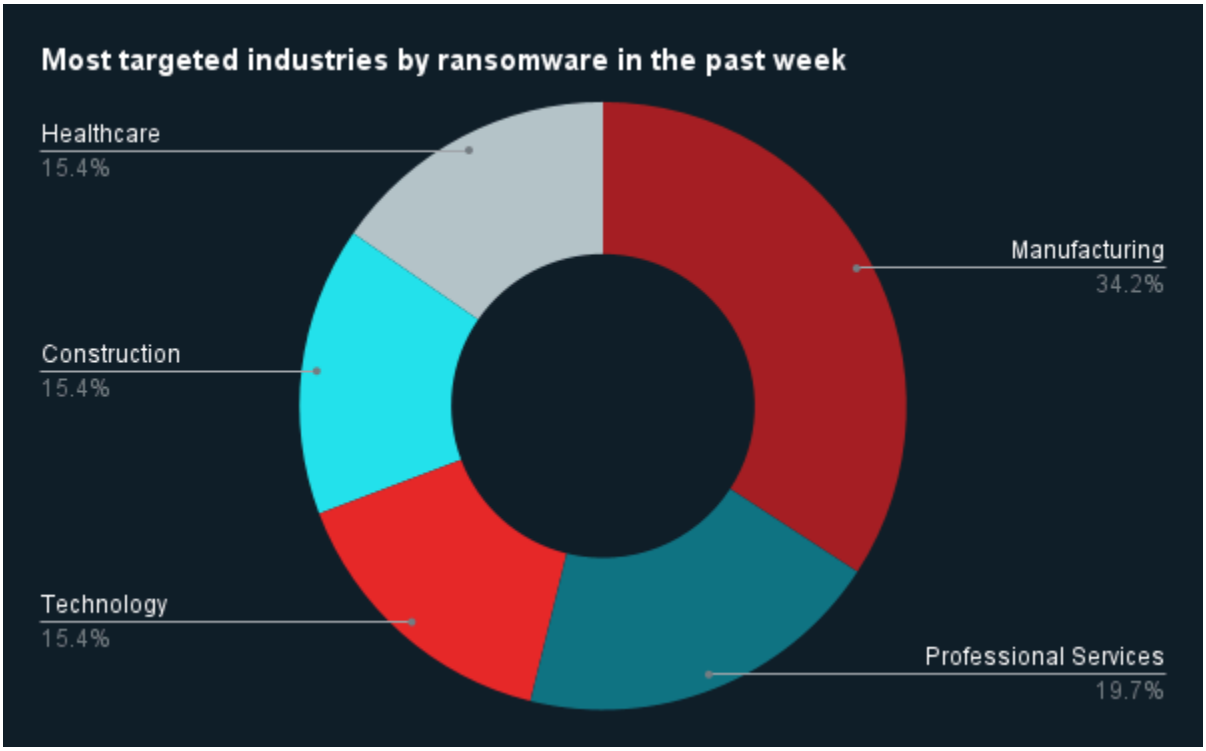
## Ransomware Group, Industry, and Region Trends




Source: ZeroFox Internal Collections

**Last week in ransomware:** In the past week, Qilin, The Gentlemen, Akira, INC Ransom, and Play were the most active ransomware groups. ZeroFox observed close to 177 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.

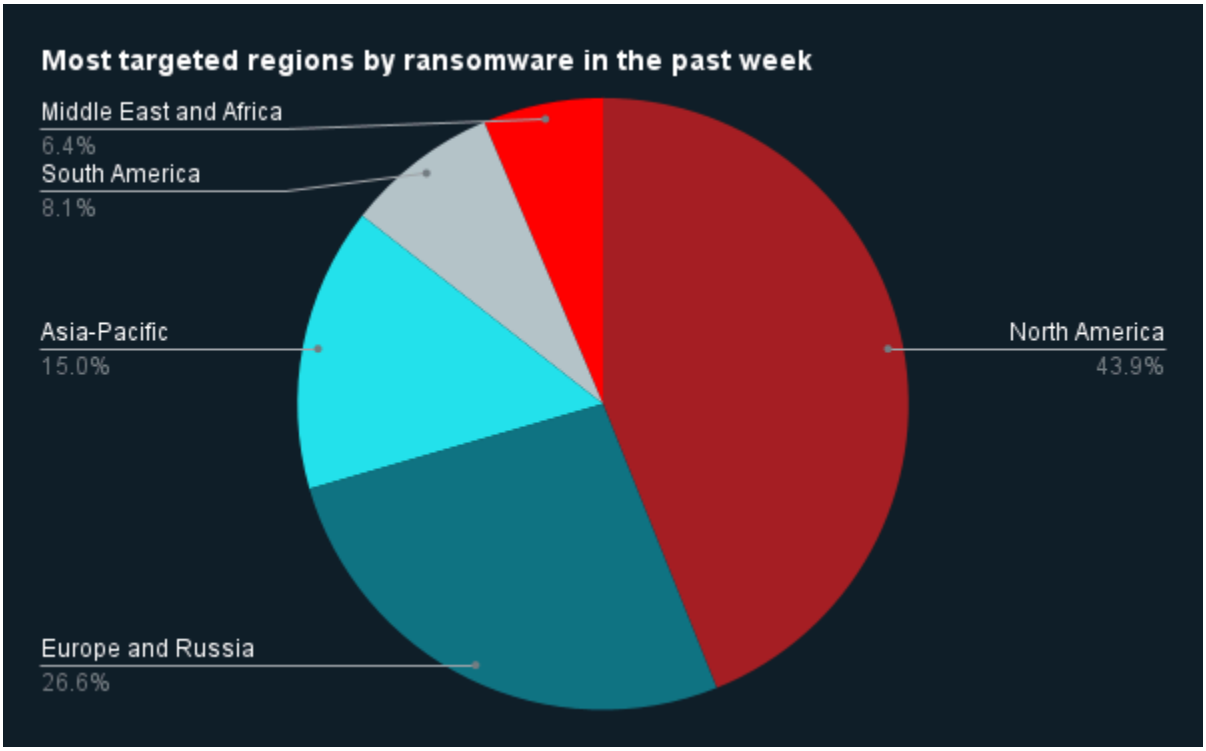
© 2026 ZeroFox, Inc. All rights reserved.




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 professional services.

© 2026 ZeroFox, Inc. All rights reserved.




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 76 ransomware attacks observed in North America, while Europe and Russia accounted for 46, Asia-Pacific (APAC) for 26, South America for 14, and Middle East and Africa for 11.

© 2026 ZeroFox, Inc. All rights reserved.

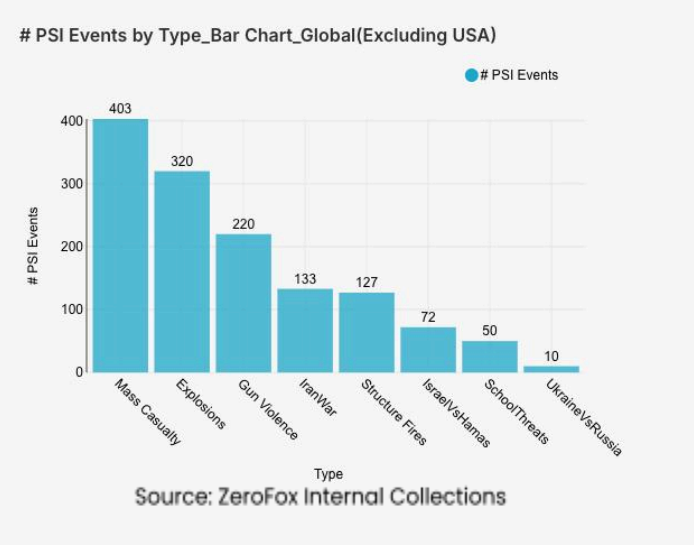
## Significant Data Breaches Reported in the Past Week

| Targeted Entity | CareCloud, Inc. | Dutch Ministry of Finance | P3 Global Intel and Crime Stoppers |
|---|---|---|---|
| Compromised Entities/Victims | CareCloud customers, including hospitals and medical practices, serving over 45,000 providers | At least 1,600 Dutch public institutions, including ministries, government agencies, educational organizations, social funds, and local governments | U.S. and Canadian law enforcement entities |
| Compromised Data Fields | Personally identifiable information (PII) and protected health information (PHI) | N/A | Tipline data such as anonymous crime tips, suspect/tipster full names, addresses, Social Security numbers (SSNs), phone numbers, and email addresses |
| Suspected Threat Actor | Unknown | N/A | Breached[.]st user iym |
| Country/Region | United States | The Netherlands | North America |
| Industry | Healthcare | Government | Security |
| Possible Repercussions | Extortion of CareCloud customers, as well as insurance fraud, blackmail, phishing, and social engineering attacks targeting exposed individuals. | Operational disruption, including fund holders unable to view the balance of their treasury accounts, as well as theft of PII and/or financial information | If the data is legitimate, exposed individuals and entities are likely to face extortion and risk to their physical safety. |

**Three major breaches observed in the past week**

© 2026 ZeroFox, Inc. All rights reserved.

# Physical and Geopolitical Intelligence Key Findings

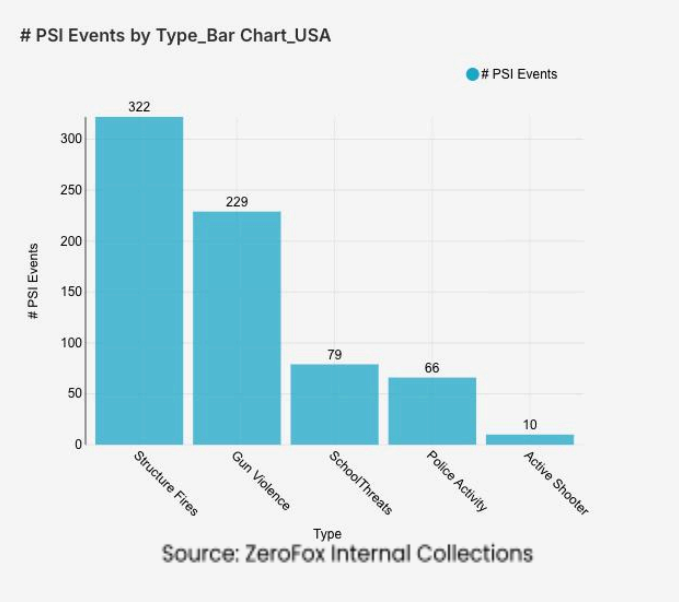



## Physical Security Intelligence: Global

**What happened:** Excluding the United States, there was a 2 percent increase in mass casualty events this week from the previous week, with the top contributing countries or territories being Iran, Iraq, and Israel, in that order. Approximately 79 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 37 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict increased by 140 percent from the previous week, and alerts related to the war in Iran decreased by 15 percent. Events related to Russia's war in Ukraine decreased by 9 percent. The top three most-alerted subtypes were explosions, which saw a 1 percent decrease from the previous week; gun violence, which increased by 39 percent; and structure fires, which increased by 19 percent. Notably, threats against educational institutions increased by 39 percent.

- **What this means:** This week saw sustained high numbers of mass casualty incidents, heavily driven by the U.S.-Israel-Iran war. Now in its 34th day, Iran, Iraq, and Israel have become the primary theaters for mass casualty alerts. For instance, on April 1, Israeli airstrikes in Lebanon killed 27 people in a 24-hour window; on the same day, around 10 ballistic missiles were fired at central Israel, in the largest Iranian salvo since the early days of the war. Ceasefire violations continue to contribute to the increase of Israel-Hamas related alerts as well. In Iraq, the U.S. Embassy in Baghdad issued urgent warnings on April 2 regarding imminent attacks by pro-Iran militias, following intense strikes in the Kurdistan Region that have utilized hundreds of drones and missiles. The data also highlights a rise in threats against educational institutions. This global trend is visible in Nigeria, where on March 30, the U.S. Embassy issued an urgent security advisory warning of potential terrorist threats targeting American-affiliated schools and public facilities in Abuja and Lagos. Overall, this week's global instability is characterized by a mix of traditional warfare, localized terrorism, and targeted institutional threats.

© 2026 ZeroFox, Inc. All rights reserved.




## 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 Texas and Pennsylvania, which together made up 21 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 decreased by 16 percent, and the top contributing states were Texas and Florida. Structure fires increased by 15 percent, and the top two states for this subtype were New York and California. Notably, active shooter alerts nationally increased by 400 percent.

- **What this means:** The past week in the United States has seen a volatile security landscape, primarily marked by a sharp increase in active shooter alerts. This surge is underscored by high-profile tragedies in the top-contributing states of Texas and Pennsylvania; for example, a mass shooting in Dickinson, Texas, on March 29 left seven people injured at a lounge, while a shooting in which a suspect shot into a crowd from a vehicle in Philadelphia, Pennsylvania, on March 30 resulted in two deaths and three injuries. Overall, there were seven mass shootings in the United States within the last seven days. Simultaneously, structure fire numbers rose as well, largely driven by incidents in New York and California, such as the large five-alarm blaze in the Bronx, New York City, New York, on March 26 that required an extensive fire department response. Furthermore, reports of coordinated public gatherings across several metropolitan areas contributed to the police activity subtype, as authorities across the country worked to manage groups that affected local traffic and business operations. These trends suggest that, while overall crime volume may fluctuate from week to week, the nature of specific threats such as active shooters and structure fires remain a concern for domestic safety and law enforcement readiness.

© 2026 ZeroFox, Inc. All rights reserved.

# 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. |

© 2026 ZeroFox, Inc. All rights reserved.

# 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% |

© 2026 ZeroFox, Inc. All rights reserved.