



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

April 5, 2025

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 April 3, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Weekly Intelligence Brief |

 This Week's ZeroFox Intelligence Reports	2
ZeroFox Intelligence April 2025 Geopolitical Assessment	2
ZeroFox Intelligence Brief – Underground Economist: Volume 5, Issue 6	2
ZeroFox Intelligence Flash Report: Turkey Protests Threaten Economic and Political Stability	2
ZeroFox Intelligence Brief Report – Remote IT Workers Fraud: Threats and Prevention	2
 Cyber and Dark Web Intelligence Key Findings	5
Phishing Platform “Lucid” Targets 169 Entities in Global Campaign	5
FTC Sends Warning Letters to EIN Service Providers over Potential Violations of Impersonation Rules	6
New Android Malware Crocodilus Targeting Spain and Turkey for Financial Theft	6
 Exploit and Vulnerability Intelligence Key Findings	9
CVE-2025-31579	9
CVE-2025-26683	10
 Ransomware and Breach Intelligence Key Findings	12
Ransomware Alert: Actors' Activity, Industry Impact, and Key Updates	12
Major Data Breaches Across the Globe in the Past Week	15
 Physical and Geopolitical Intelligence Key Findings	18
Physical Security Intelligence: Global	18
Physical Security Intelligence: The United States	19
 Appendix A: Traffic Light Protocol for Information Dissemination	20
 Appendix B: ZeroFox Intelligence Probability Scale	21

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence April 2025 Geopolitical Assessment

The sentiments of traditional U.S. allies towards the United States are shifting, and Germany's announcement on defense spending as well as developments in Canada and Australia's upcoming elections are the latest signs. The U.S. political withdrawal from Europe likely influenced the timing of the opposition crackdown in Turkey, where President Recep Erdogan will very likely pursue another term. A full Ukraine-Russia peace deal remains distant, but a temporary ceasefire in the Black Sea and on energy targets—two areas where Russia is most vulnerable to Ukrainian attacks—is likely. This is a reflection of the U.S. priority to end the war quickly on Russian terms. Crime remains the primary political issue in Latin America while protests against corruption threaten several eastern European states. Recent and upcoming U.S. tariffs are an illustration of how the Trump administration wants to make changes to trade flows and use trade to achieve other foreign policy goals.

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

The Underground Economist is an intelligence-focused series illuminating dark web findings from our ZeroFox Dark Ops intelligence team.

ZeroFox Intelligence Flash Report: Turkey Protests Threaten Economic and Political Stability

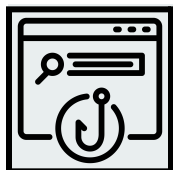
Turkey is unlikely to face significant external pressure following the arrest of a popular opposition leader. The country has made itself indispensable to international partners due to its leadership roles in Ukraine and Syria and in containing immigration. President Erdogan is unlikely to be displaced by protests. However, the protests are among the most severe in Turkey's recent history, and the government's response indicates concern that they could continue escalating. Pro-democracy groups, including cyber hackers, have voiced support for protesters and will likely target government ministries the longer protests persist with website defacements and distributed denial-of-service (DDoS) attacks.

ZeroFox Intelligence Brief Report – Remote IT Workers Fraud: Threats and Prevention

Remote IT workers fraud is an emerging threat, with some nation-state actors—such as North Korea—leveraging deepfake-enhanced deception to infiltrate organizations. Traditional hiring practices may be insufficient to detect synthetic applicants. Multi-layered identity verification, open source techniques, and biometric checks can help strengthen pre-employment screening. Artificial intelligence (AI)-generated profiles and deepfake-assisted interviews have enabled more convincing fraud, highlighting the value of live movement-based identity testing and behavioral screening. Post-hire insider threat monitoring may reduce risk, using user activity tracking, biometric analytics, and geolocation validation to identify anomalous behavior. Zero Trust security frameworks support risk mitigation by enforcing role-based access control (RBAC) and integrating Data Loss Prevention (DLP) measures. Security awareness and insider threat training remain critical components of a resilient workforce, helping employees recognize and report fraud indicators.

| Cyber and Dark Web Intelligence |

| Cyber and Dark Web Intelligence Key Findings



Phishing Platform “Lucid” Targets 169 Entities in Global Campaign

What we know:

- Lucid, a phishing-as-a-service (PhaaS) platform, has been used in attacks across 169 entities and 88 countries.
- Lucid automates these phishing attacks by deploying customizable phishing websites, primarily through SMS-based lures.
- By using Apple iMessage and Android’s Rich Communication Services (RCS), the Lucid platform effectively bypasses traditional SMS spam filters.

Background:

- China-linked threat group XinXin reportedly runs this platform, along with another PhaaS platform called Darcula v3.
- Lucid offers over 1,000 phishing domains, automated phishing sites, and mass spamming tools; subscriptions are sold via Telegram, allowing actors to target victims globally with fraudulent tax, shipping, and toll payment alerts.
- Lucid operators use large-scale iOS and Android device farms, stolen Apple IDs, and carrier exploits to distribute phishing messages, stealing financial and personal data for fraud and resale.

What is next:

- Beyond bypassing spam filters using iMessage and RCS makes the operation more cost-effective, since sending large volumes of traditional SMS messages can be expensive. This could enable threat actors to scale their phishing campaigns efficiently while minimizing operational costs.
- As a PhaaS platform, Lucid likely enables threat actors of all skill levels to launch campaigns with minimal effort. As Lucid becomes more popular, less experienced attackers can leverage its automated tools and pre-built phishing kits, while more advanced actors can integrate Lucid with other tools and platforms to execute targeted attacks, such as spear phishing.



FTC Sends Warning Letters to EIN Service Providers over Potential Violations of Impersonation Rules

What we know:

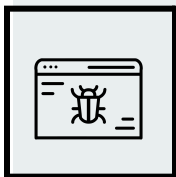
- Federal Trade Commission (FTC) staff have sent letters to website operators offering Employer Identification Number (EIN) filing and delivery services, warning that their practices may violate the FTC Act and the Impersonation Rule.

Background:

- Violations of the FTC Act and the Impersonation Rule are likely to lead to legal action, civil penalties of up to USD 53,088 per violation, and mandatory consumer refunds. Website operators are also advised to review their marketing practices, including online ads and promotions, to ensure compliance with the law.

Analyst note:

- The letters note that some services charge consumers up to USD 300 per EIN, even though EINs can be obtained for free directly from the Internal Revenue Service (IRS) website. Consumers are advised to be cautious of scammers impersonating legitimate websites and fraudulent online ads.



New Android Malware Crocodilus Targeting Spain and Turkey for Financial Theft

What we know:

- A novel Android banking malware, Crocodilus, has been discovered targeting users in Spain and Turkey. The malware is designed to steal credentials, including crypto wallet keys, which are used for theft of victims' assets.

Background:

- Crocodilus disguises itself as Google Chrome to infiltrate an Android device and requests permission to accessibility services. Once launched, it enables the malware to monitor the screen and interact with apps. Examination of the debug messages and source code reveals the threat actor is Turkish-speaking.

Analyst note:

- Crocodilus's advanced device takeover capabilities, including its signature overlay screen urging targets to back up their crypto wallet keys, are likely lead to broader geographical targeting beyond Spain and Turkey.

| **Exploit and Vulnerability Intelligence** |

| Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox has 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 a total of three vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on [March 27](#), [March 31](#), and [April 1](#). CISA also released six industrial control system (ICS) advisories on [March 27](#), [April 1](#), and [April 3](#). Microsoft identified a vulnerability, CVE-2025-1268, in a [range of Canon printer drivers](#). A Verizon Call Filter App vulnerability discovered and fixed in February 2025 enabled threat actors to [retrieve call log data for any Verizon number](#) and carry out surveillance against targets. [CVE-2025-1219](#) was found in certain versions of PHP when requesting a web resource using DOM or SimpleXML extensions, which could lead to data errors or security check bypass. Versions of Splunk Enterprise and Splunk Cloud Platform [affected with the CVE-2025-20229 vulnerability](#) could enable a least-privileged user without admin access to exploit missing security checks. Apple released a [series of patches](#) for visionOS, macOS, Safari, iOS, iPadOS, and watchOS, some of which address a zero-day vulnerability.



CRITICAL

CVE-2025-31579

What happened: A vulnerability was discovered in EXEIdeas International WordPress (WP) AutoKeyword Plugin up to 1.0. Affecting an unknown code, the flaw enables malicious actors to carry out SQL injection attacks. Reportedly, the [flaw can be exploited easily](#), though the technical details are unavailable and an exploit is not publicly available.

- **What this means:** An SQL injection attack is likely to enable a malicious actor to directly access a website's database, facilitating data theft. In the event of an exploit, it is likely to have an impact on confidentiality, integrity, and availability. Moreover, the vulnerability can be exploited remotely. The exploit's value is estimated to be between USD 0-5,000. Due to unknown countermeasures, it is recommended that users replace the affected product with an alternative.
- **Affected products:**
 - WordPress WP AutoKeyword Plugin versions 1.0 and before

**HIGH****CVE-2025-26683**

What happened: A flaw was detected in Microsoft Azure Playwright (version unknown), the exploitation of which may lead to an improper authorization vulnerability. The vulnerability leads to the product's unresponsiveness or incorrect authorization during an attempted access to a resource or an action. The flaw has neither been disclosed publicly, nor has it been exploited in the wild (EITW). There is currently no patch available.

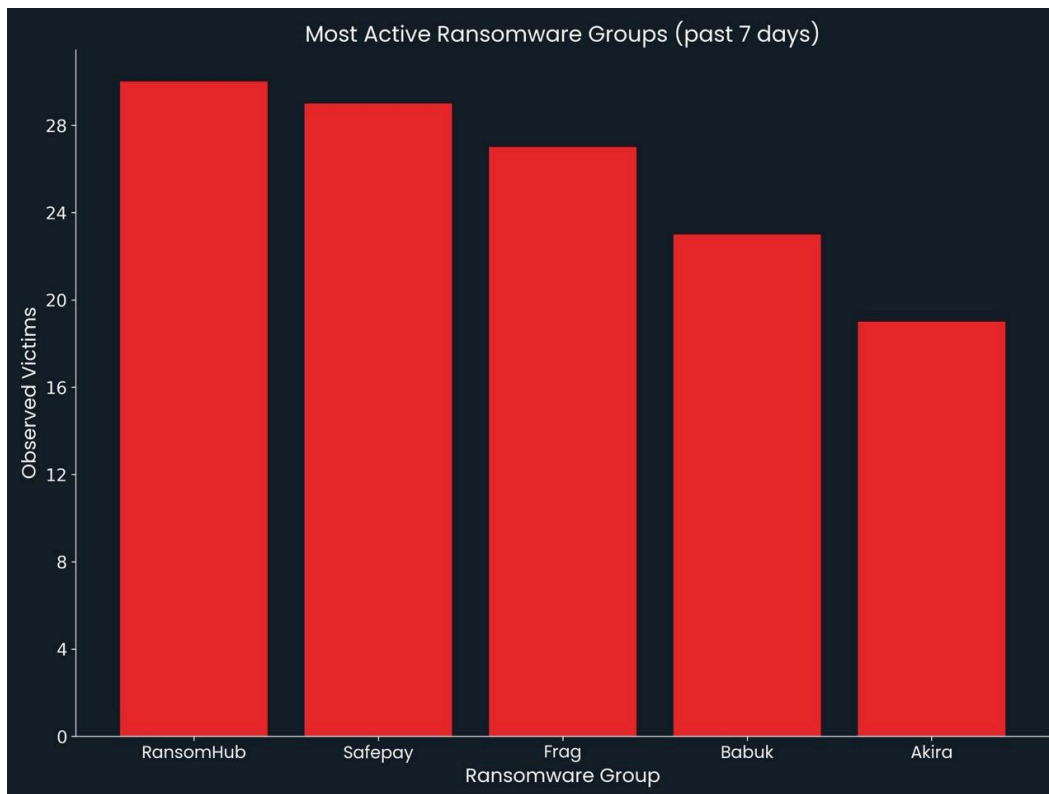
- **What this means:** There is a roughly even chance exploiting this vulnerability will lead to elevated privileges over a network. It is likely to compromise web application testing and source code.
- **Affected products:**
 - Microsoft Azure Playwright

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

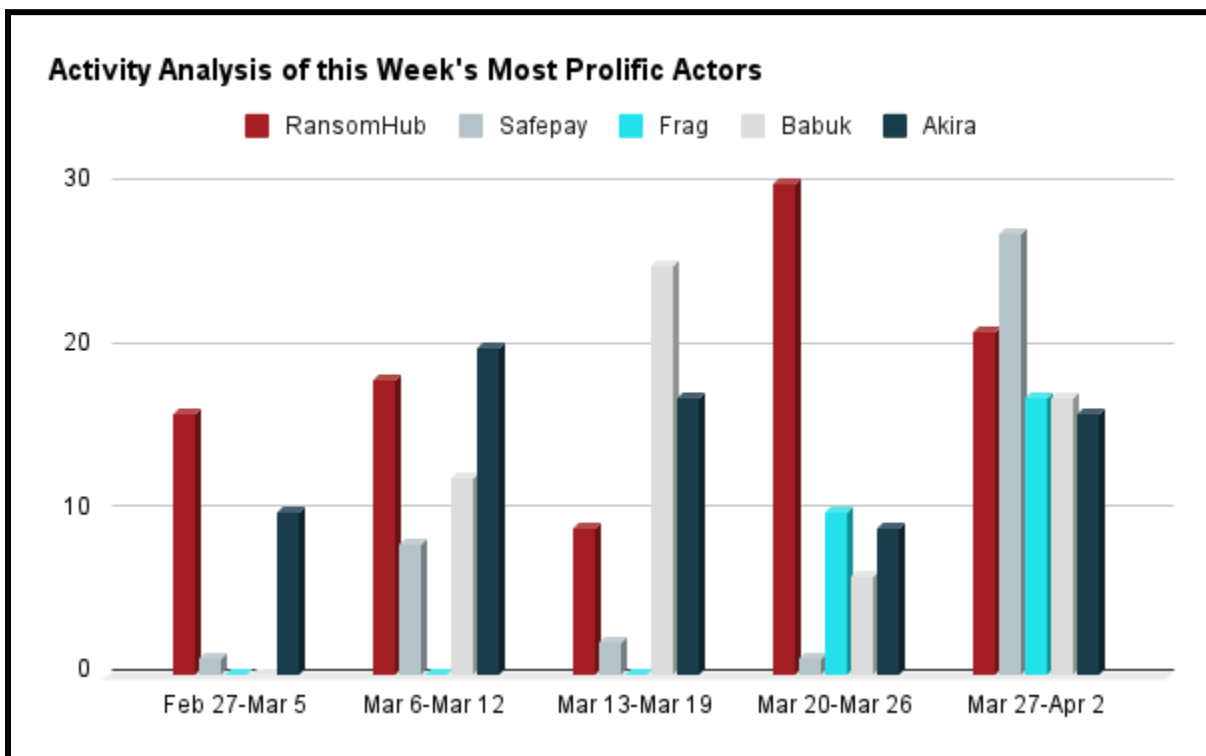


Ransomware Alert: Actors' Activity, Industry Impact, and Key Updates



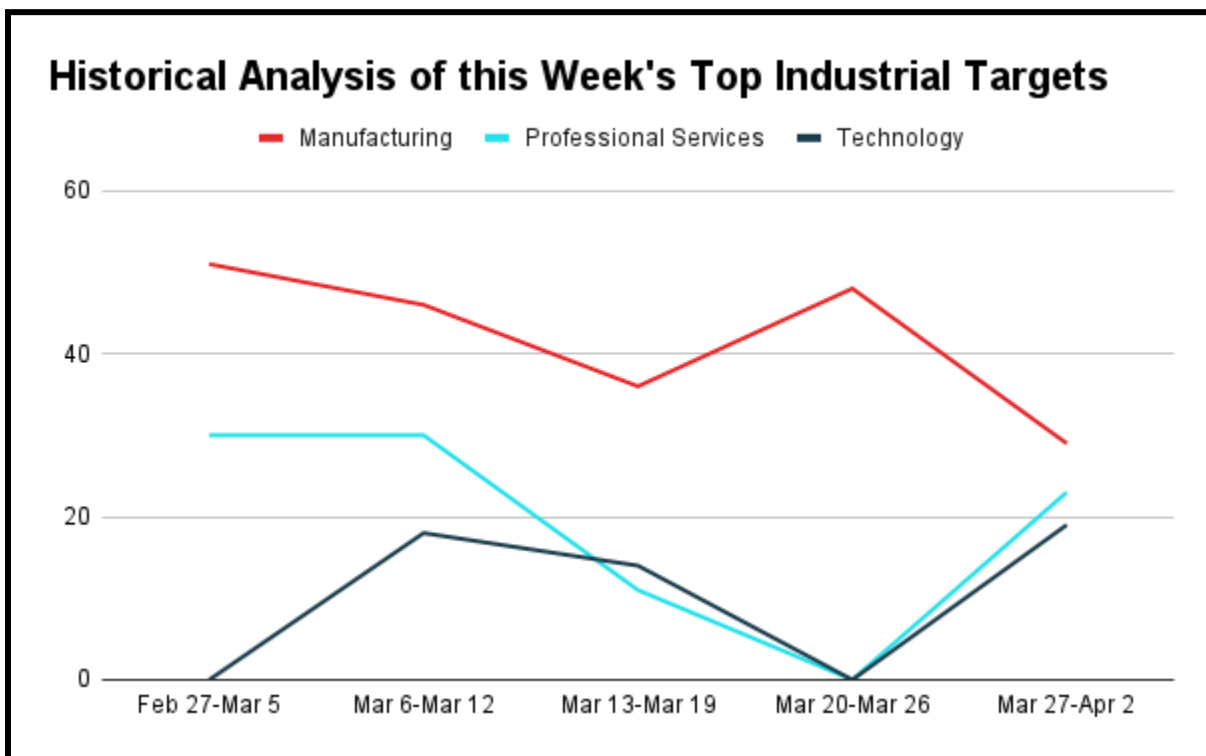
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, RansomHub, Safepay, Frag, Babuk, and Akira were the most active ransomware groups. ZeroFox observed at least 227 ransomware victims disclosed, most of which were located in North America. RansomHub accounted for the largest number of attacks.



Source: ZeroFox Internal Collections

Threat group activity trend: This week, RansomHub, Safepay, Frag, Babuk, and Akira were the most prominent groups. This graph shows their activities over the past five weeks. ZeroFox observed Frag ransomware group's activities between Week 4 and Week 5, with no activity detected in the preceding weeks. RansomHub and Akira have been active throughout all five weeks, with at least 94 and 72 attacks, respectively.



Source: ZeroFox Internal Collections

Ransomware trends in industries: Over the past five weeks, ZeroFox has observed that the majority of ransomware victims belong to the Manufacturing sector, followed by Professional Services. The Manufacturing sector, in particular, has consistently seen a high number of attacks, with at least 210 incidents recorded over the five weeks.

Recap of major ransomware events observed in the past week: A [ransomware attack on Kuala Lumpur International Airport \(KLIA\)](#) in Malaysia led to several hours of disruption. While it is unlikely for ransomware groups to engage in forums, [Qilin ransomware group has recently joined the predominantly English-language dark web forum BreachForums](#). [SimonMed Imaging recently confirmed](#) that it was affected by a cyberattack earlier this year that led to unauthorized access to patient data through one of its vendors. The Medusa ransomware group has claimed responsibility for the attack. ZeroFox observed a [new ransomware leak site](#) named for "Chaos" ransomware.



Major Data Breaches Across the Globe in the Past Week

Targeted Entity	<u>Samsung Germany</u>	<u>Oracle Health</u>	<u>X (Twitter)</u>
Number of Firms/Victims Affected	Approx. 270,000 customer records	Yet to be determined	2.8 billion users' data
Compromised Data and Infrastructure	Personally identifiable information (PII) such as names, addresses, and email addresses, as well as transaction information, order numbers, tracking URLs, support interactions, and communication between the customer and Samsung	Patient information from electronic health records	Profile metadata, such as account creation dates, user IDs and screen names, profile descriptions, and URLs; location and time zone settings; display names (current and from 2021); follower counts from both 2021 and 2025; post counts and timestamps of the last post; friends count, listed count, and favorites count; source of the last post (such as TweetDeck or X Web App); and status settings (like whether the profile is verified or protected)
Suspected Threat Actor	GHNA	Andrew	ThinkingOne
Country/Region	Germany	United States	United States
Industry	Technology	Technology	Media/Entertainment
Possible Repercussions	Impersonation, identity theft and fraud, phishing and social engineering attacks, credential harvesting and account takeovers, and financial fraud	Extortion and blackmail, identity theft and fraud, financial fraud, ransomware, phishing attacks, social engineering attacks, and doxxing	Social engineering and phishing attacks, credential stuffing and account takeover, doxxing, impersonation, identity theft, and fraud

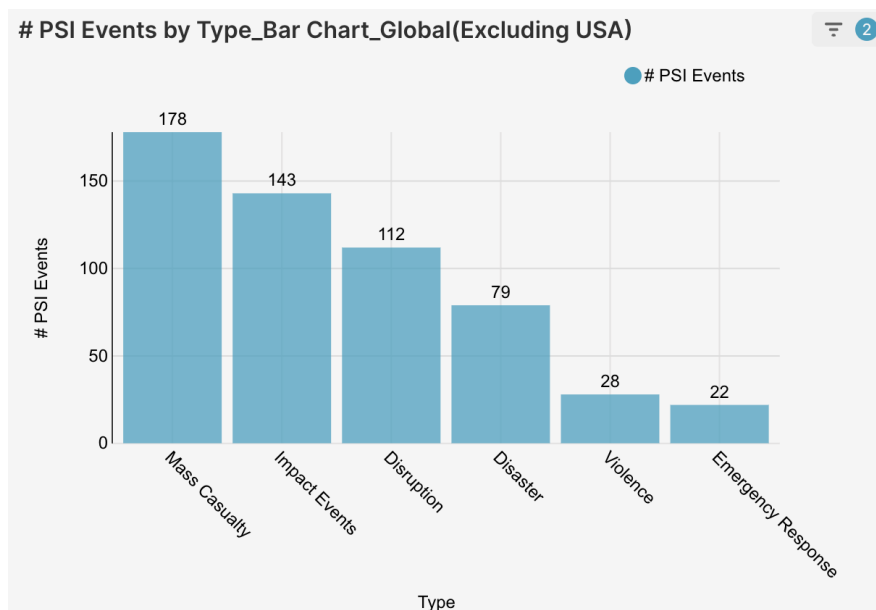
Three major breaches observed in the past week

Other major data breaches observed in the past week: [Check Point has denied a data breach](#) claimed by hacker "CoreInjection" on BreachForums, stating the data is recycled and not from a recent breach. Untested threat actor "Clear_Voice" has claimed to be [selling a GitHub user database](#). Threat actor "constanttemptin" has allegedly [advertised an alleged leak of 2.6 billion Facebook records](#) in a user:pass and phone:pass format. Untested threat actor "GHNA" claimed to have [leaked a database](#) associated with UK-based postal service and courier company Royal Mail.

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

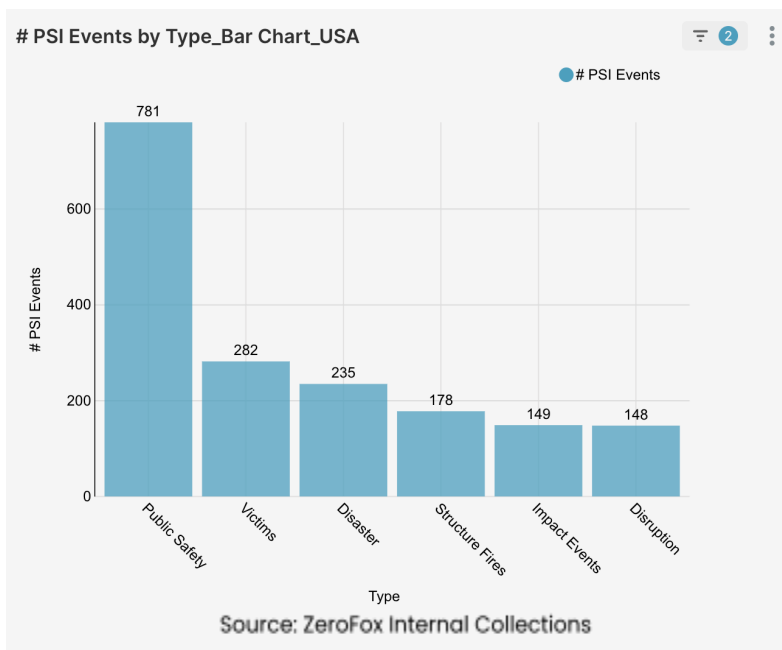
Physical Security Intelligence: Global



Source: ZeroFox Internal Collections

What happened: Excluding the United States, ZeroFox observed at least 178 mass casualty alerts and 143 impact event alerts. Turkey is [unlikely to face significant external pressure](#) following the arrest of Istanbul mayor Ekrem Imamoglu, the chief political rival of President Recep Tayyip Erdogan. The country has made itself indispensable to international partners due to its leadership roles in Ukraine and Syria and in containing immigration. News of Imamoglu's arrest triggered heavy losses in Turkish capital markets. Stocks saw their worst week since the 2008 financial crisis, losing 16 percent of their value before recovering slightly. Unrest will likely continue in the short to medium term and will remain focused around major urban areas, especially Istanbul. On April 1, 2025, [China started another round of joint military and coastguard drills](#) around Taiwan that included the Shandong aircraft. The joint exercises involved sea-air combat-readiness patrols, joint seizure of comprehensive superiority, assault on maritime and ground targets, and blockade on key areas and sea lanes, sending a warning to the self-ruled Taiwan against seeking formal independence. On April 2, 2025, South Korea, Japan, and China [held talks on responding](#) to the United States' reciprocal tariff plans. Meanwhile, Myanmar's military [has announced a temporary ceasefire](#) from April 2 to 22 to speed up relief and reconstruction efforts following last week's devastating earthquake, which has claimed more than 3,000 lives. Rebel groups had unilaterally declared a ceasefire earlier, but the military initially refused.

Physical Security Intelligence: The United States



What happened: In the past week, ZeroFox has observed that public safety was the most alerted sub-type in the United States, with New York reporting the highest number of alerts, at 98. At least 40 natural disaster alerts were observed originating in California, [amid severe weather](#) with several Californian cities being subjected to tornado warnings. A [large tornado also broke out in Lake City](#), Arkansas, one among many spotted across the state recently.

| 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%