



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

March 22, 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 March 20, 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 Brief – Underground Economist: Volume 5, Issue 5	2
ZeroFox Brief – Introduction to Social Engineering: Romance Scams	2
ZeroFox Intelligence Flash Report – GitHub Repositories Targeted in Malicious Cyber Activity	2
 Cyber and Dark Web Intelligence Key Findings	4
Ongoing Phishing Campaign Uses ClickFix and Impersonates Booking[.]com	4
Cybercriminals Spreading Malware Disguised as DeepSeek AI Web and App Installers	5
ChatGPT Flaw Sees 10,000 Attacks in a Week; Financial Institutions Susceptible	6
 Exploit and Vulnerability Intelligence Key Findings	8
CVE-2025-2345	8
CVE-2025-21590	9
 Ransomware and Breach Intelligence Key Findings	11
Ransomware Update: Top Actors, Industry Impact, and Key Updates	11
Major Data Breaches in the United States in the Past Week	14
 Physical and Geopolitical Intelligence Key Findings	16
Physical Security Intelligence: Global	16
Physical Security Intelligence: United States	17
 Appendix A: Traffic Light Protocol for Information Dissemination	18
 Appendix B: ZeroFox Intelligence Probability Scale	19

| This Week's ZeroFox Intelligence Reports

[ZeroFox Intelligence Brief – Underground Economist: Volume 5, Issue 5](#)

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

[ZeroFox Brief – Introduction to Social Engineering: Romance Scams](#)

Romance scams are a type of confidence scheme whereby a threat actor seeks to exploit a victim's romantic emotions—usually to achieve a financial objective. Romance scams take many forms and are perpetrated by a host of different types of threat actors, from individuals seeking punitive retribution to semi-structured collectives sometimes able to extort millions of dollars in revenue. Threat actors conducting romance scams are rapidly incorporating artificial intelligence (AI)-driven technology into their toolsets, augmenting attack techniques during victim selection and initial contact phases through to exploitation. Threat actors conducting romance scams are very likely to continue evolving their attack techniques in 2025, circumventing security hygiene measures and capitalizing upon the challenges faced by national and international law enforcement bodies.

[ZeroFox Intelligence Flash Report – GitHub Repositories Targeted in Malicious Cyber Activity](#)

Since approximately March 14, 2025, GitHub repositories have been targeted in two likely separate malicious cyber campaigns, resulting in the likely compromise of user credentials, accounts, and sensitive information associated with continuous integration (CI) and continuous development (CD) tools. At least 12,000 separate repositories have reportedly been targeted in a phishing campaign that leverages open authorization (OAuth) abuse to deceive users into granting attackers access to accounts and credentials. The seemingly separate targeting of GitHub Actions via a supply chain compromise tracked by the National Institute of Standards and Technology (NIST) as CVE-2025-30066 was also first reported on March 14, 2025. Subsequent research suggests that this initial incident may have facilitated the more recent targeting of the “tj-actions/changed-files” Action. As of the writing of this report the full extent of this activity is unclear, but there is a very likely chance that associated GitHub Actions remain compromised.

| Cyber and Dark Web Intelligence |

| Cyber and Dark Web Intelligence Key Findings



Ongoing Phishing Campaign Uses ClickFix and Impersonates Booking[.]com

What we know:

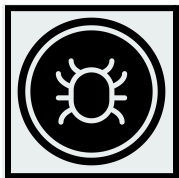
- A threat actor dubbed “Storm-1865” is impersonating Booking[.]com webpages in an ongoing campaign to trick victims into downloading malware through a technique called ClickFix.
- Storm-1865 sends targets an email pretending to be Booking[.]com, raising fake issues such as negative reviews left by customers and asking them to respond to the issue by clicking on a link.
- The link deploys a social engineering tactic that uses a fake CAPTCHA page with a blurred background mimicking Booking[.]com webpage, along with instructions for the user to launch a command on Windows to install the malware.

Background:

- The malware is capable of stealing financial data and credentials.
- The ClickFix tactic tricks users into clicking on malicious links using a dialog box and instructing users to run a command.
- Due to Booking[.]com’s international presence, threat actors are able to target users worldwide, from North America and South Asia to Oceania and Western Europe.

What is next:

- Storm-1865 is very likely to continue its phishing campaign targeting Booking[.]com’s hospitality aggregators, customers, and employees. Similar attacks have been reported in [2023](#).
- Continued Booking[.]com or similar hospitality-related phishing attempts are likely to be high during holiday seasons.
- Customers leaving public reviews on Booking[.]com are likely to be targeted by threat actors using social engineering tactics.



Cybercriminals Spreading Malware Disguised as DeepSeek AI Web and App Installers

What we know:

- Cybercriminals are exploiting DeepSeek AI's popularity to spread malware by disguising themselves as DeepSeek web and mobile app installers for Windows, Mac, and Android.

Background:

- Malicious actors are deploying search engine optimization (SEO) poisoning tactics—using trending search terms like DeepSeek AI—to redirect users to fake websites designed to spread malware such as CATCHA pages urging command execution, crypto miners, keyloggers, and password stealers.

Analyst note:

- SEO poisoning of widely searched emerging technologies could be used by cybercriminals for malicious activities. Users are advised to remain alert about website or application clones and sham installers for both personal computers and mobile phones.



ChatGPT Flaw Sees 10,000 Attacks in a Week; Financial Institutions Susceptible

What we know:

- Over 10,000 exploit attempts on a medium severity flaw (CVE-2024-27564) in ChatGPT were recorded in one week from a single IP address; the attacks targeted government and financial institutions in several countries but were primarily focused in the United States.

Background:

- The exploit, which is known as a Server-Side Request Forgery (SSRF) attack, enables hackers to make unauthorized server requests to collect sensitive data, potentially causing data leaks.

Analyst note:

- Organizations operating ChatGPT/OpenAI-driven services and integrations with vulnerable systems are likely to be susceptible to data breaches and system compromise.

| **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 five new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation on [March 18](#) and [March 19, 2025](#). CISA also released 20 Industrial Control Systems (ICS) advisories on [March 13](#) and [March 18, 2025](#). These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS. Meanwhile, a critical remote code execution (RCE) vulnerability [CVE-2025-24813](#) was exploited in Apache Tomcat. This vulnerability could enable attackers to manipulate file uploads and potentially execute malicious code to exploit it for remote code access, installing malware on affected devices. Other prominent vulnerabilities tracked this week include a popular third-party GitHub Action, tj-actions/changed-files (tracked as [CVE-2025-30066](#)), which has been compromised. The supply chain compromise allows for information disclosure of sensitive data including, but not limited to, valid access keys, GitHub Personal Access Tokens (PATs), npm tokens, and private RSA keys. [CVE-2024-10442](#) is an off-by-one error vulnerability in the transmission component of Synology Replication Service and Synology Unified Controller (DSMUC) and enables remote attackers to execute arbitrary code.

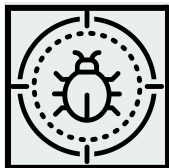


CRITICAL

CVE-2025-2345

What happened: A vulnerability was found in IROAD Dash Cam X5 and Dash Cam X6 up to 20250308. The manipulation leads to improper authorization, allowing remote attackers to potentially access sensitive user data, control device settings, or exploit the camera for malicious purposes. It is possible to initiate the attack remotely.

- **What this means:** Threat actors could access sensitive data like addresses, license plate numbers, personal conversations, and destinations, which could be leaked or sold on the dark web.
- **Affected products:**
 - IROAD Dash Cam X5
 - IROAD Dash Cam X6 up to 20250308

**MEDIUM****CVE-2025-21590**

What happened: CVE-2025-21590 is an improper isolation or compartmentalization vulnerability in the kernel of Juniper Networks Junos OS and enables a local attacker with high privileges to compromise the integrity of the device.

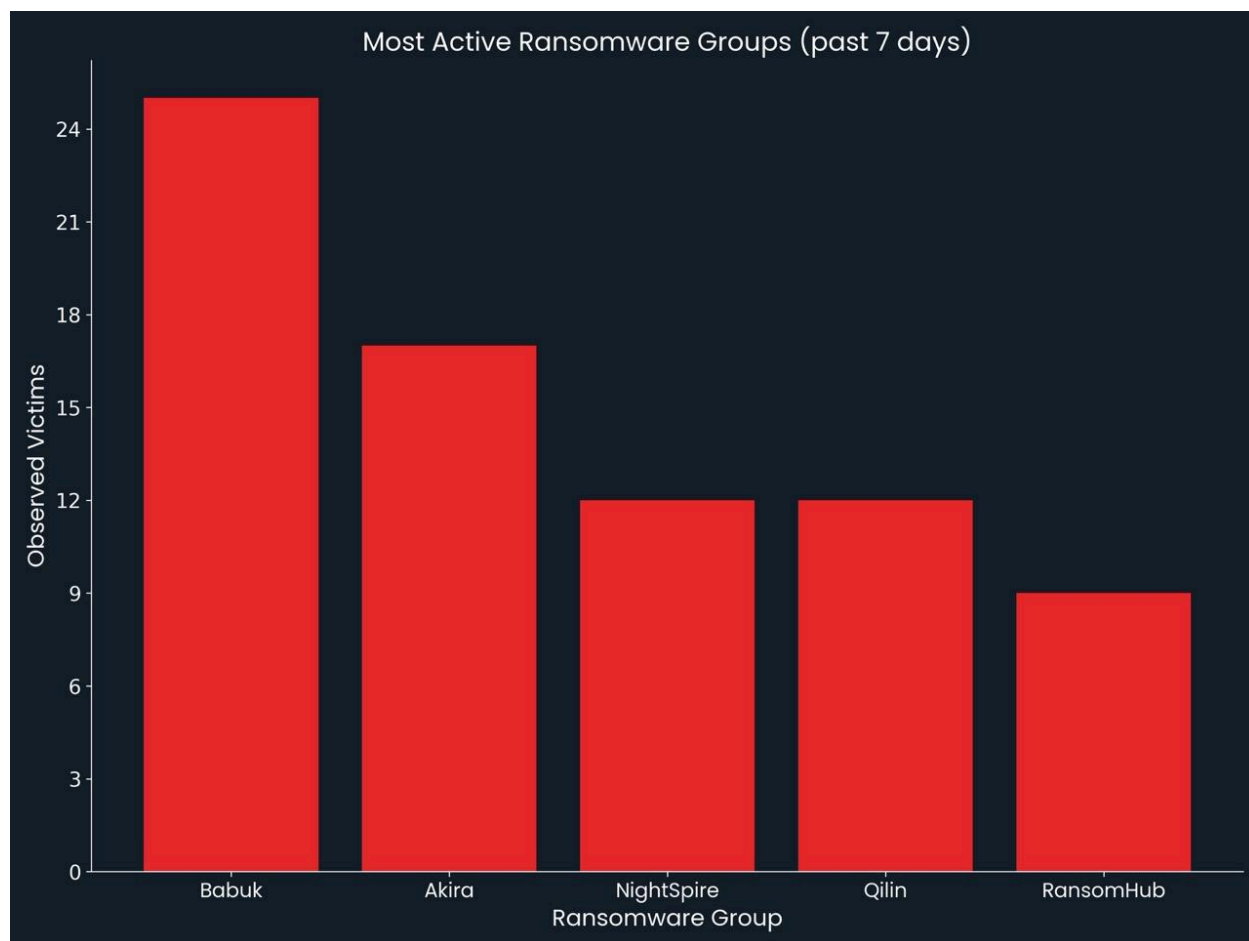
- **What this means:** EOL devices no longer receive updates and support as they reach the end of their lifecycle, but users with such devices that do not replace older models for newer ones likely expose themselves to unmitigated risks.
- **Affected products:**
 - All Junos OS versions before 21.2R3-S9
 - 21.4 versions before 21.4R3-S10
 - 22.2 versions before 22.2R3-S6
 - 22.4 versions before 22.4R3-S6
 - 23.2 versions before 23.2R2-S3
 - 23.4 versions before 23.4R2-S4
 - 24.2 versions before 24.2R1-S2, 24.2R2

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

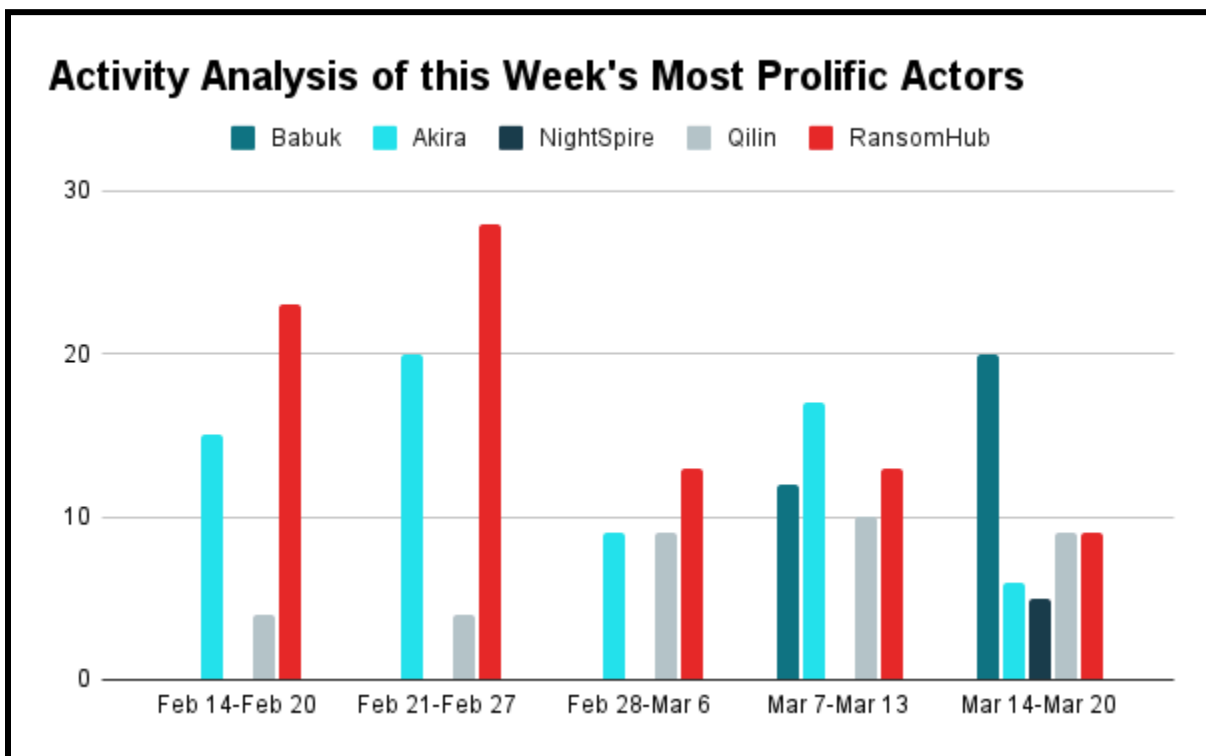


Ransomware Update: Top Actors, Industry Impact, and Key Updates



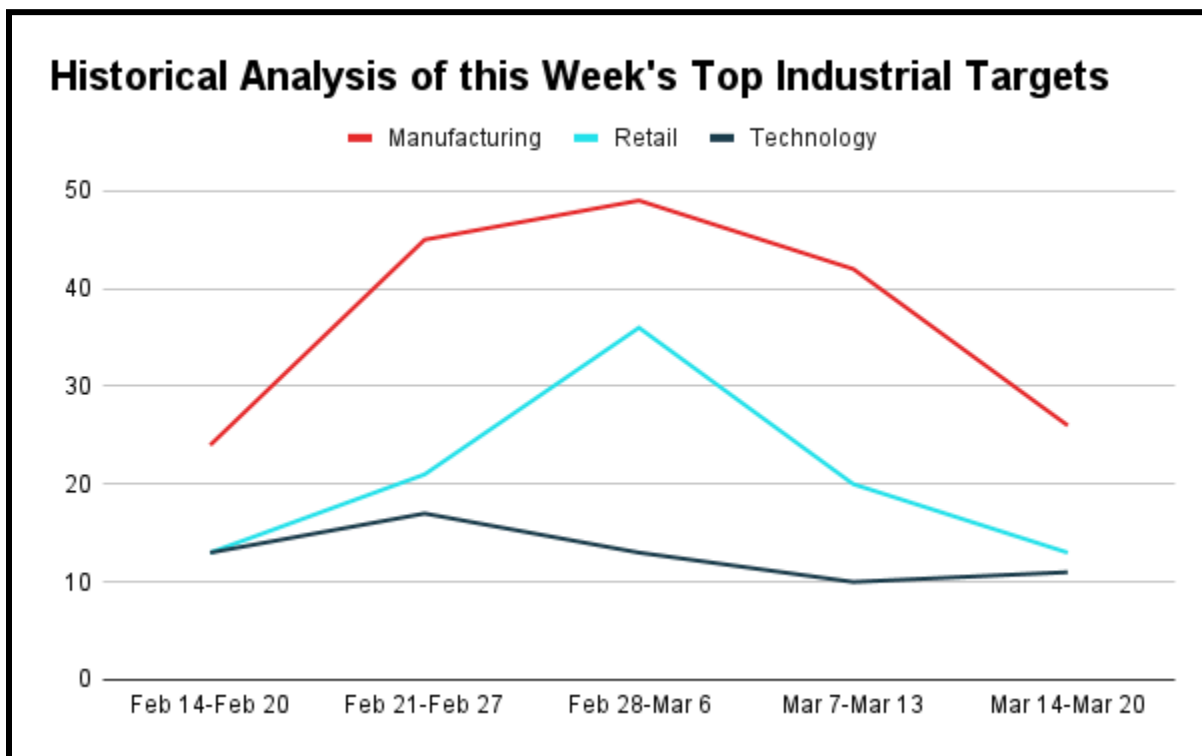
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Babuk, Akira, NightSpire, Qilin, and RansomHub were the most active ransomware groups. ZeroFox observed at least 139 ransomware victims disclosed, most of which were located in North America. The Babuk ransomware group accounted for the largest number of attacks.



Source: ZeroFox Internal Collections

Threat group activity trend: The RansomHub ransomware group was the most active during the first three weeks (Feb. 14 – Mar. 6) of the five-week review period, executing at least 86 attacks overall. ZeroFox observed that the Babuk ransomware group became active in the fourth week (Mar. 7 – Mar. 13), conducting at least 32 attacks in total during that week and the following week (Mar. 14 – Mar. 20). Additionally, a newly observed ransomware group, NightSpire, has been active over the past seven days, with at least five attacks attributed to it.



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 the retail sector. The manufacturing sector, in particular, has consistently seen a high number of attacks, with at least 186 incidents recorded over the five weeks).

Recap of major ransomware events observed in the past week: Novel ransomware group Mora_001, which has probable links to LockBit, [has been exploiting two bugs](#) (CVE-2024-55591 and CVE-2025-24472) affecting Fortinet firewall appliances to deliver ransomware strain SuperBlack. The Akira ransomware encryption on Linux/ESXi systems [has been cracked using sixteen RTX 4090 GPUs](#), allowing victims to recover locked data without paying the hackers. New incidents have emerged of [scammers falsely claiming to be affiliated with the Cl0p ransomware gang](#) in order to extort businesses and coerce companies into making payments. RansomHub is [targeting U.S. firms in a campaign involving SocGhosh](#) (a FakeUpdates malware-as-a-service), multiple threat actors, and compromised websites. According to a new analysis of leaked Black Basta chat logs, [Russian officials likely assisted the group's leader](#) (known as GG or Tramp) in escaping custody after they were detained in Armenia last June.



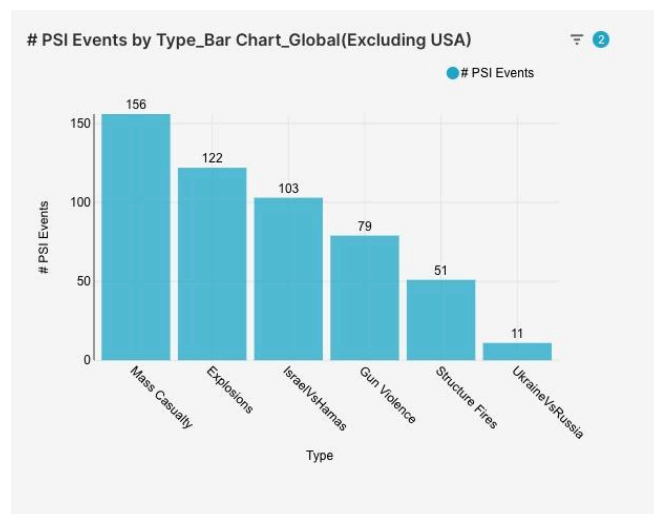
Major Data Breaches in the United States in the Past Week

Targeted Entity	California Cryobank	Western Alliance Bank	Pennsylvania State Education Association (PSEA)
Number of Firms/Victims Affected	Yet to be determined	21,899	517,487
Compromised Data Fields	Names, bank accounts and routing numbers, Social Security numbers, driver's license numbers, payment card numbers, and/or health insurance information	Personal information, including names and Social Security numbers, dates of birth, financial account numbers, driver's license numbers, tax identification numbers, and/or passport information	Personal, financial, and health data (including driver's license or state IDs), Social Security numbers, account PINs, security codes, payment card information, passport information, taxpayer ID numbers, credentials, health insurance, and medical information
Suspected Threat Actor	Yet to be determined	Yet to be determined	Yet to be determined
Country	United States	United States	United States
Industry	Healthcare	Financial Services	Education
Possible Repercussions	Identity fraud, financial fraud, medical fraud, phishing attacks, account takeover, ransomware and extortion	Financial fraud, identity theft, account takeover, social engineering and phishing attacks, tax fraud, ransomware attacks	Phishing attacks, identity theft, financial frauds, medical fraud, account takeover, social engineering and phishing attacks, tax fraud, fake claims and benefits fraud, credential theft, and ransomware and extortion

Three major breaches observed in the past week

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings



Source: ZeroFox Internal Collections

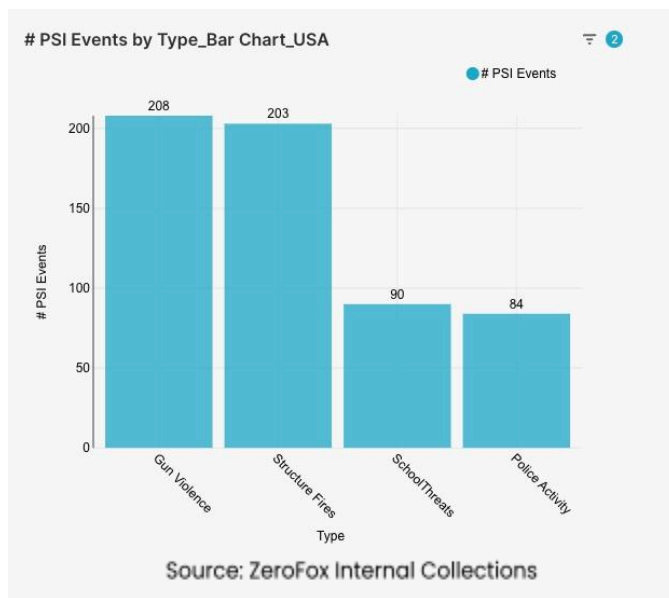
Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 7 percent decrease in mass casualty events this week from the previous week, with the top contributing countries being Palestine, Syria, and Pakistan, in that order. Approximately 78 percent of these events were explosions, and the three aforementioned countries accounted for about 45 percent of all mass casualty alerts. General alerts related to the

Israel-Hamas War (including protests, raids, and involvement in neighboring countries) increased by 45 percent from the previous week. Events related to Russia's war in Ukraine decreased by 8 percent. The top three most-alerted subtypes were explosions, which saw a 34 percent increase from the previous week; gun violence, which decreased by 15 percent; and structure fires, which increased by 96 percent. Global protest activity decreased by 2 percent.

- **What this means:** Both explosions and alerts related to the Israel-Hamas war increased significantly, which is in accordance with the fact that Israel has officially broken the already-fragile [ceasefire](#) agreement and launched heavy attacks on Gaza on March 18 that killed over 400 people. Israel also conducted strikes on March 17 in Daraq, [Syria](#), which killed at least three people and injured 19 others. These are the latest in a string of attacks targeting Syria after Sunni Muslim Islamist fighters toppled President Bashar al-Assad in December. As for the Russia-Ukraine conflict, which saw a slight decrease in alerts this week, there was a partial ceasefire instated on March 18 in which Russian President Vladimir Putin agreed to halt attacks on Ukrainian energy [infrastructure](#). U.S. talks on Ukraine are due to continue on March 23 in Saudi Arabia. Pakistan had the third highest number of mass casualty alerts this week, which may be due to growing separatist militant group activity. For instance, the [Baloch Liberation Army](#) conducted a suicide bombing on March 16 which killed at least five people just days after the same group hijacked a train and held hostages for 36 hours. Pakistani authorities have vowed to crack down on the growing insurgencies.

Physical Security Intelligence: United States



What happened: In the past week, the top three most-alerted incident subtypes were gun violence, structure fires, 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. Gun violence across the United States overall decreased by 5 percent from the week prior. Police activity alerts decreased by 2 percent. Structure fires decreased by 10 percent.

- **What this means:** This week, President Donald Trump made several contentious decisions that sparked debate. As part of his stated crackdown on immigration, Trump invoked the [Alien Enemies Act](#) to deport over 250 migrants to El Salvador earlier this week. U.S. District Judge James Boasberg was unsuccessful in his attempt to [reverse](#) the deportations, causing advocates to fear that invoking the act will open the door for targeting and deportations of other individuals, regardless of their citizenship status or criminal record. Additionally, orders to drastically cut down on funding to both the [U.S. Agency for International Development](#) and the [U.S. Department of Education](#) have resulted in protests and general dissent from citizens across the country, as well as praise from Trump's supporters. The U.S. political landscape as a whole is evolving rapidly, and it is yet to be fully determined how this will affect the overall physical security of the nation.

| 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%