



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

March 29, 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 27, 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 Flash Report: Financial Scams Threaten U.S. Tax Returns	2
ZeroFox Intelligence Flash Report: Unrest in Israel and Gaza; War Resumes	2
 Cyber and Dark Web Intelligence Key Findings	4
Oracle Debacle: Oracle Denies Breach Claims; Evidence Suggest Otherwise	4
Navigation Systems Face Rising Threats	5
Chinese Threat Actor Found Lurking in Asian Telecom Network for Four Years	5
 Exploit and Vulnerability Intelligence Key Findings	8
CVE-2025-23120	8
CVE-2025-29927	9
 Ransomware and Breach Intelligence Key Findings	11
Ransomware Update: Top Actors, Industry Impact, and Key Updates	11
Significant Data Breaches at Major Institutions	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	19
 Appendix B: ZeroFox Intelligence Probability Scale	20

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Flash Report: Financial Scams Threaten U.S. Tax Returns

As the April 15 deadline of the 2024–2025 U.S. tax season nears, ZeroFox Intelligence has identified a notable increase in financial fraud-related activity seeking to exploit the spike in use of government services such as the Internal Revenue Service (IRS) and private financial services. Historically, the end of the U.S. tax season has been perceived as a lucrative targeting opportunity by financially motivated threat actors seeking to obtain compromised account credentials, personally identifiable information (PII), or personal financial information (PFI) to exploit tax return processes. Threat actors engaging in this activity deploy targeted social engineering schemes, malicious domains mimicking popular financial service platforms, and bespoke services available in deep and dark web (DDW) forums. Malicious activity targeting U.S. tax return processes and the PII and PFI associated with them is very likely to continue over the coming weeks. If users engaging with the IRS experience delays, there is a likely chance that they will continue to be targeted in the weeks following the April 15, 2025, tax filing deadline.

ZeroFox Intelligence Flash Report: Unrest in Israel and Gaza; War Resumes

The resumption of hostilities in Gaza and a number of controversial domestic political initiatives led by Prime Minister Benjamin Netanyahu have triggered major unrest in Israel. In the absence of pressure from the United States, Israel will likely be able to continue a moderately sized offensive indefinitely. Anti-government demonstrations, regardless of their size, are unlikely to influence the Israeli government's efforts in Gaza or domestically; however, the intervention of labor unions could potentially affect the government's thinking. Cyber groups are likely to increase their threats against Israel and its allies via website defacements and distributed denial-of-service (DDoS) attacks, but the main cyber risks come from groups aiming to distribute information on Israeli military and government targets.

| Cyber and Dark Web Intelligence |

| Cyber and Dark Web Intelligence Key Findings



Oracle Debacle: Oracle Denies Breach Claims; Evidence Suggest Otherwise

What we know:

- Alleged leaked data samples and reported email exchanges between the threat actor and multiple sources suggest the Oracle cloud breach is likely authentic, despite the company's denial.
- Representatives from different companies mentioned in the sample data have reportedly confirmed the authenticity of the data associated with their respective organizations.
- Last week, Oracle publicly denied [claims made by threat actor "rose87168"](#) about having stolen six million users' data.
- The hacker demanded over USD 200 million in crypto from Oracle in exchange for revealing how they breached the servers, which the company refused to pay.

Background:

- Rose87168 reportedly shared an Archive[.]org link showing a text file on Oracle's login.us2.oraclecloud[.]com server containing its email, which likely indicates that the actor breached the server and could create files on it.
- Researchers found another Archive[.]org link that showed the login.us2.oraclecloud[.]com server was running Oracle Fusion Middleware 11g, as of February 17, 2025.
- This version of the software had a bug, CVE-2021-35587, which enables unauthenticated access to Oracle Access Manager. The actor claims this exploit was used in the breach.
- Oracle has since taken the server offline following reports of the alleged breach.

What is next:

- The threat of subsequent exploitation posed to the alleged victim organizations listed by rose87168 remains unclear.
- Should an actor obtain the advertised information, they would almost certainly encounter subsequent security challenges.
- ZeroFox notes an [apparent lack of the information and leverage needed](#) to easily conduct exploitative activity, such as decrypted passwords and the necessary tokens and certificates.



Navigation Systems Face Rising Threats

What we know:

- International organizations [are warning of increasing jamming and spoofing attacks](#) on global navigation satellite systems (GNSS) that could pose a risk to aviation, maritime, and telecom safety across the globe.

Background:

- GNSS are networks of satellites, ground stations, and receivers that provide precise positioning, navigation, and timing (PNT) data. They are essential for global transportation, telecommunications, emergency response, infrastructure management, and other industries.

Analyst note:

- Jamming and spoofing attacks are components of the ongoing hybrid warfare utilized in various conflicts. Such attacks could disrupt flight navigation, communications, hinder military movements, and threaten civilian safety. [Russia was accused](#) of such interference last year.



Chinese Threat Actor Found Lurking in Asian Telecom Network for Four Years

What we know:

- China-linked threat actor “Weaver Ant” has been discovered lurking in the network of a major Asian telecommunications company for over four years, reportedly spying and collecting sensitive information.

Background:

- Weaver Ant used a number of web shells, including the China Chopper (developed by Chinese hackers), and other tools to gain persistent access and lateral movement in the network system while avoiding detection. So far, neither the target telecom company nor its specific location has been revealed.

Analyst note:

- It is likely that Weaver Ant is among the ranks of Chinese state-sponsored actors that engage in cyber espionage missions across the world, as the [2024 iSoon APT operation revealed](#). Critical infrastructure—especially in Asia, Europe, and North America—is typically the target of such actors.

| **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) released a total of three vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on [March 24](#) and [March 26](#). CISA has also released [four](#) industrial control system (ICS) advisories. Google has patched a Chrome zero-day vulnerability, CVE-2025-2783, that was being [exploited to break out of the browser's sandbox and deliver malware](#). CVE-2025-2664 is a vulnerability [found in CodeZips Hospital Management System 1.0](#). Five critical vulnerabilities (CVE-2025-24514, CVE-2025-24513, CVE-2025-1098, CVE-2025-1097, and CVE-2025-1974) in the [Ingress NGINX Controller for Kubernetes](#) have been disclosed, which potentially enable unauthenticated remote code execution. Enterprise-grade file sharing platform CrushFTP urged users to immediately patch an [unauthenticated HTTP\(S\) port access vulnerability](#) resolved on March 21, 2025, that could result in unauthorized access. A threat actor dubbed "EncryptHub" has [reportedly exploited a newly patched zero-day](#), CVE-2025-26633, and has exfiltrated data from compromised devices.



CRITICAL

CVE-2025-23120

What happened: There is a [deserialization vulnerability](#) in Veeam Backup and Replication, which enables remote code execution (RCE) by authenticated domain users. Veeam addressed the issue in version 12.3.1 (build 12.3.1.1139). Users are advised to update to this patched version to mitigate associated risks.

- **What this means:** This flaw could enable attackers with domain user privileges to execute arbitrary code on affected systems, potentially compromising the entire network and escalating privileges for further malicious activities such as data theft, system manipulation, or full network compromise.
- **Affected products:**
 - Veeam Backup & Replication 12.3.0.310 and all earlier version 12 builds

**CRITICAL****CVE-2025-29927**

What happened: There is a critical vulnerability in the Next.js open-source web development framework that could allow attackers to bypass authorization checks. This flaw lets attackers send requests that directly reach destination paths, circumventing essential security measures. This vulnerability has been addressed in Next.js versions 14.2.25 and 15.2.3.

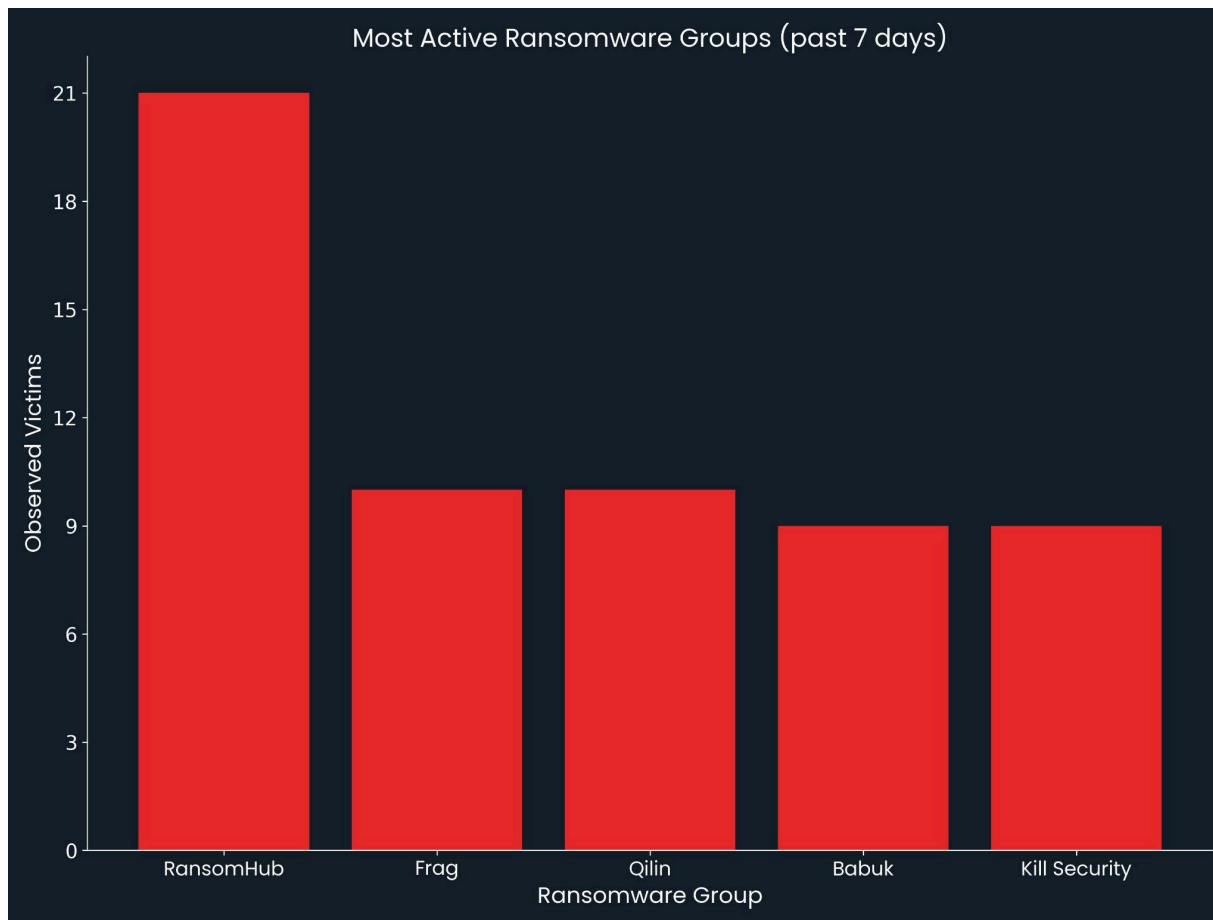
- **What this means:** This vulnerability allows attackers to bypass critical authorization checks, enabling them to access restricted resources without proper validation. This could lead to unauthorized access, data exposure, or other malicious activities, potentially compromising the security of the affected systems.
- **Affected products:**
 - Affects all Next.js versions prior to 15.2.3, 14.2.25, 13.5.9, and 12.3.5.

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

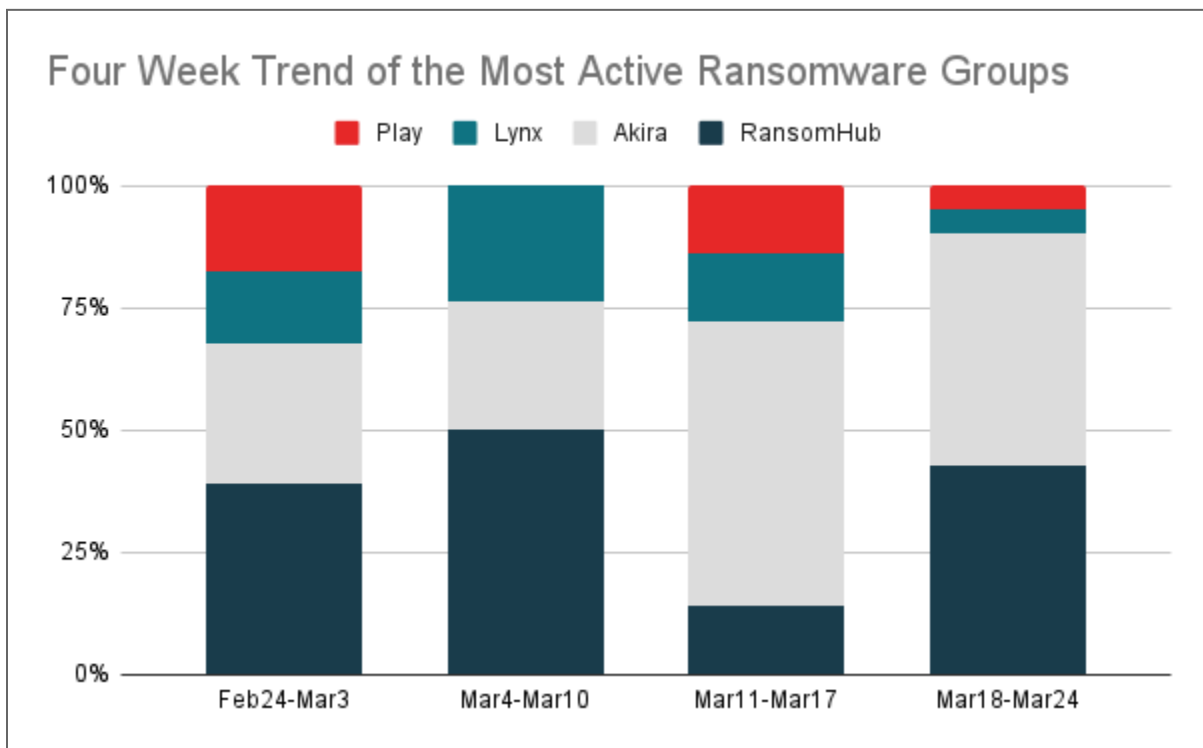


Ransomware Update: Top Actors, Industry Impact, and Key Updates



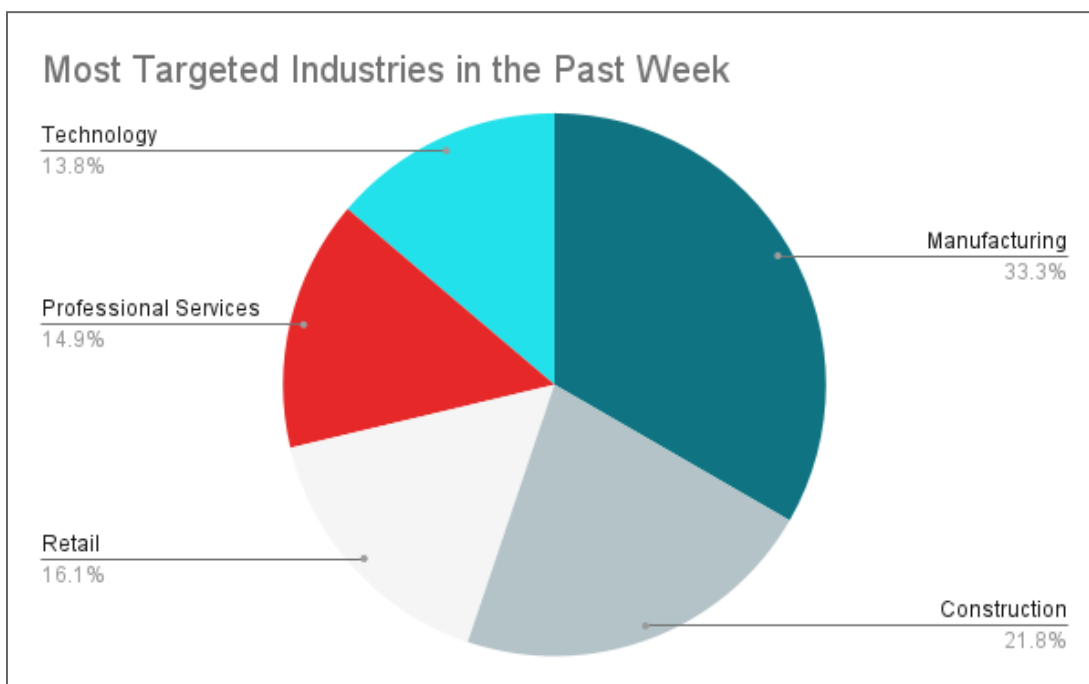
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, RansomHub, Frag, Qilin, Babuk, and Kill Security were the most active ransomware groups. ZeroFox observed at least 131 ransomware victims disclosed, most of which were located in North America. The RansomHub ransomware group accounted for the largest number of attacks.



Source: ZeroFox Internal Collections

Threat group activity trend: ZeroFox observed that ransomware groups RansomHub, Akira, Lynx, and Play conducted a total of 176 attacks in the past four weeks. RansomHub was the most active in the first week (Feb. 24 – Mar. 3), recording 29 attacks, and considerably lowered its attack tempo over the next three weeks, dropping to nine in week four (Mar. 18 – Mar. 24). Akira was the second most-active following RansomHub, conducting the most number of attacks (25) in week 3 (Mar. 11 – Mar. 17). Lynx and Play's highest number of attacks were 11 and 13, respectively, although ZeroFox observed zero attacks by Play in week two (Mar. 4 – Mar. 10).



Source: ZeroFox Internal Collections

Ransomware trends in industries: Over the past seven days, ZeroFox has observed that the majority of ransomware victims belonged to the manufacturing sector, followed by the construction sector. The manufacturing sector has consistently seen a high number of attacks, with at least 29 incidents recorded in the past week.

Recap of major ransomware events observed in the past week: A new ransomware-as-a-service (RaaS) operation called [VanHelsing has emerged](#), targeting multiple platforms and offering affiliates up to 80 percent of ransom payments. It forbids attacks on Commonwealth of Independent States (CIS) countries and has already listed three victims, including a Texas city and two tech firms. The Russian-speaking cyber espionage group [RedCurl has been linked to ransomware attacks for the first time](#), deploying a new strain called QWCrypt. This indicates a shift in tactics, with the group combining espionage with encryption-based extortion while using social engineering and dynamic link library (DLL) side-loading for stealthy infections. The Arkana Security ransomware group claims to have [hacked a U.S. telecom provider](#), stealing customer data and taking control of critical systems. Arkana Security has threatened to leak the stolen data unless a ransom is paid, leveraging doxxing and extortion tactics.



Significant Data Breaches at Major Institutions

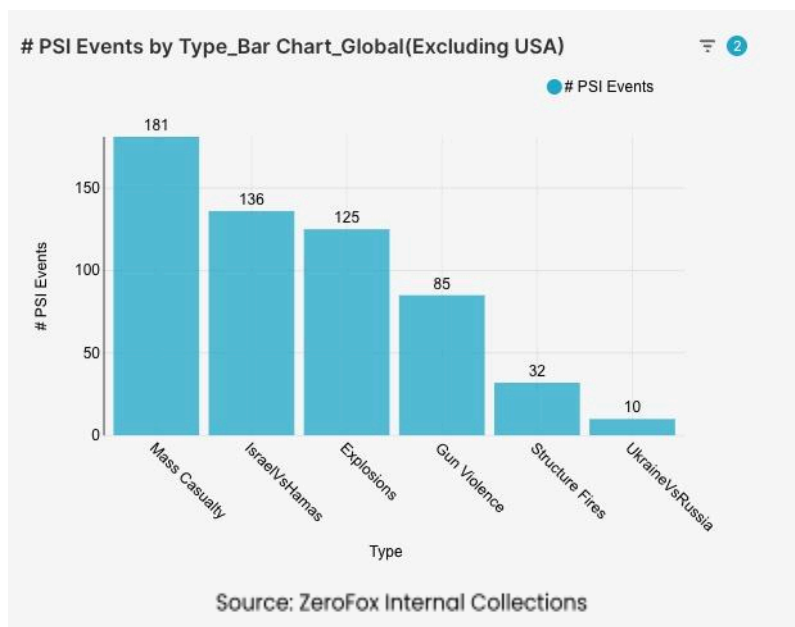
Targeted Entity	Numotion	Unnamed Telco Company	NYU
Number of Firms/Victims Affected	494,326 individuals	1 company affected	3 million applicants
Compromised Data and Infrastructure	Email accounts, names, dates of birth, product information, payment and financial account information, health insurance information, medical information, Social Security numbers, and driver license numbers	Network intelligence, credential harvesting, and continuous access to data	Applicants' names, test scores, majors, and zip codes, as well as information about family members and financial aid dating back to at least 1989; demographic data, city and zip codes, and citizenship status; and Common Application data
Suspected Threat Actor	Unidentified	Weaver Ant	Unidentified
Country/Region	United States	Asia	United States
Industry	Healthcare	Telecommunications	Education
Possible Repercussions	Identity theft, phishing scams, financial fraud, and unauthorized access	Remote code execution, initial access sold on the dark web, and data exfiltration	Extortions and blackmail, doxxing, fraudulent loan applications, phishing scams, and identity theft

Three major breaches observed in the past week

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global



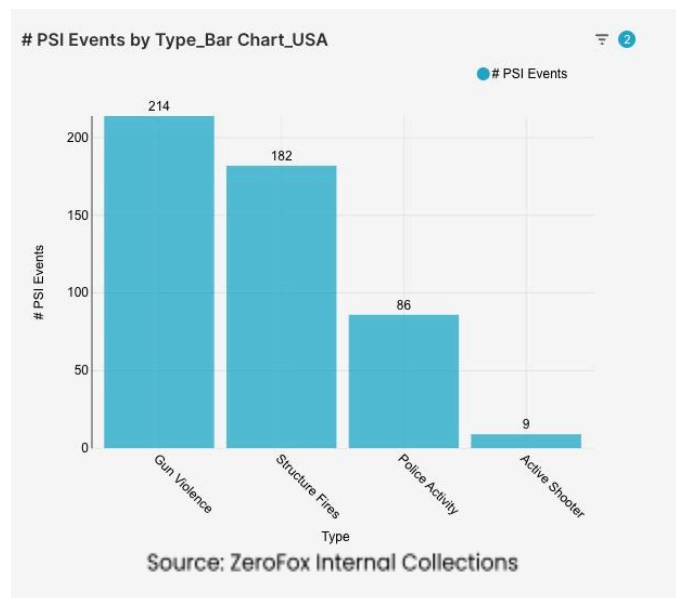
What happened: Excluding the United States, there was a 16 percent increase in mass casualty events this week from the previous week, with the top contributing countries being Palestine, Syria, and Israel (in that order). Approximately 69 percent of these events were explosions, and the three aforementioned countries accounted for about 33 percent of all mass casualty alerts. General alerts related to the Israel-Hamas War (including protests, raids, and involvement

in neighboring countries) increased by 32 percent from the previous week. Events related to Russia's war in Ukraine decreased by 9 percent. The top three most-alerted subtypes were explosions, which saw a 2 percent increase from the previous week; gun violence, which increased by 8 percent; and structure fires, which decreased by 37 percent. Global protest activity increased by 70 percent. On March 28, [a strong 7.7-magnitude earthquake hit Mandalay, Myanmar](#), with tremors felt in Bangkok, the capital of Thailand, and the northern city of Chiang Mai.

- **What this means:** After the dismantling of the ceasefire between Israel and Hamas last week, Israel has [launched](#) a new wave of airstrikes followed by ground operations in three key areas of Palestine: the Netzarim Corridor, Gaza's northern coastline, and Rafah. This may explain the rise in mass casualty alerts, explosions, and general alerts related to the Israel-Hamas war this past week, along with Palestine having the highest number of mass casualty alerts. With 59 Israeli hostages remaining in captivity under Hamas, Israel has seen some of its biggest [protests](#) since the beginning of the war; on March 2, more than 100,000 people demonstrated in Tel Aviv, Jerusalem, and other cities calling for the release of the hostages as well as new elections in the Israeli government. This is reflected in the sharp spike in protests alerted this week, as these demonstrations have [continued](#) for

several consecutive days. Israel is also engaging in attacks against Syria, which had the second-highest number of mass casualty alerts this week. On March 25, six people were killed in an Israeli [attack](#) in Koya, Syria, as part of a string of violence along the border between the two countries. Israeli Prime Minister Benjamin Netanyahu has demanded the complete demilitarization of southern Syria, to which the current government may not agree.

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. The top two states that had the most gun violence alerts were Illinois and Ohio, which together made up 19 percent of this week's nationwide total. Gun violence across the United States overall increased by 3

percent from the week prior. Police activity alerts increased by 2 percent, and the top contributing state was California. Structure fires decreased by 10 percent, and the top two states for this subtype were California and New York. Notably, protest activity increased by 19 percent, and active shooter alerts increased by 125 percent.

- **What this means:** This week, there were eight [mass shootings](#) in the United States, which contributed to the significant increase of active shooter alerts. One of these events took place on March 21 in [Las Cruces, New Mexico](#), and resulted in three deaths and 15 injuries; another in [Jackson, Mississippi](#), on March 22 caused the death of one person and injured seven others. The Jackson incident along with the slight increases in police activity and gun violence nationwide, may be connected to the plethora of St. Patrick's Day festivities which occurred over the weekend, as many people gather in crowded areas and may consume alcohol in excessive amounts. Protest activity also saw a notable increase this week, with New York and District of Columbia being the top contributing locations. These

demonstrations have been organized by groups such as People Over Profits and Disruption Project to denounce Tesla CEO [Elon Musk](#) and his involvement in the federal government. Protestors have gathered in large numbers at Tesla showrooms in major cities, and there have been instances of people setting charging stations and individually owned Tesla vehicles on [fire](#).

| 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%