



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

March 15, 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 13, 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 – Anonymous Sudan Announces Return in Telegram Group	2
ZeroFox Flash Report – Cyberattack Suspected in Worldwide X Outage	2
U.S. Policy Shift in Ukraine Upends European Defense Sector	3
 Cyber and Dark Web Intelligence Key Findings	5
SideWinder APT Expands Reach Across Multiple Industries in Asia, the Middle East, and Africa	5
Chinese Spy Volt Typhoon's Cyberattack on U.S. Power Utility Lasted a Year	6
FBI Denver Warns of Online File Converter Scam	6
 Exploit and Vulnerability Intelligence Key Findings	9
CVE-2025-24201	9
CVE-2025-21590	10
 Ransomware and Breach Intelligence Key Findings	12
This Week in Ransomware: Group and Industry Trends	12
Data Breaches Hit Critical Infrastructure	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 – Anonymous Sudan Announces Return in Telegram Group

In January 2025, ZeroFox observed a new Telegram channel claiming to be associated with the hacktivist collective Anonymous Sudan. According to posts made in the channel, the collective has resumed operations under the name “Anonymous Sudan Second Battalion.” Statements posted in the channel indicate the resurgence is very likely motivated by an intent to inflict punitive retribution against institutions perceived by the collective as opposed to the political policies of the Russian Federation, Palestinians, and Sudan. During January, the collective claimed to have conducted a number of distributed denial-of-service (DDoS) attacks targeting entities located in African nations (primarily Uganda and Libya). There is a likely chance that the new Telegram channel is reflective of a legitimate Anonymous Sudan resurgence. In such a case, there is a roughly even chance that the collective will resume the targeting of U.S., Europe, and Israel-based entities in the short to medium term.

ZeroFox Flash Report – Cyberattack Suspected in Worldwide X Outage

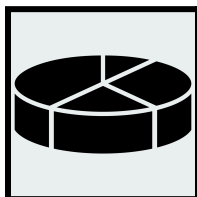
On March 10, 2025, social media platform X (formerly Twitter) experienced multiple service outages affecting a reported 1.6 million users worldwide and lasting several hours. As of the writing of this report, X services appear to be functional. Several hours later, the Dark Storm threat collective posted on its Telegram channel, claiming to have conducted a DDoS attack which resulted in X being “taken offline.” Ideologically motivated hackers, particularly pro-Russia hacktivist collectives, almost certainly view Elon Musk—and his high-profile government appointment and assumed political allegiances—as an acceptable and in-bounds target for disruptive cyberattacks. There is a likely chance that Dark Storm is responsible for a DDoS attack targeting X infrastructure as claimed. Although the collective offered no evidence to support its involvement, there is a robust correlation between the chosen target, Dark Storm’s publicly stated allegiances and motivations, and the historic tactics, techniques, and procedures (TTPs) of other pro-Russia, anti-Western hacktivist collectives.

U.S. Policy Shift in Ukraine Upends European Defense Sector

Trump administration officials have signaled their priority is to end the conflict between Russia and Ukraine—and return Russia to the global economy—rather than to continue to lend military and financial support to assist Ukraine’s war efforts with Russia. European states have responded to this drastic policy shift from post-World War II security arrangements with significant alterations to their defense spending and military postures. ZeroFox has observed an increase in financially motivated threat actors targeting European defense companies, which will likely benefit from the additional trillions in defense spending.

| Cyber and Dark Web Intelligence |

| Cyber and Dark Web Intelligence Key Findings



SideWinder APT Expands Reach Across Multiple Industries in Asia, the Middle East, and Africa

What we know:

- SideWinder, an advanced persistent threat (APT) group, has focused its attacks on maritime and logistics companies across South and Southeast Asia, the Middle East, and Africa.
- Recent attacks follow a pattern whereby spear phishing emails distribute infected documents that exploit a vulnerability within a mathematical tool in a popular documentation application.
- These attacks initiate a multi-phase process leading to the use of a .NET downloader called ModuleInstaller that ultimately deploys StealerBot, a post-exploitation toolkit.

Background:

- The APT also targets the telecommunications, real estate, IT services, and hospitality sectors.
- The APT group has also focused on diplomatic entities in various nations, including Afghanistan, India, and Saudi Arabia.
- Lure documents related to the nuclear and maritime sectors have been observed as part of the group's social engineering efforts.
- The group had previously been suspected to be based in India.
- The group continuously updates its tools to bypass security measures, maintain access, and conceal its presence on compromised networks.

What is next:

- Targeting diplomatic entities could risk sensitive negotiations and potentially expose classified information, putting national security at risk and leading to diplomatic fallout, retaliatory actions, and a disruption in global cooperation on various issues.
- StealerBot facilitates post-exploitation activities, such as stealing sensitive data, credential harvesting, and enabling further system compromise, potentially leading to significant financial, operational, and strategic damage.

- Given the group's diverse targeting across multiple regions and sectors, SideWinder is very likely to continue its campaign against critical infrastructure and diplomatic entities in various countries.



Chinese Spy Volt Typhoon's Cyberattack on U.S. Power Utility Lasted a Year

What we know:

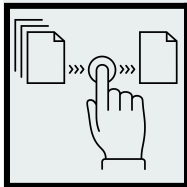
- Chinese espionage group Volt Typhoon was observed stealing critical infrastructure data, including information on geographical distribution of energy, from a U.S. power utility grid for 300 days in 2023.

Background:

- Littleton Electric Light and Water Departments (LELWD) in Massachusetts, which powers two towns with a collective population of 15,000, is a small and unusual target that reportedly has [no access](#) to large critical infrastructure.

Analyst note:

- The nature of the target suggests that Volt Typhoon was very likely seeking to [pre-position](#) itself into critical infrastructure networks, modify its TTPs to match the victim's environment for similar future attacks on possible larger targets, and prepare to disrupt operations in case of a major conflict with the United States.



FBI Denver Warns of Online File Converter Scam

What we know:

- The FBI Denver Field Office is warning online users that threat actors are exploiting free online document converter and downloader tools to load malware onto victims' computers, leading to incidents such as ransomware and identity theft.

Background:

- These cybercriminals are using free online tools that scrape submitted documents for personally identifiable information, banking data, and more.

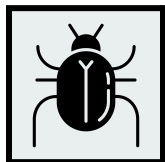
Analyst note:

- In this ongoing campaign, scammers are likely stealing financial information (including cryptocurrency account details) to make unauthorized transfers, conduct social engineering attempts like phishing, and maintain persistent access to these accounts to target entities transacting with affected users.

| **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 two Industrial Control System (ICS) advisories on March 11, 2025. It also added a total of 11 vulnerabilities to its [Known Exploited Vulnerabilities \(KEV\) Catalog](#) based on [evidence of active exploitation](#). Microsoft released its [March 2025 Patch Tuesday security updates](#) addressing 57 vulnerabilities, including patches for six actively exploited zero-day bugs. China-linked cyber espionage group UNC3886 has been exploiting an [improper isolation or compartmentalization vulnerability \(CVE-2025-21590\)](#) in end-of-life (EOL) Juniper MX routers. CVE-2025-25015 causes [prototype pollution in Kibana](#), which leads to arbitrary code execution via a crafted file upload and specifically crafted HTTP requests. Facebook warns that a [FreeType vulnerability \(CVE-2025-27363\)](#) can lead to arbitrary code execution and has been exploited in attacks. Apple has released patches for a zero-day bug (CVE-2025-24201) exploited in an ["extremely sophisticated attack against specific targeted individuals."](#)

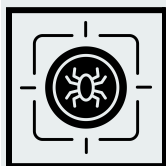


HIGH

CVE-2025-24201

What happened: Apple has released patches for a zero-day bug (CVE-2025-24201) that has been exploited in a sophisticated attack against targeted individuals. The vulnerability affects the WebKit of browsers like Safari, Chrome, and Firefox on Apple devices (with exceptions for alternate browsers in the European Union). The bug has been patched in iOS 18.3.2, iPadOS 18.3.2, and Apple Vision Pro visionOS 2.3.2.

- **What this means:** Without the patches, it is very likely hackers could track—or are already tracking—user activity on browsers and may attempt to target systems beyond browsers. Politically inclined persons or government officials are likely to be targeted, as similar flaws allegedly have been exploited by threat actors like Russian-backed Cozy Bear (aka APT29) in the past.
- **Affected products:**
 - Versions of iOS before iOS 17.2

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

What happened: China-linked cyber espionage group UNC3886 has been exploiting CVE-2025-21590 in the kernel of Juniper Networks' Junos OS end-of-life (EOL) Juniper MX routers. The improper isolation or compartmentalization flaw enables a local attacker with elevated privileges to compromise the integrity of the affected device.

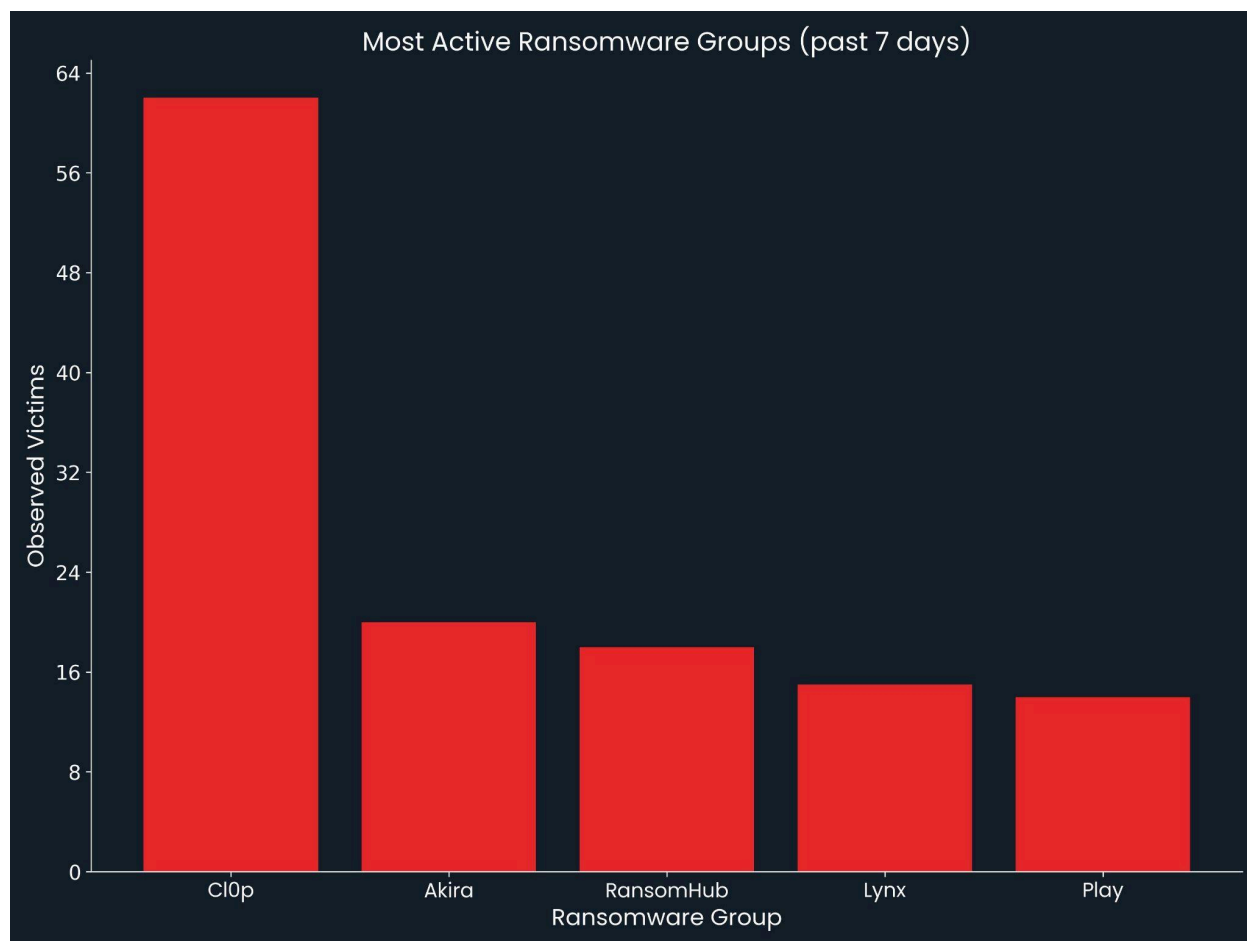
- **What this means:** EOL devices, such as the targeted Juniper MX routers, no longer receive software updates or support from the manufacturer. Any vulnerabilities discovered in these devices, including CVE-2025-21590, will remain unpatched, leaving them susceptible to exploitation by threat actors. Organizations that continue to use EOL devices likely expose themselves to significant security risks, as these devices become easy targets for attackers who are aware of their unmitigated vulnerabilities.
- **Affected products:**
 - All versions of Junos OS before 21.2R3-S9
 - Junos OS 21.4 versions before 21.4R3-S10
 - Junos OS 21.4 22.2 versions before 22.2R3-S6
 - Junos OS 21.4 22.4 versions before 22.4R3-S6
 - Junos OS 21.4 23.2 versions before 23.2R2-S3
 - Junos OS 21.4 23.4 versions before 23.4R2-S4
 - Junos OS 21.4 24.2 versions before 24.2R1-S2 and 24.2R2

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

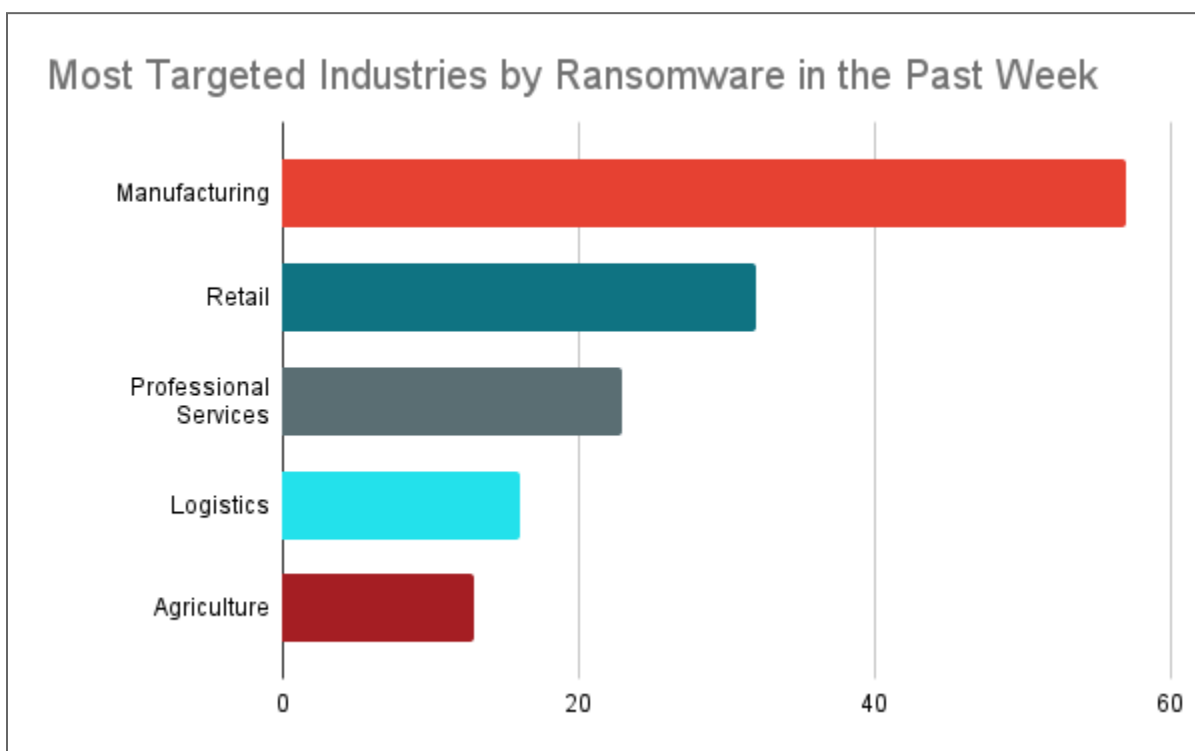


This Week in Ransomware: Group and Industry Trends



Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Cl0p, Akira, RansomHub, Lynx, and Play were the most active ransomware groups. ZeroFox observed at least 227 ransomware victims disclosed, most of which are located in North America. The Cl0p ransomware group accounted for the largest number of attacks.



Source: ZeroFox Internal Collections

Ransomware trends in industries: In the past week, the manufacturing and retail industries have been the most affected by ransomware attacks, followed by professional services, logistics, and agriculture. ZeroFox observed that the top five most-affected industries experienced a total of 141 attacks, with manufacturing facing 57 incidents.

Recap of major ransomware events observed in the past week: [Sunflower Medical Group has suffered a cyberattack](#) exposing the data of nearly 221,000 patients, including sensitive personal and medical details. The Rhysida ransomware gang has claimed responsibility, demanding a ransom. CISA and others have released a report ([#StopRansomware: Medusa Ransomware](#)) detailing TTPs, indicators of compromise, and detection methods associated with known Medusa ransomware activity. [Hunters International has claimed to have leaked 1.4 TB](#) of data reportedly stolen from Tata Technologies (Tata), including employee details and business contracts. The attack follows Tata's January disclosure of a ransomware incident affecting some IT assets.



Data Breaches Hit Critical Infrastructure

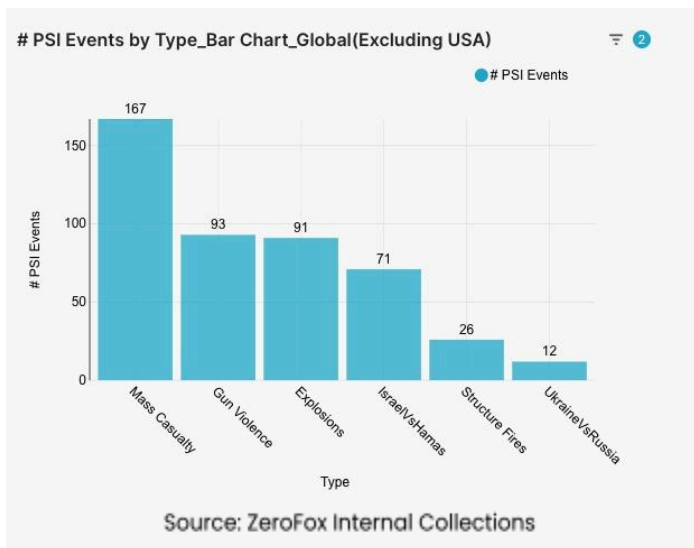
Targeted Entity	Center for Digestive Health	NTT Communications Corporation
Number of Firms/Victims Affected	122,437 individuals	18,000 corporate customers
Compromised Data Fields	Patient information like Social Security number, date of birth, and health information	Customer name (registered contract name), customer representative's name, contract number, phone number, email address, physical address, and service usage information
Suspected Threat Actor	BianLian	Not revealed
Country	The United States	Japan
Industry	Healthcare	Telecommunications
Possible Repercussions	Patient privacy violations, ransomware and digital extortion, blackmail, and further breaches	Remote control, persistence, scams, data sold to other actors, and identity theft

Two major breaches observed in the past week

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

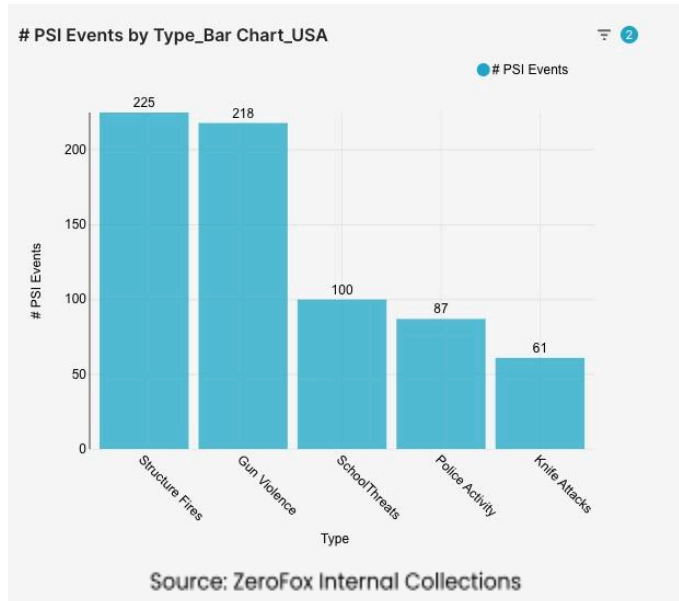


What happened: Excluding the United States, there was a 20 percent increase in mass casualty events this week from the previous week, with the top contributing countries being Syria, Palestine, and India (in that order). Approximately 54 percent of these events were explosions, and the three aforementioned countries accounted for about 32 percent of all mass casualty alerts. General alerts related to the Israel-Hamas War (including protests, raids, and involvement in neighboring countries) increased by 3

percent from the previous week. Events related to Russia's war in Ukraine decreased by 20 percent. The top three most-alerted subtypes were explosions, which saw a 2 percent increase from the previous week; gun violence, which increased by 33 percent; and structure fires, which decreased by 26 percent. Global protest activity increased by 18 percent.

- What this means:** This week saw a significant spike in gun violence, with Palestine having the most alerts for this subtype. On Wednesday, March 5, Israeli forces [raided](#) the Palestinian towns of Nablus, Qusra, Al-Rihiya village, and [Ramallah](#), all of which resulted in several civilians being shot. Israel's total [blockade](#) of the Gaza Strip continues as well, with no aid allowed to cross into the territory; meanwhile, Hamas representatives, Israeli delegates, and U.S. Envoy Steve Witkoff arrived in Qatar on March 12 to discuss a potential [ceasefire](#). In Syria, which saw the highest number of mass casualty events this week, [sectarian violence](#) has resulted in the deaths of at least 800 people in clashes between supporters of Bashar al-Assad and those loyal to the new Syrian regime. This, along with the ongoing violence in Gaza, may explain the significant increase in mass casualty events overall this week. As for Russia's war in Ukraine (which saw a decrease in alerts this week), talks of a 30-day [ceasefire](#) are being conducted; Ukrainian President Zelenskyy has suggested that this time can be used to draft a peace plan. Whether the Kremlin will be receptive to such a deal is still uncertain currently.

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 that had the most gun violence alerts were Illinois and California, which together made up 24 percent of this week's nationwide total. Gun violence across the United States overall

decreased by 14 percent from the week prior. Police activity alerts decreased by 27 percent, and the top contributing states were California and Texas. Structure fires decreased by 9 percent, and the top two states for this subtype were New York and California. Notably, knife attacks increased by 45 percent.

- What this means:** This week, New York had the highest number of fires, which is likely due to the [Long Island wildfires](#) that caused Governor Kathy Hochul to declare a state of emergency over the weekend. The fires have been completely contained, and officials will continue to patrol and address hot spots as they come up. Over the next week, however, nearly every region of the country will be at risk of [severe weather](#) due an upcoming storm that will cause hurricane-force winds, major flooding, blizzard conditions, and a possible tornado outbreak. While gun violence and police activity saw decreases this past week, knife attacks showed a significant spike, with California being the top contributor. One such instance involved a double stabbing in [Carmichael, CA](#), on March 6; just a few days later, a woman was stabbed on a train in [San Francisco, CA](#). Lastly, there are ongoing political tensions surrounding the detention and possible deportation of [Mahmoud Khalil](#), a pro-Palestinian protestor at Columbia University. The arrest sparked various demonstrations, as President Donald Trump heralded Khalil's arrest as the first "of many to come" and vowed on social media to deport individuals engaging in similar activities, which could lead to further protests across the country.

| Appendix A: Traffic Light Protocol for Information Dissemination

WHEN SHOULD IT BE USED?

Red

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.

Amber

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

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.

Clear

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%