



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

April 12, 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 10, 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 – Speculation Unfolds Surrounding RansomHub Cessation	2
 Cyber and Dark Web Intelligence Key Findings	4
AkiraBot AI Spam Campaign Targets 400,000 Websites	4
HellCat Ransomware Hits Four Firms Using Jira Credentials Acquired via Infostealers	5
New Hacking Assistant Xanthorox AI Emerges	5
 Exploit and Vulnerability Intelligence Key Findings	8
CVE-2025-32013	8
CVE-2024-48887	9
 Ransomware and Breach Intelligence Key Findings	11
Ransomware in Focus: Actors' Activity, Targeted Industries, and Ongoing Campaigns	11
Notable Data Breaches Worldwide in the Past Week	14
 Physical and Geopolitical Intelligence Key Findings	17
Physical Security Intelligence: Global	17
Physical Security Intelligence: United States	18
 Appendix A: Traffic Light Protocol for Information Dissemination	19
 Appendix B: ZeroFox Intelligence Probability Scale	20

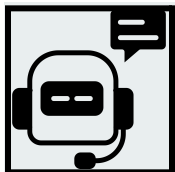
| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Flash Report – Speculation Unfolds Surrounding RansomHub Cessation

Ransomware and digital extortion (R&DE) collective RansomHub's dark web victim leak site has been offline since April 1, 2025, and no new victims have been observed. Around April 4, an account associated with the DragonForce R&DE collective posted on the Russian-speaking deep and dark web (DDW) forum RAMP, claiming that RansomHub "will be up soon" and that RansomHub had decided to move to DragonForce's infrastructure. As of the writing of this report, RansomHub is very likely non-operational, posing a significantly reduced threat to global organizations across industries. There is a likely chance that RansomHub will remain non-operational during the coming weeks. Should RansomHub's operations recommence, the collective will very likely suffer from significant reputational damage, regardless of whether original RansomHub or DragonForce infrastructure is leveraged.

| Cyber and Dark Web Intelligence |

| Cyber and Dark Web Intelligence Key Findings



AkiraBot AI Spam Campaign Targets 400,000 Websites

What we know:

- Malicious actors have used AkiraBot, a new artificial intelligence (AI)-driven spamming bot, to target over 400,000 websites since September 2024.
- The AI bot has managed to spam contact forms and chat widgets on at least 80,000 websites, making it harder to find genuine messages and thereby impacting customer trust in the businesses.
- The bot sends customized AI-written messages to target businesses with fraudulent services for a search engine optimization (SEO) network.

Background:

- AkiraBot uses large language models (LLM) such as GPT-4o-mini to craft personalized spam messages based on the targeted business that can bypass spam filters.
- The bot also evades network detections by using proxy services like the ones popular among advertisers.
- It mostly targets small and medium-sized businesses (SMBs) on popular website builders, largely due to their basic security measures.

What is next:

- Threat actors are likely to use AkiraBot or similar AI-driven bots to expand the phishing attack surface to include chat bots and contact forms on websites.
- These spam attacks are likely to result in disruptions to operations or lead to financial loss or data theft for SMBs.
- The generative AI-written, personalized nature of the spam messages is likely to increase the possibility of targets falling victim to malicious bots.



HellCat Ransomware Hits Four Firms Using Jira Credentials Acquired via Infostealers

What we know:

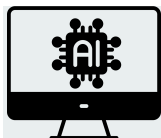
- The HellCat ransomware group has been observed targeting four companies in the United States and Europe using stolen Jira credentials. The group claims to have stolen files, financial information, and emails and has threatened to release them if its demands are not met.

Background:

- HellCat used stolen Jira credentials harvested by infostealer malware (StealC, Raccoon, Redline, and Lumma Stealer) months earlier to access internal systems, harvest data, and launch ransomware attacks.

Analyst note:

- HellCat likely targeted these companies' Jira accounts to access critical workflows, customer data, and internal documentation. Jira credentials could be associated with other clients and third-party companies, allowing the threat actors to use this stolen information as a valuable bargaining chip to extort ransom multiple times from the affected companies and their clients.



New Hacking Assistant Xanthorox AI Emerges

What we know:

- A sophisticated new AI platform, Xanthorox AI, has recently been observed circulating in cybercrime communities and forums and is reportedly based on five AI models.

Background:

- This AI platform offers a fully custom-built, modular system for code generation, vulnerability exploitation, data analysis, voice and image processing, and more. Unlike previous malicious AI tools, Xanthorox reportedly operates on private servers with proprietary models, enhancing attack precision and scalability.

Analyst note:

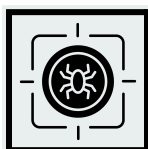
- This advanced AI tool is likely to assist in malware creation, vulnerability exploitation, and live voice-based social engineering campaigns. Additionally, attackers with little technical skill

could automate complex tasks, making it easier for less-experienced threat actors to launch attacks.

| **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 six vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on [April 4](#), [April 7](#), [April 8](#), and [April 9](#). Additionally, Ivanti released security updates to address CVE-2025-22457 in Ivanti Connect Secure, Policy Secure & ZTA Gateways; [CISA added this vulnerability](#) to its KEV catalog. [This month's Microsoft Patch Tuesday](#) includes security updates addressing 126 vulnerabilities, one of which is a zero-day flaw (CVE-2025-29824) that is currently being actively exploited. Among the fixes, 11 vulnerabilities are classified as "Critical," all of which are remote code execution flaws. [CVE-2025-30065 is a vulnerability in Apache Parquet](#) that enables attackers to exploit unsafe deserialization in malicious Parquet files to take control of target systems. A now-patched dynamic link library (DLL) search order hijacking [vulnerability in ESET's antivirus software](#) is being exploited by suspected China-backed advanced persistent threat group "ToddyCat".



HIGH

CVE-2025-32013

What happened: A server-side request forgery (SSRF) vulnerability has been discovered in LNbits' LNURL authentication-handling functionality.

- **What this means:** LNbits is a Lightning wallet and accounts system. This vulnerability could enable attackers to specify internal network addresses and access internal resources on affected devices. This is likely to enable unauthorized access to internal resources of a wallet, like the seed phrase, resulting in theft.
- **Affected products:**
 - LNbits versions before 0.12.12 and 0.12.12



CRITICAL
CVE-2024-48887

What happened: An unverified password change vulnerability in Fortinet's FortiSwitch graphical user interface (GUI) could enable a remote unauthenticated attacker to change admin passwords via a specially crafted request.

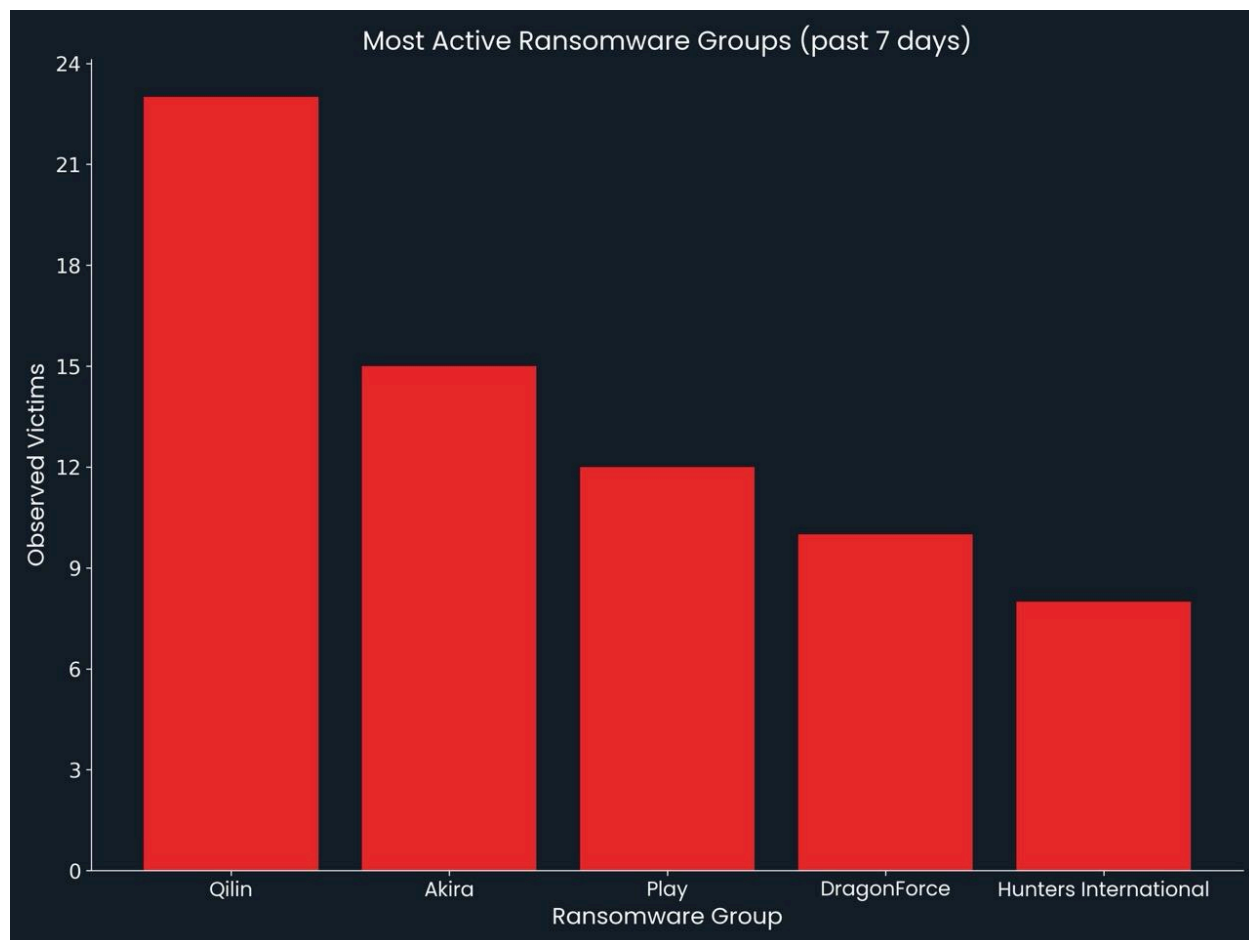
- **What this means:** By changing admin passwords, threat actors could disable security settings and introduce backdoors into affected devices.
- **Affected products:**
 - Fortinet FortiSwitch versions 7.6.0, from 7.4.0 through 7.4.4
 - Fortinet FortiSwitch versions 7.2.0 through 7.2.8
 - Fortinet FortiSwitch versions 7.0.0 through 7.0.10
 - Fortinet FortiSwitch versions 6.4.0 through 6.4.14

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

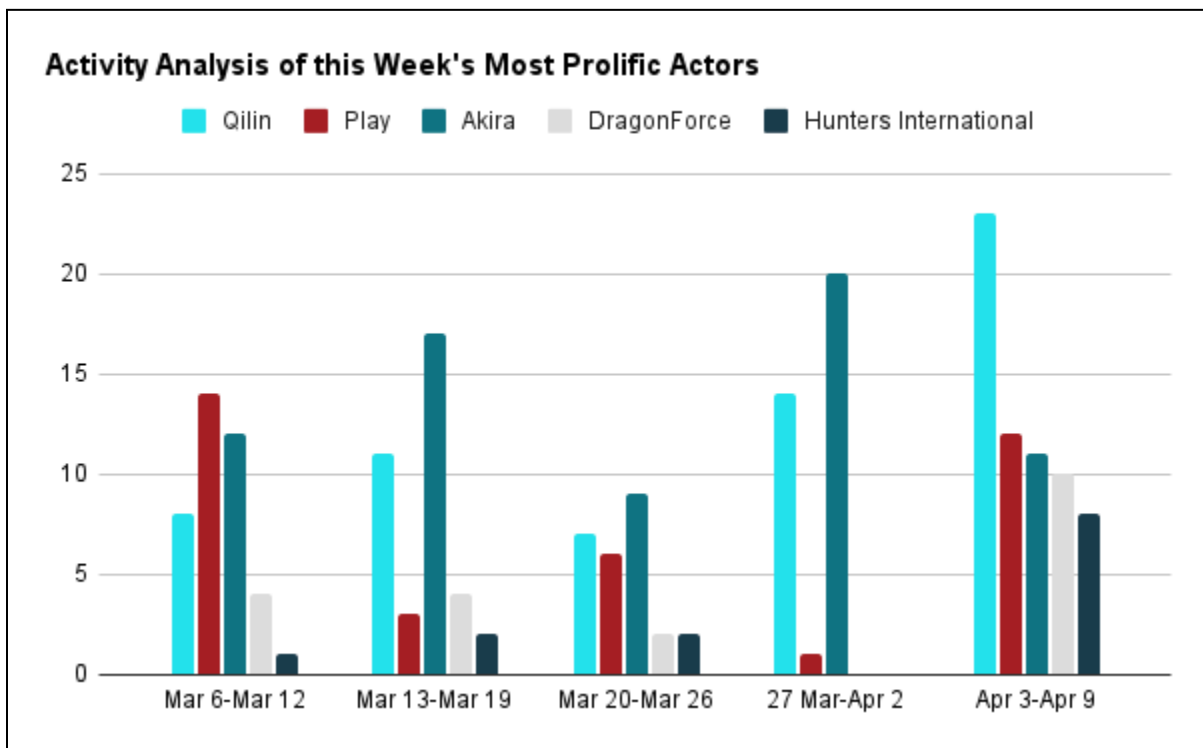


Ransomware in Focus: Actors' Activity, Targeted Industries, and Ongoing Campaigns



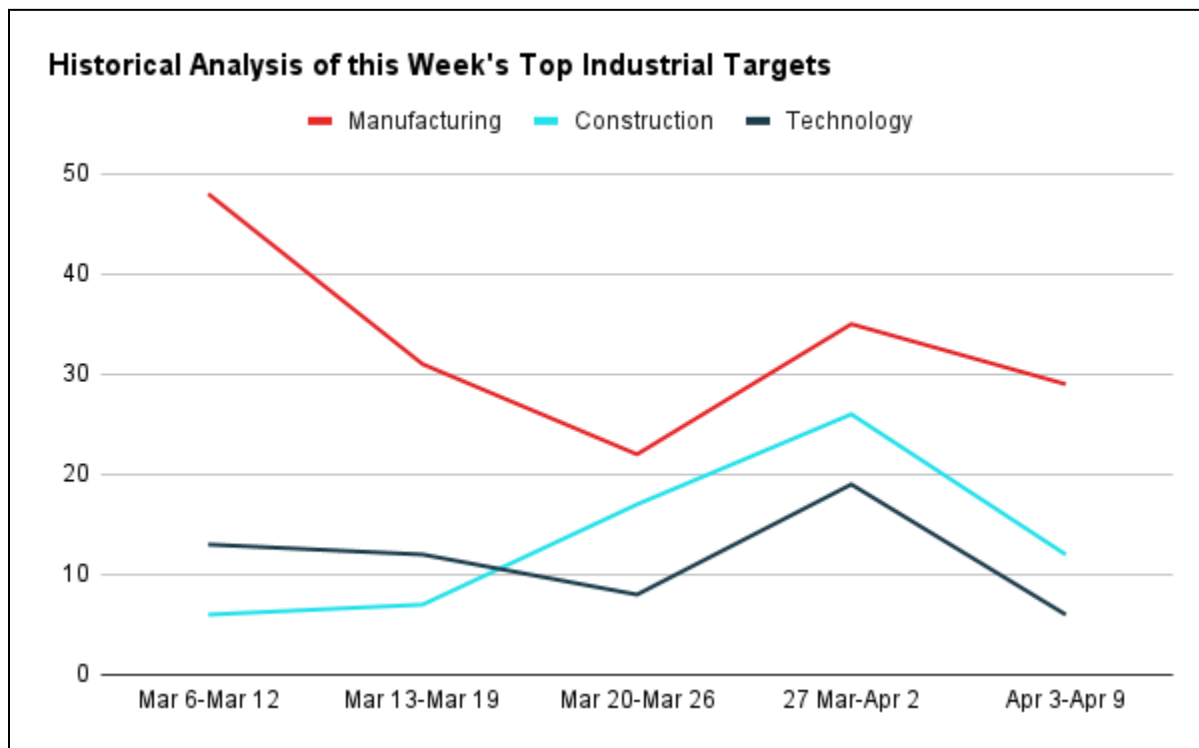
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Qilin, Akira, Play, DragonForce, and Hunters International were the most active ransomware groups. ZeroFox observed at least 130 ransomware victims disclosed, most of which were located in North America. Qilin accounted for the largest number of attacks.



Source: ZeroFox Internal Collections

Threat group activity trend: This week, Qilin, Akira, Play, DragonForce, and Hunters International were the most prominent groups. This graph shows their activities over the past five weeks. Akira and Qilin have been active throughout all five weeks, with at least 69 and 63 attacks, respectively.



Source: ZeroFox Internal Collections

Ransomware trends in industries: Over the past five weeks, ZeroFox has observed that the majority of ransomware victims are in the Manufacturing sector, followed by Construction. The Manufacturing sector, in particular, has consistently seen a high number of attacks, with at least 165 incidents recorded over the five weeks.

Recap of major ransomware events observed in the past week: The Medusa ransomware gang has [added NASCAR to its list of victims](#), demanding a USD 4 million ransom and threatening to release internal data if not paid. The group has also claimed McFarland Commercial Insurance Services, Bridgebank Ltd, and Pulse Urgent Care as its new targets. The Everest ransomware group has reportedly [taken down its leak site](#) after an unknown individual defaced it with a sarcastic message. The HellCat ransomware group has [launched a new wave of attacks](#) on four companies in the United States and Europe, exploiting stolen Jira credentials harvested by infostealer malware as part of its global campaign. ZeroFox observed the [Kill Security ransomware group announcing the global exploitation](#) of vulnerabilities within CrushFTP servers. U.S. sensor maker Sensata [experienced a ransomware attack](#) on April 6, disrupted operations, with the hackers encrypting devices and stealing data.



Notable Data Breaches Worldwide in the Past Week

Targeted Entity	<u>Bangchak Corporation</u>	<u>WK Kellogg Co</u>	<u>Emerson Electric</u>
Number of Firms/Victims Affected	7 million users' information	Yet to be determined	225,684 clients
Compromised Data and Infrastructure	Email addresses, phone numbers, and citizen IDs	Name and Social Security number	Name, email, phone, city, and budget for house purchases
Suspected Threat Actor	betway	CI0p	kekspurki
Country/Region	Thailand	United States	France
Industry	Energy	Manufacture	Technology
Possible Repercussions	Identity theft and social engineering attacks; spear phishing and business email compromise; SIM swapping and account takeovers; credential stuffing and brute force attacks; and blackmail	Phishing attacks, tax fraud, impersonation, employment scams, social engineering attacks, and financial fraud	Phishing and business email compromise, financial fraud, identity theft, social engineering attacks, whaling, impersonation, and ransomware

Three major breaches observed in the past week

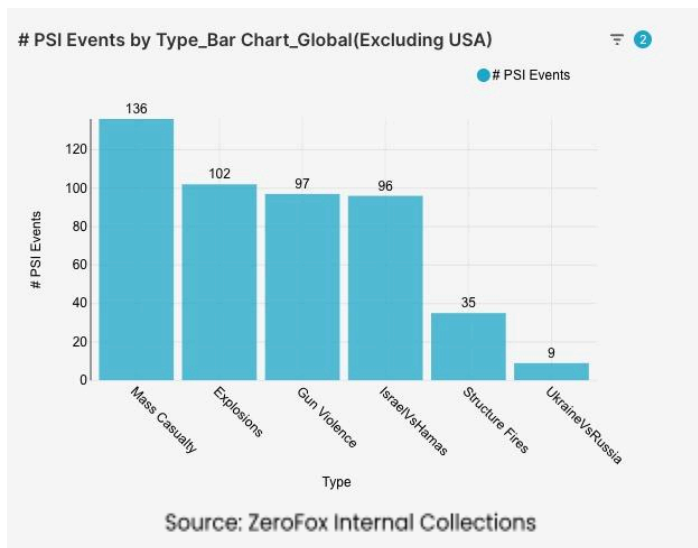
Other major data breaches observed in the past week: Hackers have targeted [Australia's major pension funds](#) in a series of coordinated attacks, stealing savings from some members of the largest fund and compromising over 20,000 accounts. The Port of Seattle is informing [approximately 90,000 individuals](#) about a data breach following a ransomware attack in August 2024 that compromised their personal information. A hacker named "Satanic" claims to have

[breached Magento via a third-party vulnerability](#), leaking customer relationship management (CRM) data of over 700,000 users, including emails, phone numbers, and company details. [The same hacker has also claimed responsibility](#) for a WooCommerce data breach through a third-party service, selling data on more than 4.4 million users and clients linked to various major organizations.

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

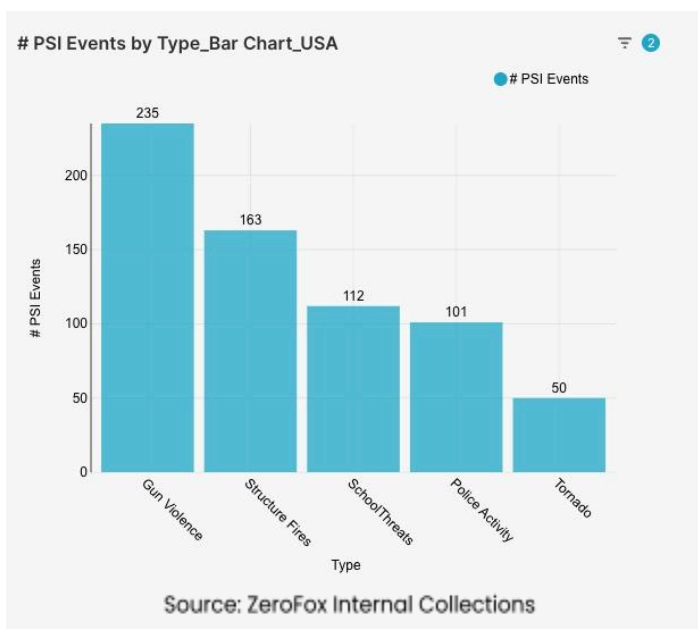


What happened: Excluding the United States, there was a 25 percent decrease in mass casualty events this week from the previous week, with the top contributing countries being Palestine, Syria, and Lebanon, in that order. Approximately 75 percent of these events were explosions, and the three aforementioned countries accounted for about 30 percent of all mass casualty alerts. General alerts related to the Israel-Hamas War (including protests, raids, and involvement in neighboring countries) increased by 52 percent from

the previous week. Events related to Russia's war in Ukraine decreased by 50 percent. The top three most-alerted subtypes were explosions, which saw a 14 percent decrease from the previous week; gun violence, which increased by 62 percent; and structure fires, which decreased by 22 percent. Global protest activity increased by 15 percent.

- What this means:** This week, while mass casualty events globally decreased, alerts related to the Israel-Hamas conflict saw a significant increase due to the [expansion](#) of operations across the Gaza Strip in Palestine since the end of the ceasefire. Israel now controls over 50 percent of the territory, which has doubled in size in recent weeks. These [ground invasions](#) could also have contributed to the increase in gun violence seen within the last week, as Palestine was the second-highest contributor to this number. Israel is also fighting over influence in Syria, which had the second-highest number of mass casualty events this week. On April 2, Israel [bombed](#) several military targets in the country as an affront against Turkey, who is also grappling for power in Syria. Israel's likely goal is to keep Syria and Lebanon [unstable](#) in order to remain the strongest regional power. Protest activity increased this week, with several countries across the globe taking part in the ["Hands Off"](#) demonstrations on April 5 opposing U.S. President Donald Trump's policies. Alongside the United States, protesters rallied in Frankfurt, Berlin, Paris, London, and Lisbon.

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 California and Texas, which together made up 21 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 16 percent, and the top contributing states were California and Pennsylvania. Structure fires decreased by 11 percent, and the top two states for this subtype were California and New York. Protest activity increased by 15 percent, and threats related to schools (excluding protests) increased by 26 percent.

- **What this means:** This week, U.S. protest activity increased by the same percentage as international protests (15 percent), likely due to the nationwide [“Hands Off”](#) protests on April 5 in which demonstrators rallied against President Trump’s policies on tariffs, immigration, and government downsizing. Another national protest is being planned for [April 19](#) in opposition to the Trump administration’s actions and policies. California was the top contributing state for all three leading subtypes this week (police activity, structure fires, and gun violence). One such instance involved a [mass shooting](#) on April 5 in which one person died and another four were injured in Los Angeles, CA. There was also [severe weather](#) in several states this week, with tornadoes and floods causing fatalities in Kentucky, Indiana, Tennessee, and Missouri. At least eight people have died, and many more were injured. Since the outbreak of severe weather began on April 2, there have been more than four dozen reported tornadoes from Arkansas to Ohio, with more flooding expected to come within the next week.

| 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%