



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

April 19, 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 17, 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 7	2
ZeroFox Intelligence Flash Report – Dark Web Discussion Centers on BreachForums Outage	2
ZeroFox Intelligence Flash Report – Residential Privacy Risks Amplified by High-Profile Incident	2
ZeroFox Intelligence Flash Report – Incident Report: British Steel Operational Disruption	3
 Cyber and Dark Web Intelligence Key Findings	5
BreachForums Down; New Forums Emerge	5
CISA Flags Threat from Exposed Credentials in Legacy Oracle Environment	6
Data Security Program Implements Export Control on U.S. Critical Data	6
 Exploit and Vulnerability Intelligence Key Findings	8
CVE-2025-24859	8
Fortinet Vulnerabilities	9
 Ransomware and Breach Intelligence Key Findings	11
Ransomware in Focus: Most Active Actors, Affected Regions, and Their Trends	11
Significant Global Data Breaches 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 Brief – Underground Economist: Volume 5, Issue 7](#)

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

[ZeroFox Intelligence Flash Report – Dark Web Discussion Centers on BreachForums Outage](#)

On April 15, 2025, ZeroFox observed that the popular deep web hacking forum BreachForums was no longer online, with the domain breachforums[.]st displaying an error code which remains as of the writing of this report. On the same day, the hacking collective “Dark Storm” posted to its Telegram channel seemingly claiming responsibility and providing a check-host URL which confirmed the forum’s outage. Conflicting information has also been circulating amongst threat actors, with many instead claiming that the Federal Bureau of Investigation (FBI) is behind BreachForums’ closure. ZeroFox observed discussions taking place in deep and dark web (DDW) forums and Telegram channels surrounding the alleged arrest of notorious threat actor “IntelBroker”, who is known for publishing prominent data leaks and previously fulfilling an administrator role within BreachForums. As of the writing of this report, it is unclear whether a law enforcement (LE) operation or a hacktivist group such as Dark Storm (who has not indicated any specific motive) is responsible for the BreachForums outage.

[ZeroFox Intelligence Flash Report – Residential Privacy Risks Amplified by High-Profile Incident](#)

An April 13, 2025, attack on the official residence of Pennsylvania Governor Josh Shapiro underscores the continued risk residential exposures pose to public figures and executives. While Governor Shapiro was targeted in the official state residence rather than a private residence, the governor and his family were home at the time, and the incident highlights broader concerns around publicly accessible address information and the physical security of family dwellings. Personal addresses and home details are increasingly accessible online through public records, real estate listings, mapping services, and data aggregator sites, increasing high-profile individuals’ risk of physical targeting. The suspect, identified as Cody A. Balmer, was arrested and charged with several felonies, including attempted homicide, terrorism, aggravated arson, and burglary.

ZeroFox Intelligence Flash Report – Incident Report: British Steel Operational Disruption

On April 12, 2025, the United Kingdom (UK) government took action to ensure continued operations at British Steel's Scunthorpe site—home to the UK's last remaining blast furnaces—due to a critical disruption in the supply of raw materials. This disruption arose after the site's Chinese parent company, Jingye Group, ceased procurement of essential raw materials and began selling existing supplies, leading to concerns that British Steel may be forced to cease operations. In response, the UK government enacted emergency legislation, the Steel Industry (Special Measures) Act 2025, granting it emergency powers to intervene in critical steel manufacturing operations. Under this legislation, UK ministers assumed operational control of key steel assets and the Scunthorpe site. To sustain operations at British Steel's Scunthorpe site, the UK government has secured emergency shipments of the needed raw materials, cooking coal and iron ore, from the United States and Australia. This incident highlights the risks of foreign ownership in critical national infrastructure, particularly where assets vital to national security are controlled by foreign organizations with potential links to adversarial states.

| Cyber and Dark Web Intelligence |

| Cyber and Dark Web Intelligence Key Findings



BreachForums Down; New Forums Emerge

What we know:

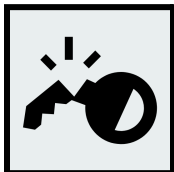
- ZeroFox has observed that dark web forum [BreachForums has become inaccessible](#). As of reporting, its clearnet and onion sites are displaying a "502 Bad Gateway" error.
- ZeroFox also observed the creation and advertisement of numerous domains appearing to masquerade as a BreachForums replacement, such as breachforums[.]cc.

Background:

- BreachForums has been offline since April 15, 2025, prompting a spike in underground activity with new forums and Telegram channels emerging.
- Suspicious domains like "breachforums[.]im" appeared, initially soliciting crypto payments for access before switching to a domain-for-sale message.
- Speculation is growing surrounding the possible arrest of BreachForums' former administrator "IntelBroker", especially after their move to cracked[.]io, which was recently seized in an international law enforcement operation involving the Federal Bureau of Investigation (FBI).
- A document allegedly leaked on a Russian-language dark web forum claims BreachForums has been an FBI honeypot since March 2025 under the classified operation "Spectral Tango."

What is next:

- It is likely that the forum is now under FBI control and has been taken down. However, the marketplace is very likely to resurface with a new domain, as it did after a law enforcement takedown in May 2024.
- The sudden unavailability of BreachForums has likely disrupted a key hub for cybercriminal activity, leaving some of its user base to rely on other illegal forums to begin their criminal activities anew.
- The appearance of new forums and domains could result in scams, impersonation, and other fraud.



CISA Flags Threat from Exposed Credentials in Legacy Oracle Environment

What we know:

- The Cybersecurity and Infrastructure Security Agency (CISA) is warning of possible unauthorized access to a legacy Oracle cloud environment. The exposure of credential material threatens organizations and individuals if credentials are reused or embedded across systems.

Background:

- Recently, Oracle [released over 300 security patches](#) in its second critical patch update of 2025. Patching existing vulnerabilities and implementing cybersecurity best practices are essential to mitigate this risk.

Analyst note:

- Threat actors could exploit exposed reused credentials to move laterally, escalate privileges, or maintain persistent access—leading to data theft, service disruption, and further supply chain attacks.



Data Security Program Implements Export Control on U.S. Critical Data

What we know:

- The U.S. government has implemented the Data Security Program to safeguard the data of government entities and personally identifiable information (PII) of U.S. persons from foreign adversaries like China, Russia, and Iran.

Background:

- U.S. persons and businesses are expected to comply with the program, especially when dealing with information-sharing with individuals and entities directly related to foreign governments or working under their influence or jurisdiction.

Analyst note:

- Data aggregators, entities working with the U.S. government, and social media companies are likely to be affected by the program. The Data Security Program is likely to create a trail or record of the sale or sharing of information related to the U.S. government and persons, enabling greater accountability in cases of misuse of information.

| **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. CISA has released [nine Industrial Control Systems \(ICS\) advisories](#) and added [one vulnerability to its Known Exploited Vulnerability \(KEV\) catalog](#). NVIDIA's patch for a [critical container escape flaw](#), CVE-2024-0132, was incomplete, leaving systems still vulnerable to attacks. The vulnerability (CVE-2025-23391) in [SUSE Rancher](#)—a Kubernetes management platform—enables a Restricted Administrator to reset the passwords of the administrators. [Delta Electronics COMMGR v1 and v2](#) uses insufficiently randomized values to generate session IDs (CWE-338), enabling attackers to brute force IDs and execute arbitrary code. Threat actors have reportedly exploited [CVE-2025-30406](#) to target seven organizations, while over 100 endpoints have registered unusual activity. The flaw in [Erlang/OTP before versions 27.3.3, 26.2.5.11, and 25.3.2.20](#) allows unauthenticated remote code execution (RCE) via its SSH server. Apple has released [security updates for iOS, iPadOS, macOS Sequoia, tvOS, and visionOS](#) to address two vulnerabilities (CVE-2025-31200 and CVE-2025-31201) that are being actively exploited in the wild.



CRITICAL

CVE-2025-24859

What happened: A critical security vulnerability has been revealed in Apache Roller open-source, Java-based blogging server software. It could enable malicious actors to maintain unauthorized persistent access to the system, even after users change their password.

- **What this means:** This vulnerability enables threat actors to maintain persistent, unauthorized access to the system, even after passwords are changed. This could lead to data theft, unauthorized content manipulation, or the use of the compromised server to launch further attacks.
- **Affected products:**
 - All versions of Apache Roller up to and including 6.1.4

**CRITICAL****Fortinet Vulnerabilities**

What happened: Fortinet has issued an [alert](#) warning that a threat actor is actively exploiting known vulnerabilities (CVE-2024-21762, CVE-2023-27997, and CVE-2022-42475) in FortiGate devices. The attacker is using these vulnerabilities to deploy a malicious file that grants unauthorized, read-only access to sensitive configuration data.

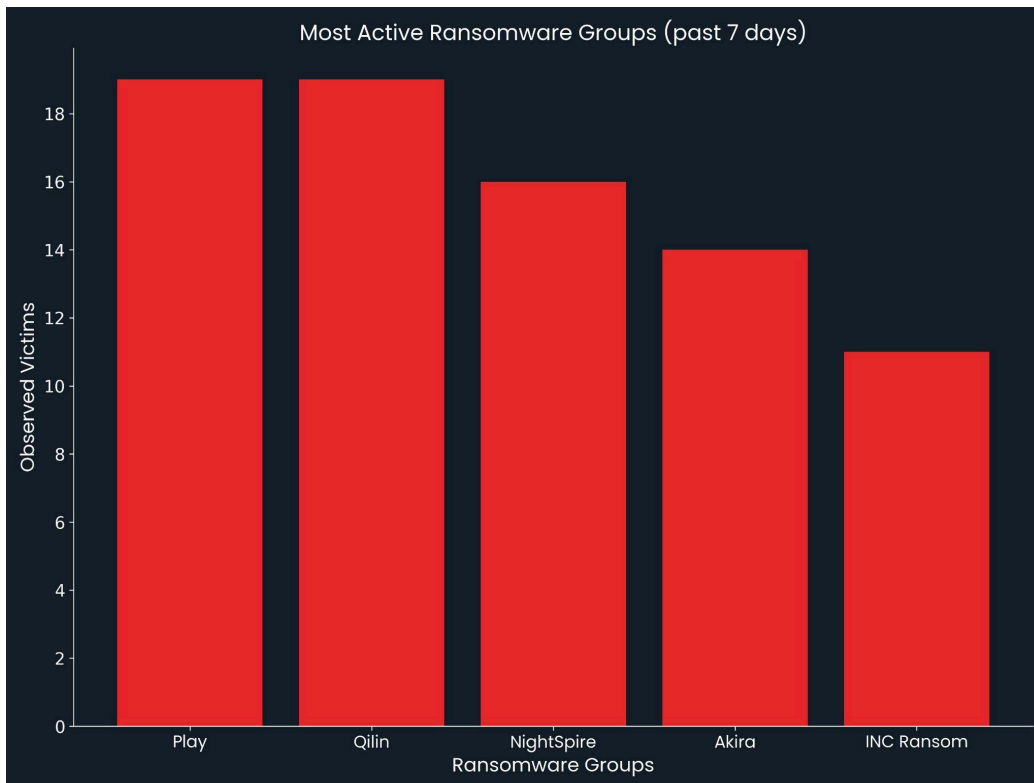
- **What this means:** This flaw allows attackers to access sensitive FortiGate configuration data, potentially exposing network infrastructure details. This unauthorized access can lead to further targeted attacks, lateral movement within networks, and long-term persistence by threat actors. Users are advised to update to the patched FortiOS versions (7.6.2, 7.4.7, 7.2.11, 7.0.17, and 6.4.16), reset credentials, and disable SSL-VPN.
- **Affected products:**
 - The affected products have been listed in this [update](#).

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

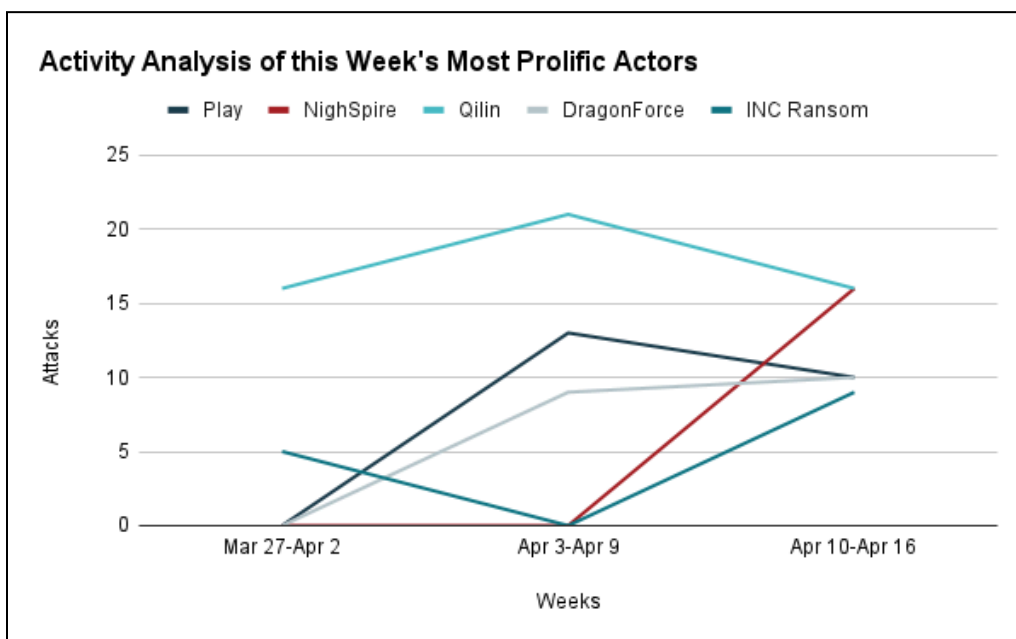


Ransomware in Focus: Most Active Actors, Affected Regions, and Their Trends



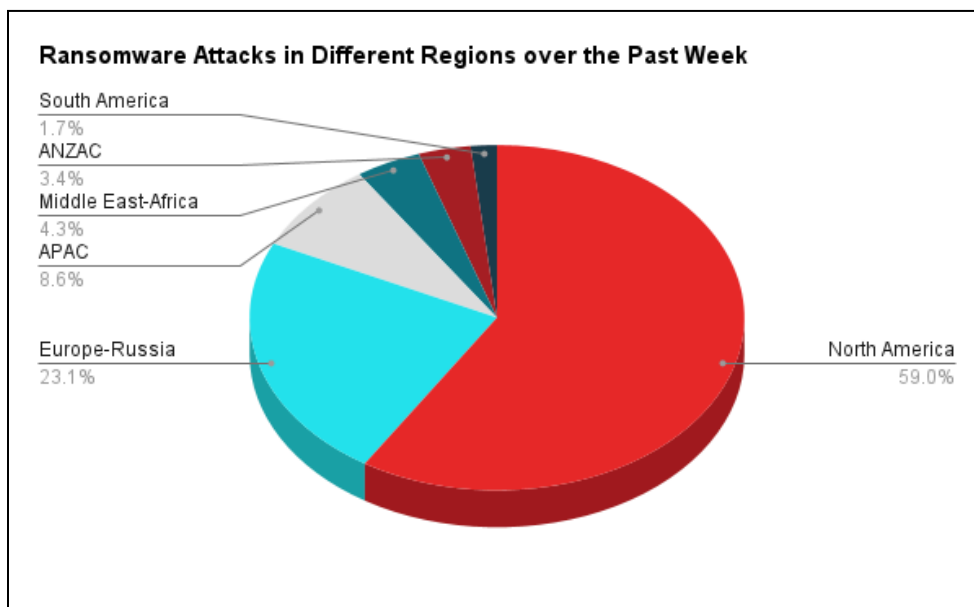
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Qilin, Play, NightSpire, Akira, and INC Ransom were the most active ransomware groups. ZeroFox observed at least 117 ransomware victims disclosed, most of which were located in North America. Play and Qilin accounted for the largest number of attacks.



Source: ZeroFox Internal Collections

Threat group activity trend: This week Play, NightSpire, Qilin, DragonForce, and INC Ransom were the most prominent groups. This graph shows their activities over the past three weeks. Qilin and Play have been the most active, with at least 53 and 23 attacks, respectively.



Source: ZeroFox Internal Collections

Regional ransomware trends: In the past seven days, ZeroFox has observed that North America was the most targeted region by ransomware attacks, followed by Europe–Russia.



Significant Global Data Breaches in the Past Week

Targeted Entity	<u>Landmark Admin</u>	<u>Hertz</u>	<u>Moroccan National Social Security Fund (CNSS)</u>
Number of Firms/Victims Affected	1,613,773	At least 3,409 customers	2 million individuals' information
Compromised Data and Infrastructure	Customers' first and last names, physical addresses, Social Security numbers, tax identification numbers, driver's license numbers and state-issued identification cards, passport numbers, financial account numbers, medical information, dates of birth, health insurance policy numbers, and life and annuity policy information	Customers' names, contact information, dates of birth, credit card information, driver's license information, workers' compensation claims, Social Security numbers, passport information, Medicare or Medicaid ID (linked to workers' compensation claims), or injury-related information	Names, government identification numbers, phone numbers, email addresses, and bank account details
Suspected Threat Actor	Yet to be determined	Cl0p	Reportedly, JabaROOT
Country/Region	United States	United States	Morocco
Industry	Insurance	Customer Service	Government
Possible Repercussions	Phishing, social engineering and impersonation attacks, tax fraud	Credit card fraud, phishing, social engineering, and impersonation attacks	Phishing and social engineering attacks

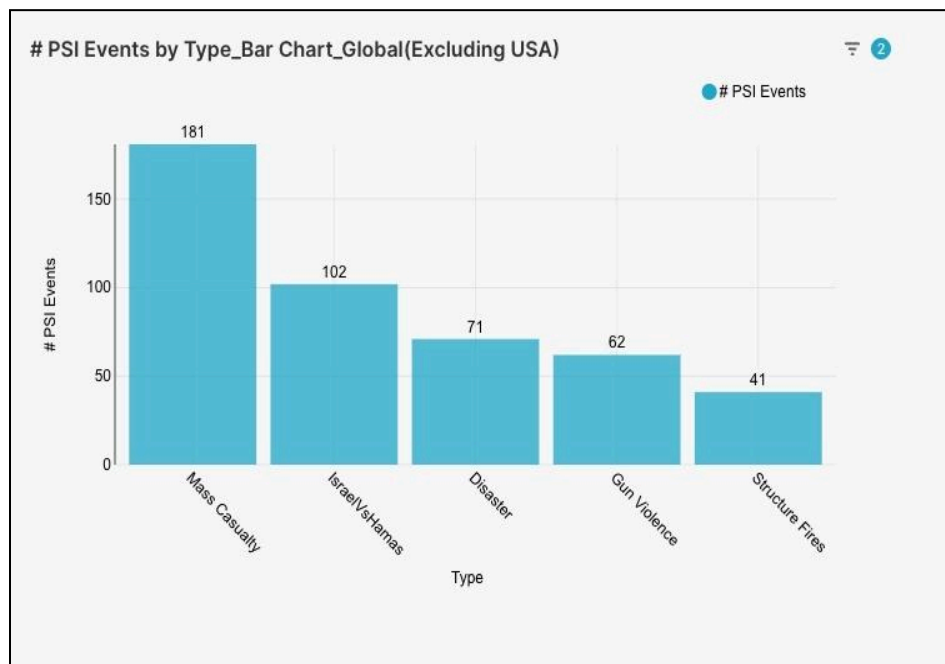
Three major breaches observed in the past week

Other major data breaches observed in the past week: Business services company and U.S. government contractor [Conduent confirmed data theft](#) in a January 2025 cyberattack that included client data. E-commerce company [WooCommerce has denied](#) any direct data breach by threat actor “Satanic,” saying the data likely originated from third-party aggregators. Misconfiguration in a staff management database by United Kingdom (UK) software firm Logezy has [exposed eight million](#) UK healthcare worker records, including financial data. A hacker reportedly phished an employee of [private jet company NetJets](#) to steal information on some of its clients, who were later informed of the breach by the company. CISA is warning of possible unauthorized access to a [legacy Oracle cloud environment](#) that is likely to lead to exposure of credentials. Australian institution Western Sydney University (WSU) [disclosed a compromise of its single sign-on](#) (SSO), potentially exposing the PII of about 10,000 current and former students. The infamous message board [4chan was allegedly hacked](#) and internal data has been leaked.

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

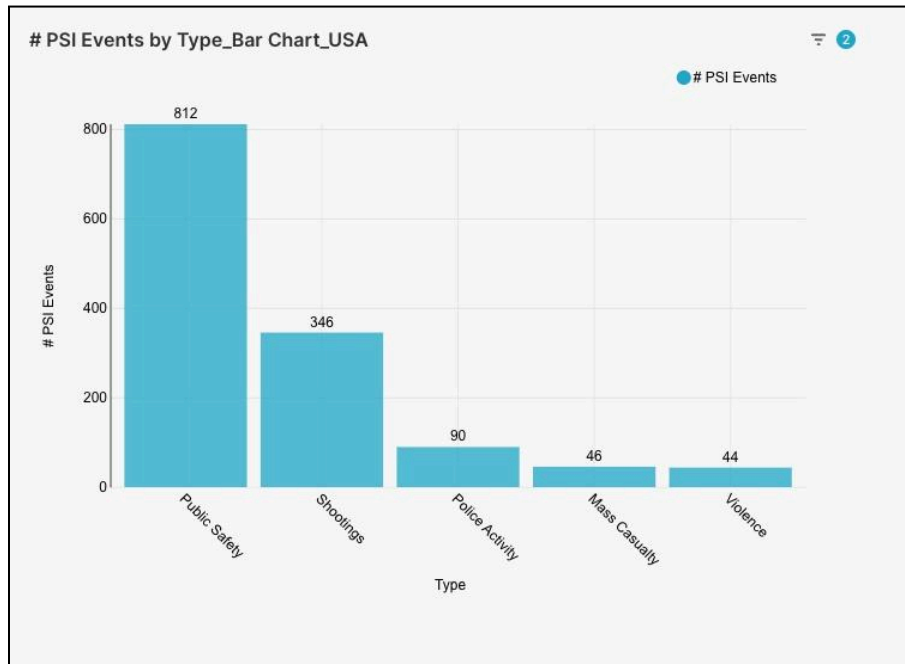
Physical Security Intelligence: Global



Source: ZeroFox Internal Collections

What happened: In the past week, ZeroFox has observed that mass casualty events were the most alerted sub-type globally, followed by the Israel-Hamas war. U.S. officials condemned the [Russian double-tap strike on Ukraine](#) on April 13, 2025, which killed at least 35 people and wounded 117 others. It also sparked discussions around the necessity of hastening the ceasefire. A [sandstorm in Iraq](#) has caused at least 700 suffocation cases, while hundreds reported experiencing breathing difficulties. Many regions are experiencing power outages, and flights have been restricted to certain areas. In India's eastern state of West Bengal, [violent demonstrations erupted](#) following changes made to the Waqf laws that govern Muslim charitable properties. This follows last week's violence in the Muslim-dominated district of Murshidabad, where three people were killed and 200 were arrested. [GPS-spoofing attacks](#) have been reported recently in [Myanmar](#) and Southeast Asia's airspace, impacting air and sea transportation. On April 16, 2025, [Latvia's parliament voted](#) to exit the Ottawa Convention to better-defend against increased military threats from Russia.

Physical Security Intelligence: United States



Source: ZeroFox Internal Collections

What happened: In the past week, the top three most-alerted incident subtypes were public safety, shootings, and police activity. California reported the highest number of public safety alerts, at 102, followed by shootings. The top two states that had the most shooting alerts were New York and California. Meanwhile, an [individual has been arrested and charged](#) for sending death threats via text messages to Director of National Intelligence (DNI) Tulsi Gabbard and her family. Measles cases are [reportedly being underreported](#) in the United States, as public health officials struggle to secure the resources needed to respond to a rapidly growing outbreak in the Southwest. A man dressed in tactical gear and wearing a gas mask reportedly [forced his way into a courthouse in the Boston area](#) early this week, allegedly pepper-spraying and physically assaulting multiple individuals before being taken into custody. President Donald Trump has [granted the U.S. military authority](#) over federal lands along the southern border as part of efforts to advance his immigration policies.

| 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%