



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

May 3, 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 May 1, 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 8	2
ZeroFox Intelligence Flash Report – India-Pakistan Tensions Likely to Escalate	2
ZeroFox Intelligence Flash Report – Australia Elections	2
ZeroFox Intelligence Flash Report – Marks & Spencer Cyber Incident	3
ZeroFox Intelligence Flash Report – Hacktivists Claim Responsibility for Recent Power Outages	3
ZeroFox Intelligence May 2025 Geopolitical Assessment	3
Romania's Presidential Elections Crisis	4
 Cyber and Dark Web Intelligence Key Findings	6
International Operation Dismantles JokerOTP Phishing Tool; Two Arrested	6
ToyMaker Powers Double Extortion Attacks with LAGTOY Malware	6
Original BreachForums Domain Releases Update on Forum's Fate	7
 Exploit and Vulnerability Intelligence Key Findings	9
CVE-2025-31324	9
CVE-2025-34028	10
 Ransomware and Breach Intelligence Key Findings	12
Ransomware Roundup: Most Active Actors, Affected Industries, Regions, and More	12
Notable Data Breaches in the Past Seven Days	15
 Physical and Geopolitical Intelligence Key Findings	18
Physical Security Intelligence: Global	18
Physical Security Intelligence: United States	19
 Appendix A: Traffic Light Protocol for Information Dissemination	20
 Appendix B: ZeroFox Intelligence Probability Scale	21

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Brief – Underground Economist: Volume 5, Issue 8

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

ZeroFox Intelligence Flash Report – India-Pakistan Tensions Likely to Escalate

A military escalation between India and Pakistan is likely in the coming weeks after gunmen likely affiliated with a Pakistani-based terror group targeted a tourism hotspot in Kashmir. Indian Prime Minister Narendra Modi has exerted a large amount of political capital since 2019 to ensure the public Kashmir was safe, while also establishing a military precedent that Pakistan can be held responsible for jihadist attacks in the region. Hacktivist groups on both sides of the conflict have begun targeting public and private entities in India and Pakistan, while social media users have been sharing incendiary posts that will likely worsen tensions and contribute to public pressure on both governments to take retaliatory actions.

ZeroFox Intelligence Flash Report – Australia Elections

Australia holds general elections on May 3, 2025, with final polls reporting a small lead for Anthony Albanese's incumbent Labor party over Peter Dutton's opposition Coalition. The policies of U.S. President Donald Trump have likely impacted voter candidate preferences in the Australian election, and there is evidence that Chinese-backed cyber threat actors have attempted to influence the election in support of current Prime Minister Anthony Albanese. The biggest cyber risks to the election come from financially motivated deep and dark web (DDW) actors selling compromised account credentials linked to voters and online election infrastructure.

ZeroFox Intelligence Flash Report – Marks & Spencer Cyber Incident

On April 22, 2025, Marks & Spencer (M&S), one of the United Kingdom's leading retailers, publicly confirmed that it was managing a cyber incident. While M&S has not officially stated a cyberattack has occurred, the characteristics observed in this incident are consistent with ransomware attacks. Investigations remain ongoing, with M&S confirming it has called in the UK's National Cyber Security Centre to assist in containing and resolving the incident. M&S has also reported the incident to the Information Commissioners Officer (ICO). The M&S cyber incident highlights the growing cybersecurity risks faced by the UK retail sector. Disruption to services critical to customer experience can have an immediate impact on reputation and consumer trust.

ZeroFox Intelligence Flash Report – Hacktivists Claim Responsibility for Recent Power Outages

On April 28, 2025, hacktivist collective "Dark Storm" posted on the social media platform X (formerly Twitter) claiming that—in conjunction with fellow hacktivist group "NoName057"—it was responsible for a recent power outage that affected Spain, Portugal, and parts of Southern France. Several subsequent posts have been observed within both Dark Storm's Telegram channel and X account referencing the outages and claiming additional attacks targeting the infrastructure of European nations. As of this writing, the Spanish government is continuing to investigate the cause of these outages and has publicly denied they are the result of a cyberattack. While the exact cause of the power outage is currently unclear, it is unlikely that it was caused by a Dark Storm-led distributed denial-of-service (DDoS) attack, as the group very likely lacks the capabilities to conduct such an attack.

ZeroFox Intelligence May 2025 Geopolitical Assessment

While Russia has escalated its war in Ukraine, and U.S. efforts at a diplomatic solution largely failed to gain traction, the contours of an agreement are visible. A military escalation between India and Pakistan is likely in the coming weeks after gunmen likely affiliated with a * Pakistani-based terror group targeted a tourism hotspot in Kashmir. U.S. tariff policy is very likely already causing key supply chain disruptions, and the next major deadline is July 8, 2025, when the 90-day pause ends. Several Asian and European nations are holding elections in May 2025 wherein the primary issues are trade relations with the United States and China or Russia's war in Ukraine.

Romania's Presidential Elections Crisis

Romania's 2024 presidential election was annulled after evidence of Russian hybrid interference came to light, exposing vulnerabilities in the country's democratic and cyber defenses. As Romania prepares for a re-run election on May 4, 2025, two distinct political strategies have emerged: the country will either reaffirm its Euro-Atlantic commitments by electing pro-Western candidates or weaken NATO-EU cohesion by voting in nationalist and sovereigntist leaders. The outcome will have immediate consequences for Black Sea security, European stability, and Russia's influence in Eastern Europe.

Cyber and Dark Web Intelligence

| Cyber and Dark Web Intelligence Key Findings



International Operation Dismantles JokerOTP Phishing Tool; Two Arrested

What we know:

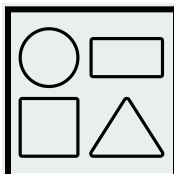
- An international operation dismantling JokerOTP, a phishing tool used to intercept two-factor authentication (2FA) codes, resulted in two arrests.
- The tool enabled cybercriminals to steal over GBP 7.5 million (approx. USD 9 million).
- The criminals face several charges, including money laundering, blackmail, and more.

Background:

- The arrests followed a three-year investigation led by Cleveland Police's Cyber Crime Unit.
- JokerOTP was used in over 28,000 attacks across 13 countries, targeting victims via phone scams.

What is next:

- Fraudsters used JokerOTP to impersonate trusted organizations and trick victims into revealing 2FA codes, which gave them access to accounts—likely leading to financial loss, identity theft, and more targeted cyberattacks.



ToyMaker Powers Double Extortion Attacks with LAGTOY Malware

What we know:

- Initial access broker "ToyMaker" has been reportedly compromising systems using custom malware called LAGTOY (aka HOLERUN) and selling network access to ransomware groups like CACTUS for double extortion attacks.

Background:

- LAGTOY has been linked to the threat group UNC961 (aka Gold Melody/Prophet Spider) and exploits known internet-facing vulnerabilities. The malware is deployed soon after reconnaissance and credential theft.

Analyst note:

- LAGTOY enables ransomware groups to rapidly gain access to vulnerable networks, facilitating the deployment of destructive attacks. Victims are likely to face operational disruption, financial loss, and data theft.



Original BreachForums Domain Releases Update on Forum's Fate

What we know:

- On April 28, 2025, ZeroFox observed an admin message update on the original BreachForums domain breachforums[.]st claiming that the infrastructure had been shut down due to the presence of a MyBB zero-day exploit.

Background:

- The admin assured users that the domain was not compromised and that no BreachForums team members had been arrested. Currently, a re-write of the forum's backend is allegedly underway. After the domain's shut down, speculations were rife that it was taken down by law enforcement.

Analyst note:

- The admin message on the domain is likely legitimate. Numerous other clone domains of BreachForums are very likely to be scam sites.

| **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 28](#), [April 29](#), and [May 1, 2025](#). CISA also released a total of 10 industrial control system (ICS) advisories on [April 24](#) and [April 29, 2025](#). Meanwhile, two newly disclosed Craft CMS critical vulnerabilities, CVE-2024-58136 and CVE-2025-32432 (patched in certain versions), have been observed being [actively exploited by threat actors in zero-day attacks](#). Researchers have disclosed [23 vulnerabilities in Apple's AirPlay protocol and software development kits \(SDKs\)](#), enabling zero-click and wormable remote code execution that affects both Apple and third-party devices. [IPW Systems' Metazo versions up to 8.1.3 are vulnerable](#) to unauthenticated remote code execution due to a flaw in smartyValidator[.]php enabling unauthorized control over the server, exfiltration of data, and more. [A vulnerability in Siemens' TeleControl Server Basic system \(CVE-2025-27495\)](#) enables SQL injection leading to remote code execution that enables network access permissions and denial-of-service conditions.



CRITICAL

CVE-2025-31324

What happened: This is a [missing authentication and authorization vulnerability](#) in SAP NetWeaver Visual Composer's development server part, which is used to design business tools without writing code. The bug enables remote exploitation using standard web communication methods (HTTP/HTTPS) without the need for an account to carry out the intrusion.

- **What this means:** The bug likely enables unauthorized persons to upload dangerous executable files to the target system. It also likely results in full system takeover due to lacking checks to verify if a user has the required permissions.
- **Affected products:**
 - VCFRAMEWORK 7.50

**CRITICAL****CVE-2025-34028**

What happened: A [vulnerability in Commvault Command Center enables](#) arbitrary code execution on affected systems, leading to complete compromise of the Command Center environment. The bug has been patched in versions 11.38.20 and 11.38.25.

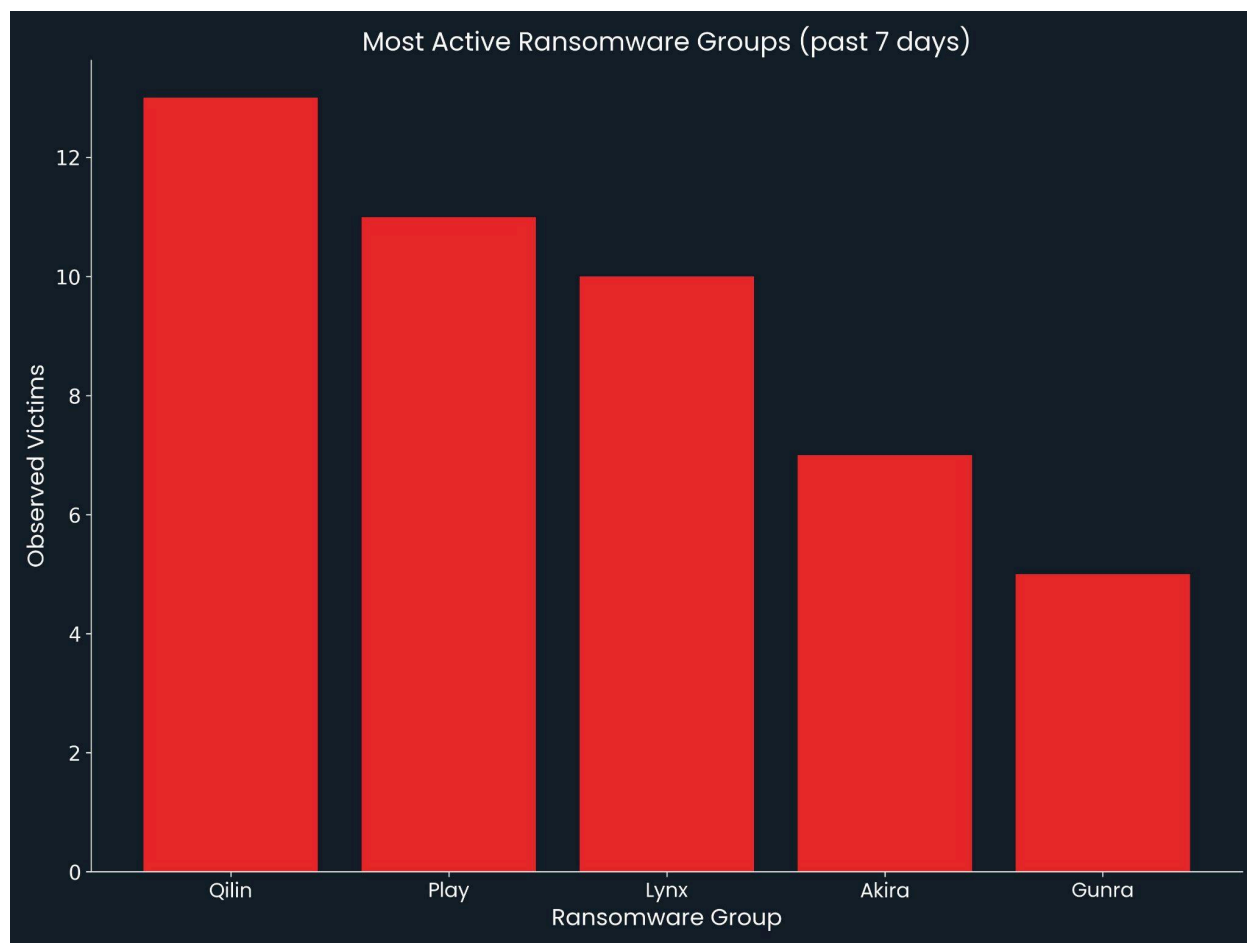
- **What this means:** The Information Technology (IT) industry and IT departments within other organizations are likely to be the most affected by this vulnerability, as Commvault Command Center systems are used for data protection and backups.
- **Affected products:**
 - Innovation Release versions from 11.38.0 through 11.38.19

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

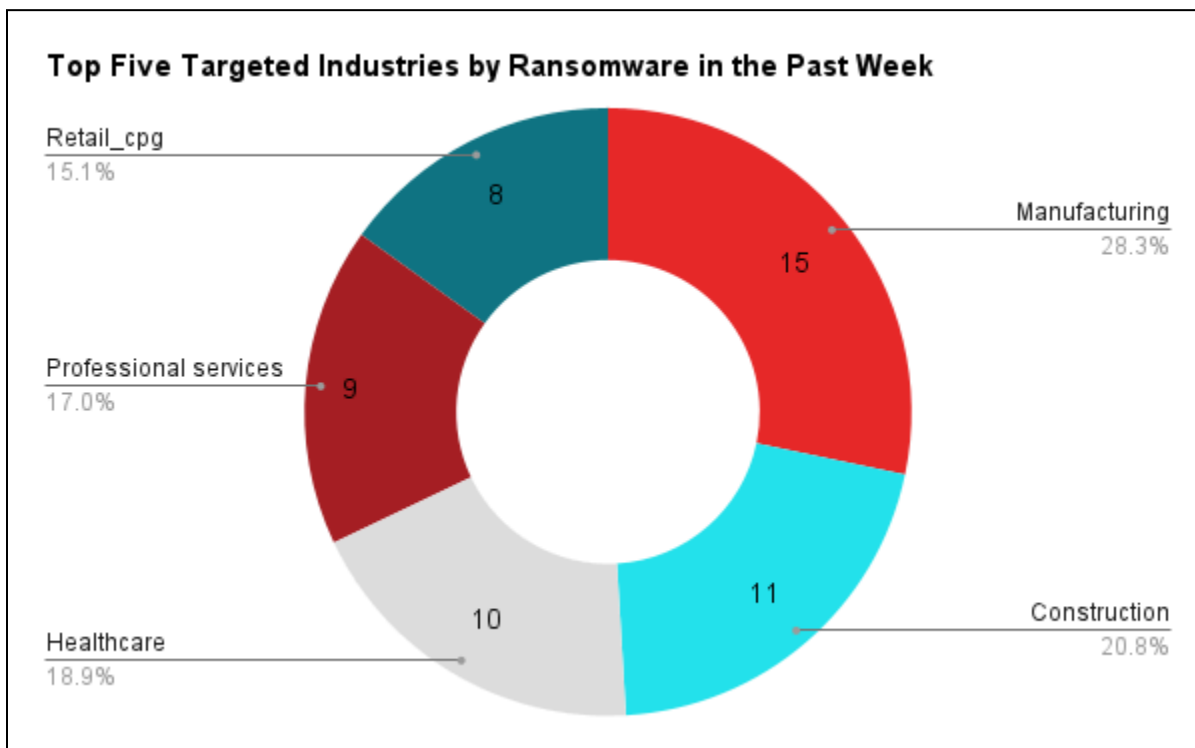


Ransomware Roundup: Most Active Actors, Affected Industries, Regions, and More



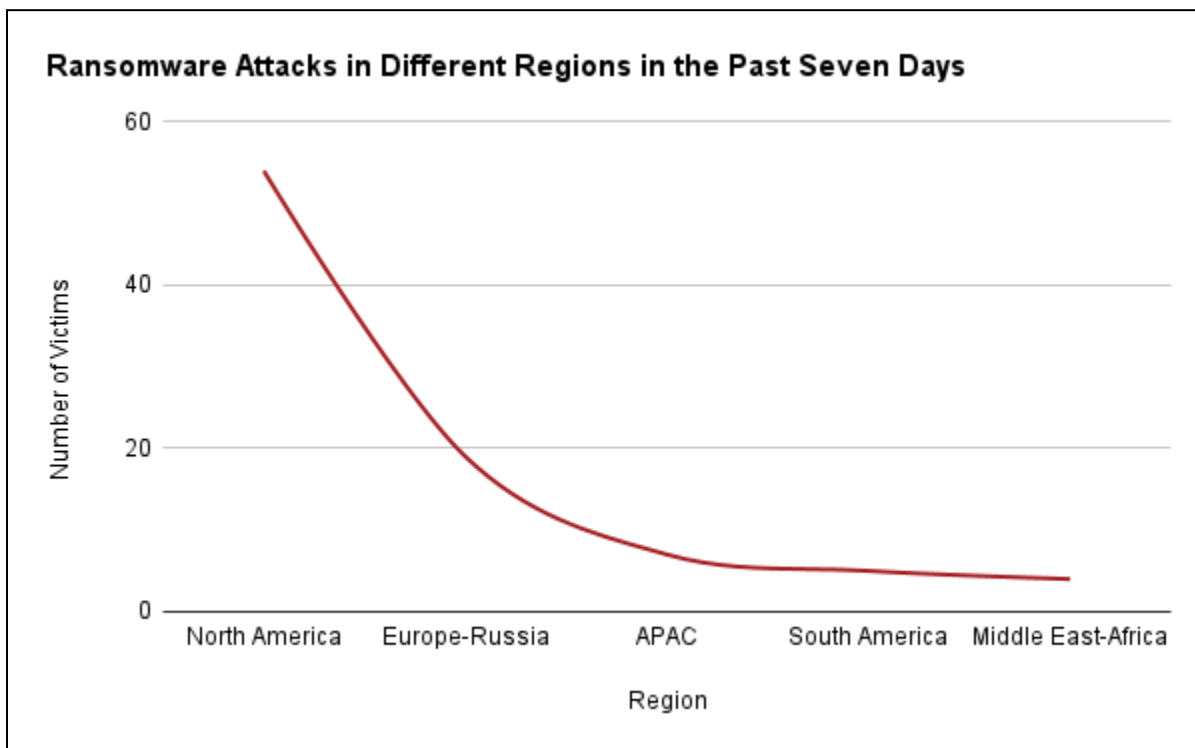
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Qilin, Play, Lynx, Akira, and Gunra were the most active ransomware groups. ZeroFox observed at least 46 ransomware victims disclosed, most of which are located in North America. Qilin and Play accounted for the largest number of attacks.



Source: ZeroFox Internal Collections

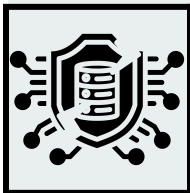
Industry ransomware trend: In the past week, manufacturing, construction, healthcare, professional services, and retail were the most targeted industries by ransomware attacks. The graph above shows the number of ransomware attacks suffered by the industries. The Manufacturing and Construction industries were the most targeted, with 15 and 11 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.

Recap of major ransomware events observed in the past week: Ransomware-as-a-service (RaaS) group [Qilin's recent activity and disclosures on its leak site suggest](#) that cybercriminals affiliated with RansomHub have likely migrated to the Russian-speaking collective (Qilin). ZeroFox has observed that the [Everest ransomware group has re-emerged](#), after being previously affected by a web defacement incident. A Ukrainian citizen has been extradited from Spain to the United States to face charges related to [allegedly carrying out Nefilim ransomware attacks targeting various companies](#). ZeroFox has observed an [announcement regarding the reorganization](#) of the ransomware landscape, wherein the DragonForce ransomware group is establishing a cartel-like structure that permits other RaaS operations to affiliate with them. Hitachi Vantara, a subsidiary of the Japanese multinational conglomerate Hitachi, [had to take its servers offline](#) in response to a ransomware attack linked to the Akira strain. Ongoing outages at British retail giant Marks & Spencer are reportedly the result of a ransomware attack, believed to be [carried out by threat group "Scattered Spider,"](#) according to multiple sources.



Notable Data Breaches in the Past Seven Days

Targeted Entity	<u>Ascension</u>	<u>SK Telecom</u>	<u>VeriSource</u>
Number of Victims/Amount of Data Stolen	Yet to be determined	Yet to be determined	4 million
Compromised Data and Infrastructure	Personal information, including name, address, phone number(s), email address, date of birth, race, gender, Social Security number (SSN), and health information	Universal Subscriber Identity Module (USIM) data, including International Mobile Subscriber Identity (IMSI), Mobile Station ISDN Number (MSISDN), authentication keys, network usage data, and SMS or contacts if stored on the SIM	Personal information, including employee's full name, address, date of birth, gender, and SSN.
Suspected Threat Actor	Yet to be determined	Yet to be determined	Yet to be determined
Country/Region	United States	South Korea	United States
Industry	Healthcare	Communication	Professional services
Possible Repercussions	Identity theft, phishing, social engineering attacks, financial fraud, account takeover attacks, blackmail, extortion, and ransomware	SIM cloning, SIM swap attacks, interception of calls and SMS, location tracking, surveillance, phishing, SMS spoofing, fraud, and espionage	Identity theft, phishing and social engineering attacks, credential stuffing, accounts takeover, and fraud

Three major breaches observed in the past week

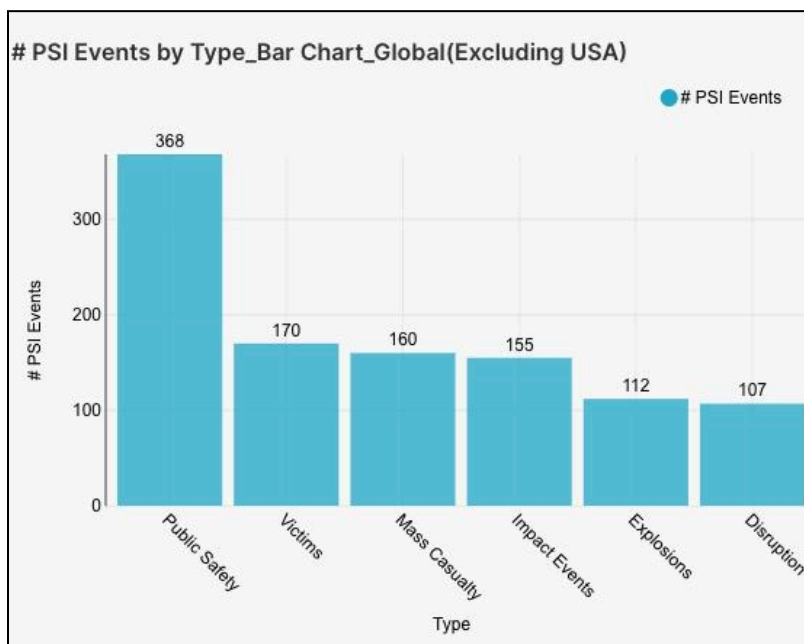
Other major data breaches observed in the past week: British supermarket chain [Co-op shut down certain sections of its IT systems](#) after detecting an attempted breach of its network, leading to disruptions in back-office operations and call center services. Commvault (provider of data

protection solutions) has reported that, although [a nation-state threat actor breached its Azure environment](#), no customer backup data was accessed during the incident. ZeroFox has observed untested threat actor "HuanEbashers" advertising the [sale of a data-breach package for an unnamed U.S.-based healthcare](#) company on RAMP. A misconfigured and unsecured database [belonging to TicketToCash exposed](#) the personal and partial financial information of 520,000 customers.

| Physical and Geopolitical Intelligence |

| Physical and Geopolitical Intelligence Key Findings

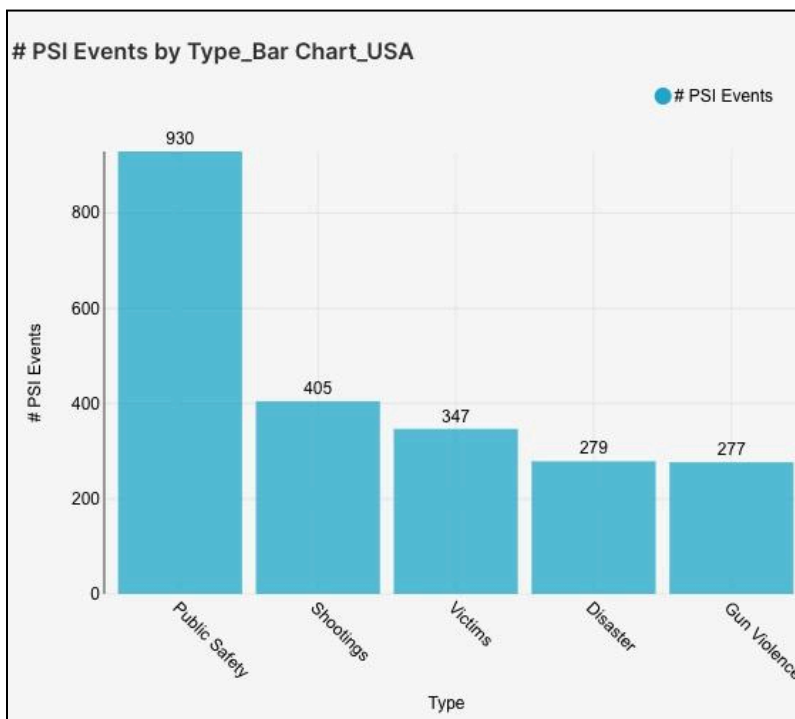
Physical Security Intelligence: Global



Source: ZeroFox Internal Collections

What happened: In the past week, ZeroFox observed at least 368 alerts related to public safety, followed by at least 170 victim alerts globally, barring the United States. [Wildfires broke out on the outskirts of Jerusalem](#) on April 30, forcing evacuation and prompting the closure of a major highway as Israel sought international assistance to help combat the blaze. [Pakistani troops reportedly continued unprovoked firing for the eighth consecutive night](#) along the border with India, prompting retaliation from the Indian Army. Poland announced it has applied to the [European Union \(EU\) for the "escape clause"](#) that would exempt it from increased defense spending. In Kenya's Nairobi, on the evening of April 30, 2025, motorcycle-borne [gunmen assassinated a lawmaker](#) while he was in his vehicle. A [massive blast was reported at Iran's Bandar Abbas port city](#) on April 26, 2025, killing at least 18 people and injuring over 500 others. In Vancouver, Canada, an [individual was arrested for ploughing their car into a crowd](#) during a street festival on April 26, 2025. China has claimed [sovereignty over a tiny reef](#) called Sandy Cay in the South China Sea in an escalation of dispute with the Philippines.

Physical Security Intelligence: United States



Source: ZeroFox Internal Collections

What happened: In the past week, ZeroFox observed at least 930 public safety alerts, followed by 405 shooting alerts, and at least 277 gun violence alerts in the United States. Meanwhile, on April 27, 2025, a [mass shooting at Elizabeth City State University](#) in North Carolina killed one person and injured six others. On the night of April 26, a [mass shooting at Myrtle Beach](#) in South Carolina led to one person's death and 11 injuries. On April 29, nine people were shot and five were killed in [Minneapolis during a mass shooting](#). On April 30, [two people were killed](#) after being swept in floodwaters as heavy rain struck Oklahoma and Texas. In Tennessee, [a single-engine plane crash](#) on April 26 killed three people on board.

| 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%