



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

May 10, 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 8, 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 – Series of Cyberattacks Target UK Retail Organizations	2
ZeroFox Intelligence Flash Report – Data Breach Exposes Operational LockBit Information	2
 Cyber and Dark Web Intelligence Key Findings	4
Unsophisticated Cyber Actors Targeting Operational Technology	4
Luna Moth Continues to Extort Legal and Financial Firms	5
U.S. Sanctions Myanmar Militia Involved in Cyber Scams	5
 Exploit and Vulnerability Intelligence Key Findings	7
CVE-2025-46337	7
CVE-2025-4104	8
 Ransomware and Breach Intelligence Key Findings	10
Ransomware in Focus: Major Groups and Regional Trends	10
Data Breaches Affecting Companies and Customers	12
 Physical and Geopolitical Intelligence Key Findings	14
Physical Security Intelligence: Global	14
Physical Security Intelligence: United States	15
 Appendix A: Traffic Light Protocol for Information Dissemination	16
 Appendix B: ZeroFox Intelligence Probability Scale	17

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Flash Report – Series of Cyberattacks Target UK Retail Organizations

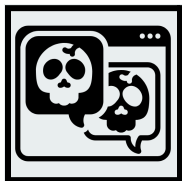
A series of prominent cyber incidents have targeted UK-based retail organizations in recent days, including Marks & Spencer (M&S) and The Co-operative Group (Co-op). DragonForce, a ransomware & digital extortion (R&DE) collective that operates as-a-service within deep and dark web (DDW) forums, has claimed responsibility for the attacks. As of the writing of this report, DragonForce's dark web [.]onion victim leak page is inaccessible, and it is unknown if any of the affected organizations have been named on the site. If DragonForce is responsible for these attacks and its extortion attempts are unsuccessful, there is a very likely chance that the collective will begin publishing stolen data to its leak site in the coming weeks.

ZeroFox Intelligence Flash Report – Data Breach Exposes Operational LockBit Information

On May 7, 2025, actor "Rey" posted on the social media platform X (formerly Twitter) claiming that digital infrastructure associated with the once-prominent ransomware-as-a-service (RaaS) collective LockBit had been breached. As of the writing of this report, several of LockBit's dark web [.]onion blog domains display the message "Don't do crime CRIME IS BAD xoxo from Prague", accompanied by a download link containing a MySQL data dump. Tables available within a MySQL download include information pertaining to ongoing LockBit operations, including victim negotiations, Bitcoin addresses, and malware build configurations. At the time of writing, it is unclear who is responsible for the breach, though an almost-identical message was posted on the [.]onion victim leak side of the ransomware collective Everest in April 2025. This incident will very likely exacerbate LockBit's ongoing efforts to re-establish operational continuity, maintain a steady attack tempo, and attract affiliates, following the collective's February 2024 disruption by law enforcement (LE) entities.

Cyber and Dark Web Intelligence

| Cyber and Dark Web Intelligence Key Findings



Unsophisticated Cyber Actors Targeting Operational Technology

What we know:

- The Cybersecurity and Infrastructure Security Agency (CISA) has warned of unsophisticated threat actors targeting Industrial Control Systems (ICS) and Operational Technology (OT) systems within U.S. critical infrastructure sectors.
- Systems in the energy and transportation sectors have been frequently targeted.
- These amateur threat actors are known to utilize basic and elementary intrusion techniques.

Background:

- This type of targeting is especially effective against organizations with insecure and exposed assets with poor cyber hygiene.
- OT devices have been regarded as easy targets when connected to the public internet, as they lack authentication and authorization methods.
- CISA has urged critical infrastructure asset owners and operators to [implement the mitigations outlined in its advisory](#).

What is next:

- Critical infrastructure entities with public-facing assets are likely to be vulnerable to such threat actor activities.
- Assets with remote access enabled are also likely to be targeted.
- Threat actors are likely to tamper with OT for defacement, configuration changes, operational disruptions, and physical damage.
- Actors ranging from state-sponsored entities to financially motivated cybercriminals are likely to deploy basic intrusion techniques to target critical infrastructure.



Luna Moth Continues to Extort Legal and Financial Firms

What we know:

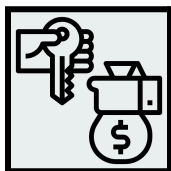
- Data extortion group Luna Moth has been conducting callback phishing attacks on U.S. legal and financial firms. They have been stealing sensitive data and extorting victims with ransom demands up to USD 8 million.

Background:

- Callback phishing is a social engineering tactic in which attackers pose as support staff to trick victims into calling fake numbers and handing over sensitive information or remote access.

Analyst note:

- This group is likely targeting legal and financial firms to access large databases containing sensitive client data, proprietary information, and business dealings—assets that, if stolen, could threaten them financially and operationally.



U.S. Sanctions Myanmar Militia Involved in Cyber Scams

What we know:

- The U.S. Treasury has sanctioned Myanmar militia group Karen National Army (KNA) and associated members for facilitating cyber scams targeting American citizens.

Background:

- The group's leader and two other individuals were also sanctioned. KNA is also involved in human trafficking and cross-border smuggling; it controls the Myanmar border area with Thailand.

Analyst note:

- The sanctions are likely going to disrupt the operations of cybercrime networks prevalent in Southeast Asia, including "pig butchering" scams. Furthermore, the sanctions are likely to dissuade other individuals from engaging with KNA.

| **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 added a total of six vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on [May 2](#), [May 5](#), [May 6](#), and [May 7](#). CISA has also released [three ICS advisories](#). A vulnerability (CVE-2024-38475) in [Apache HTTP Server mod_rewrite \(up to version 2.4.59\)](#) enables attackers to access unintended files or execute code via unsafe URL mappings. An already patched vulnerability, CVE-2025-3248, [impacts the open-source Langflow platform](#) and is being actively exploited. Hackers are actively exploiting an [unauthenticated remote code execution \(RCE\) vulnerability in Samsung MagicINFO 9 Server](#), a centralized content management platform. Researchers have found [flaws in SysAid's on-premise software](#) that allow unauthenticated attackers to remotely execute code with elevated privileges. The PGS Core plugin for WordPress is affected by a [PHP Object Injection vulnerability](#) (CVE-2025-0855) in all versions up to and including 5.8.0. Cisco has released fixes for a [critical IOS XE Wireless Controller flaw](#) that could enable unauthenticated remote attackers to upload arbitrary files.



CRITICAL

CVE-2025-46337

What happened: ADOdb is a hypertext preprocessor (PHP) database class library used for executing queries and managing databases. In versions prior to 5.22.9 (the patched version), there was a vulnerability whereby improper escaping of a query parameter could enable an attacker to execute arbitrary structured query language (SQL) commands.

- **What this means:** This vulnerability enables attackers to manipulate database queries through SQL injection, potentially gaining unauthorized access to sensitive data or modifying database contents. Such attacks are likely to lead to data breaches or even full system compromise.
- **Affected products:**
 - ADOdb's PostgreSQL database versions prior to 5.22.9

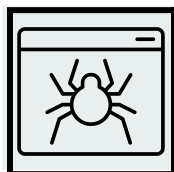
**CRITICAL****CVE-2025-4104**

What happened: The Frontend Dashboard plugin for WordPress had a vulnerability in versions 1.0 to 2.2.6 wherein the “`fed_wp_ajax_fed_login_form_post()`” function lacked proper capability checks. This enabled unauthenticated attackers to exploit the function to reset the administrator's email and password.

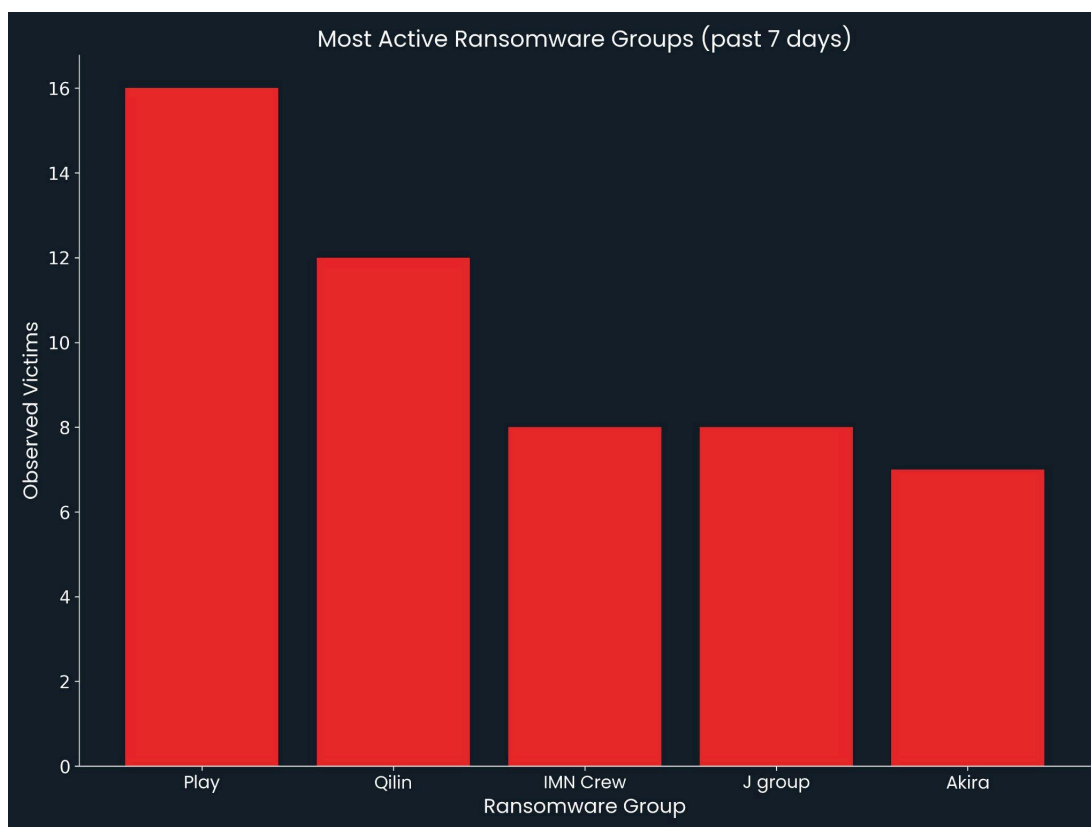
- **What this means:** This flaw enabled attackers to take over admin accounts without logging in, effectively giving them full control over the affected WordPress site. This could lead to site defacement, data theft, malware injection, or complete loss of site integrity.
- **Affected products:**
 - Versions 1.0 to 2.2.6

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

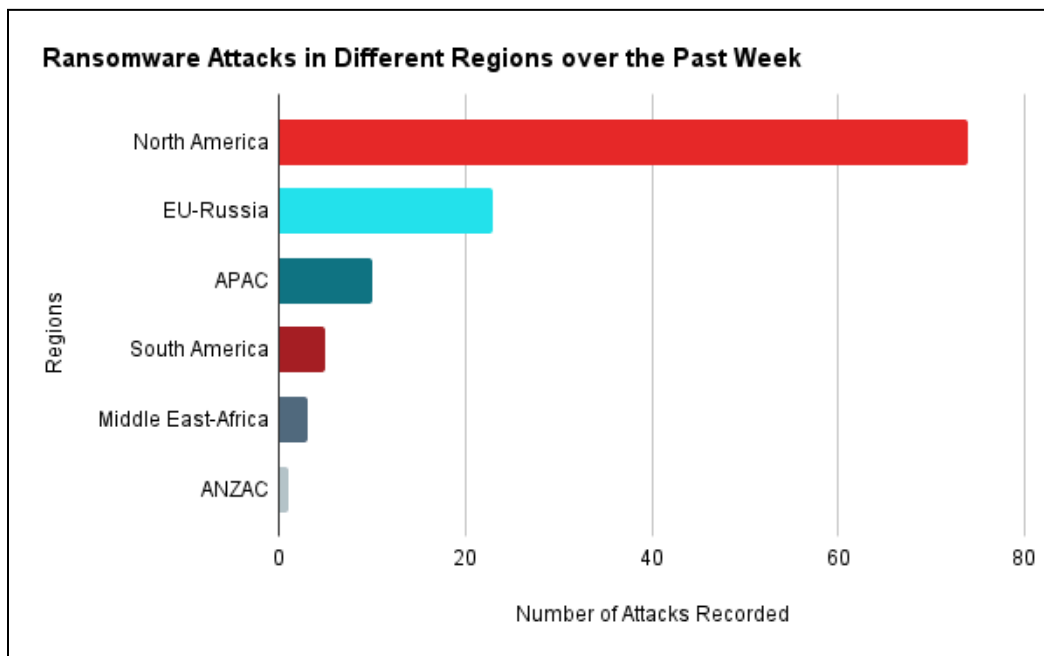


Ransomware in Focus: Major Groups and Regional Trends



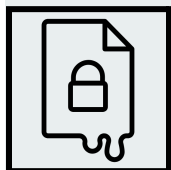
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Play, Qilin, IMN Group, J Group, and Akira were the most active ransomware groups. ZeroFox observed at least 116 ransomware victims disclosed, most of which are located in North America. Play and Qilin accounted for the largest number of attacks.



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. In North America, ZeroFox has observed at least 63 ransomware incidents, with the Manufacturing industry being the most affected. This week, the Play ransomware group was the most active in this region.



Data Breaches Affecting Companies and Customers

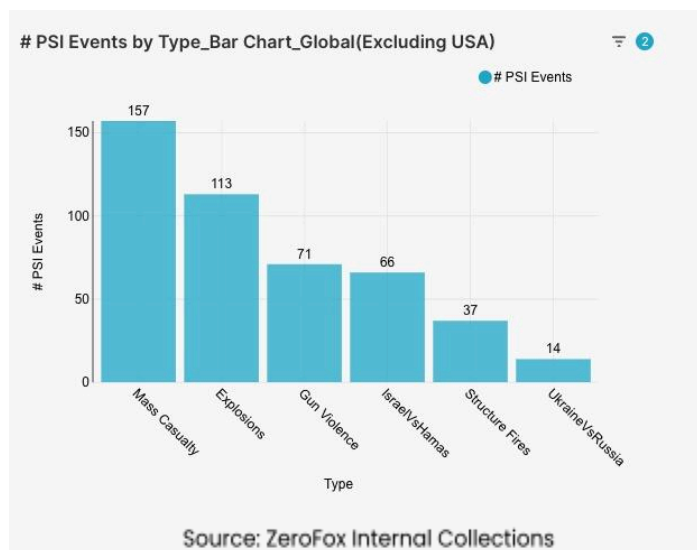
Targeted Entity	<u>Social Services, Health Care and Rescue Services Division of Helsinki</u>	<u>Texas Health and Human Services Commission</u>	<u>ClickFunnels</u>
Impacted Entities	Client data between 2012 and 2019	33,529 customers	Victim and third-party
Compromised Data and Infrastructure	Family law services's client data, including names, personal identity codes, and custody arrangements	Names, addresses, phone numbers, dates of birth, and email addresses;; Social Security, numbers, Medicaid, and Medicare identification numbers;; financial, employment, benefits, and insurance information, licenses, and more	90,000 phone numbers and 69,000 unique email addresses connected with a third party; and ClickFunnels's two large data tables involving 514,000 and 460,000 entries
Suspected Threat Actor	Unspecified	Employees	Satanic
Country/Region	Helsinki	Texas	United States
Industry	Government and Healthcare	Healthcare	Professional Services
Possible Repercussions	The data has now been secured with access controls. Although the data was not exposed to actors outside the division, it is possible that employees with unauthorized access could have exfiltrated data before mitigation steps were enforced.	This leaked healthcare data could enable threat actors to target patients in identity and financial frauds. Patients could be persuaded to meet the threat actors' feel compelled to give in to their demands to protect their data and privacy.	Investigations are currently underway to confirm this breach. If the threat actor's claims are true, it is likely that the actor will extort affected companies (the third party and ClickFunnels) and sell their data on DDW deep and dark web forums.

Three major breaches observed in the past week

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

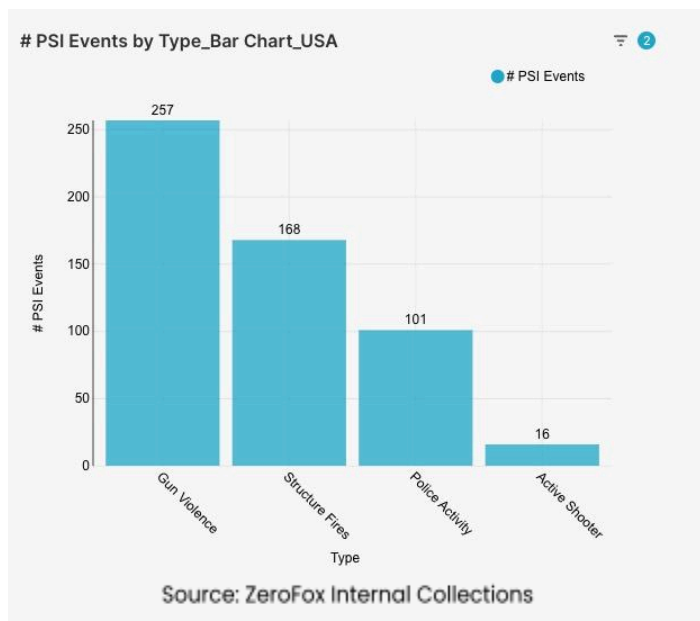


What happened: Excluding the United States, there was a 4 percent decrease in mass casualty events this week from the previous week, with the top contributing countries being Palestine, Syria, and India, in that order. Approximately 72 percent of these events were explosions, and the three aforementioned countries accounted for about 35 percent of all mass casualty alerts. General alerts related to the Israel-Hamas War (including protests, raids, and involvement in neighboring countries) decreased by 8 percent from the

previous week. Events related to Russia's war in Ukraine increased by 100 percent. The top three most-alerted subtypes were explosions, which saw a 3 percent decrease from the previous week; gun violence, which decreased by 8 percent; and structure fires, which decreased by 5 percent. Global protest activity decreased by 13 percent.

- **What this means:** The multiple percentage decreases in this week's data points likely reflect shifting conflict dynamics and sociopolitical pressures in key regions. The 4 percent overall decrease in mass casualty events may be attributed to temporary ceasefires, exhausted militant resources, or international diplomatic interventions—particularly in Gaza, where [humanitarian pauses](#) have occasionally slowed hostilities. The 8 percent drop in Israel-Hamas War-related alerts could signal a temporary de-escalation or media fatigue affecting alerting algorithms, while the sharp 100 percent spike in Russia-Ukraine war events suggests [renewed offensives](#) or territorial escalations, possibly in response to [Western aid](#) or shifting front lines. The United States, Russia, and Ukraine have continued to discuss potential [ceasefire](#) deals but have not yet agreed to anything. Meanwhile, the decline in gun violence, structure fires, and protest activity globally—13 percent fewer protests, despite widespread [May Day](#) demonstrations—may be influenced by stricter security measures, protest fatigue, or distraction by other crises leading to temporary lulls in civil action.

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 New York, which together made up 23 percent of this week's nationwide total. Gun violence

across the United States overall remained flat from the week prior. Police activity alerts decreased by 5 percent, and the top contributing states were California and Texas. Structure fires decreased by 6 percent, and the top two states for this subtype were New York and California. Notably, the number of active shooter incidents nationally doubled from the previous week.

- **What this means:** This week's incident alert data highlights both persistent and shifting public safety concerns across the United States. Gun violence remained steady overall, with California and New York accounting for 23 percent of alerts—likely driven by urban crime hotspots and consistent shootings in areas like the Bronx in New York City and Los Angeles. Police activity alerts fell by 5 percent, possibly due to fewer large-scale events or protests, though California and Texas continued to lead due to ongoing security concerns. Structure fires decreased by 6 percent, potentially aided by improved weather or prevention efforts, particularly in fire-prone California. The state has named May 4–10 as [Fire Prevention Week](#) and is making efforts in infrastructural changes and vegetation management ahead of its annual wildfire season. Notably, active shooter incidents doubled from the week prior, driven by several mass shootings—including one in [Houston](#), Texas, that killed one person and injured 15 on May 4. As the summer season commences, we expect to see increased numbers going forward.

| 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%