



*Weekly Intelligence Brief*

Classification: TLP:GREEN

July 1, 2024

## Scope Note

ZeroFox's Weekly Intelligence Briefing highlights the major developments and trends across the cyber threat landscape. 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 12:00 PM (EDT) on June 28, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

# | Weekly Intelligence Brief |

|                                                                                                          |           |
|----------------------------------------------------------------------------------------------------------|-----------|
| <b>  This Week's ZeroFox Intelligence Reports</b>                                                        | <b>2</b>  |
| ZeroFox Intelligence Brief – Cyber Threats to UK Elections                                               | 2         |
| ZeroFox Intelligence Flash Report – IntelBroker Sells Zero-Day Vulnerability Leveraged in Recent Attacks | 2         |
| ZeroFox Intelligence Brief – Political Upheaval Likely in French Elections                               | 3         |
| <b>  Cyber Intelligence Key Findings</b>                                                                 | <b>5</b>  |
| Russian Satellite Interference Under Review After International Complaints                               | 5         |
| Kaspersky Faces Sanctions from U.S. Treasury Soon After Ban                                              | 5         |
| CISA and Partners Explore Memory Safety in Critical Open Source Projects                                 | 6         |
| <b>  Deep and Dark Web Intelligence Key Findings</b>                                                     | <b>8</b>  |
| Interpol Argentina's Data Leaked on the Dark Web                                                         | 8         |
| Threat Actor Group Announces Attacks in France, to Include Paris Olympics                                | 8         |
| Threat Actors Advertising New Chrome Zero-Day Exploit                                                    | 9         |
| <b>  Exploit and Vulnerability Intelligence Key Findings</b>                                             | <b>11</b> |
| CVE-2024-5655                                                                                            | 11        |
| CVE-2024-5276                                                                                            | 12        |
| <b>  Ransomware and Breach Intelligence Key Findings</b>                                                 | <b>14</b> |
| Ransomware Intelligence: Ransomware Targets Governments and Critical Infrastructure Worldwide            | 14        |
| Breach Intelligence: Data Security Incidents Across the Globe                                            | 15        |
| <b>  Physical and Geopolitical Intelligence Key Findings</b>                                             | <b>18</b> |
| Physical Security Intelligence: Global                                                                   | 18        |
| Physical Security Intelligence: United States                                                            | 19        |
| <b>  Appendix A: Traffic Light Protocol for Information Dissemination</b>                                | <b>20</b> |
| <b>  Appendix B: ZeroFox Intelligence Probability Scale</b>                                              | <b>21</b> |

## **| This Week's ZeroFox Intelligence Reports**

### **ZeroFox Intelligence Brief – Cyber Threats to UK Elections**

When the United Kingdom (UK) holds its general election on July 4, 2024, Prime Minister Rishi Sunak's Conservative Party is very likely to lose its majority to the main opposition: the Labour Party led by Keir Starmer. Recent polling indicates that, should Labour win, the Conservatives may not even be the largest opposition party, with the upstart Reform UK party threatening to further reduce its share of voters. Nevertheless, Conservatives will be campaigning in an attempt to prevent the loss of seats, while Labour will primarily be campaigning to win as many seats as possible to avoid the need to form a coalition with other parties. The 2024 UK elections are also taking place during a period of massive weaponization of cyberspace for covert, as well as overt, digital influence and intimidation campaigns. Many of the cyber instances ZeroFox discovered (including the propagation of deepfakes, tactical disclosure of "technically legitimate" half-truths in malinformation campaigns, and stealthy-yet-mass-scale disinformation campaigns) are at least partially designed to influence voter behavior to narrow the margin of a Labour victory or a Conservative defeat. ZeroFox discovered geopolitical and financially motivated data breaches and distributed denial-of-service (DDoS) attacks conducted by so-called "hacktivists" tied to the election as well.

### **ZeroFox Intelligence Flash Report – IntelBroker Sells Zero-Day Vulnerability Leveraged in Recent Attacks**

Prominent and well-regarded threat actor "IntelBroker" has registered an account on the popular illicit hacking forum BreachForums—one day after removing themselves from the platform. Shortly after returning to the forum, IntelBroker began advertising numerous illicit network accesses and data breaches targeting high-profile organizations from a multitude of industries. The majority of these attacks alluded to the exploitation of an unspecified vulnerability targeting Atlassian software. Later, IntelBroker advertised the sale of a zero-day vulnerability that targets Atlassian Jira software via remote code execution (RCE). This was purchased by an unknown actor between June 20 and June 24, 2024, though it is unlikely that IntelBroker received the exorbitant asking price of USD 800,000. The details provided in the announcement of the three attacks were almost certainly intended to serve as an advertisement or proof of concept for the zero-day vulnerability.

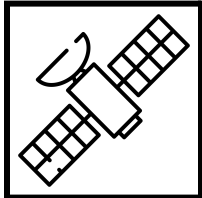
## **ZeroFox Intelligence Brief – Political Upheaval Likely in French Elections**

Following the unexpectedly strong performance of the far-right Rassemblement Nationale (RN) party in European parliamentary elections on June 6-9, French President Emmanuel Macron declared a snap parliamentary election for the end of the month. This decision has thrown France's political system into chaos, as it is unclear what party or coalition will hold power for the next three years. Observers were initially taken by surprise when Macron dissolved the Assemblée Nationale, as—despite his party's poor results in the European Union (EU) parliamentary elections—he was in no way obligated to do so. Calling for elections immediately after a major defeat may be atypical but has a political logic: Macron is likely trying to rally his centrist coalition with that of the left as a bulwark against the rising influence of the right. Failing that, Macron may still benefit from a strong showing by the RN, in that it would force them to take part in governing and expose them to the negativity surrounding decision-making. In this way, Macron could better-position himself for the more consequential 2027 presidential elections.

# | Cyber Intelligence |

## | Cyber Intelligence Key Findings

### Russian Satellite Interference Under Review After International Complaints



**What happened:** The International Telecommunications Union (ITU) is reviewing complaints from Ukraine and European countries about Russian satellite interference impacting navigation services and television broadcasts. The interference, which includes GPS jamming and broadcasting violent images on children's television channels, has prompted Ukraine and other nations to request ITU intervention to stop the disruptions. France, Sweden, the Netherlands, and Luxembourg also reported similar issues. Russia's Geneva diplomatic mission denied these allegations, stating compliance with ITU rules and accusing NATO countries of similar actions. This situation follows accusations from Western officials that Russia launched a major cyberattack on a Ukrainian satellite network during its 2022 invasion. Airlines have also reported increased GPS interference, and Estonia has blamed Russia for disrupting navigation above the Baltic states. The ITU, responsible for global satellite coordination, aims to resolve the interference issue but has not specified how it will address the complaints.

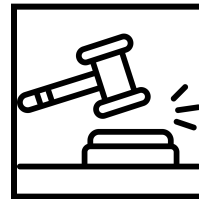
- **What this means:** The use of cyberattacks for political purposes is an established tactic, with satellite interference emerging as a significant threat. Global satellite networks are lucrative targets for state-sponsored adversaries acting with geopolitical intentions to spread propaganda and influence target populations; such cyberattacks can lead to more tangible threats. The jamming of GPS signals can significantly disrupt air traffic control, potentially endangering lives and impacting commerce. The manipulation of television broadcasts to insert violent war images is likely a psychological warfare weapon. Cyberattacks on satellites, especially commercial ones, are cheaper and harder to trace compared to traditional anti-satellite tactics. The repercussions of such attacks extend beyond immediate replacement costs, affecting aviation, railroads, marine transportation, and financial services reliant on precise timestamps. Moreover, accusations of sabotage between Russia and NATO countries further complicate international relations amid the ongoing Russia-Ukraine war. An active attempt to interfere with another country's satellites signals the possibility such geopolitical tensions could spillover into the realms of cybersecurity and space.

### Kaspersky Faces Sanctions from U.S. Treasury Soon After Ban

**What happened:** The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) imposed [sanctions](#) on 12 senior executives at Kaspersky Lab shortly after the Department of Commerce banned the Russian company and its affiliates from operating in the United States.

This ban, effective July 20, 2024, includes placing Kaspersky on the Entity List due to concerns over national security. These actions follow long-standing allegations of ties between Kaspersky Lab and the Russian government, which the company denies.

- **What this means:** The sanctions imposed on Kaspersky's 12 senior executives block all their property and interests within the United States or controlled by Americans. By prohibiting Kaspersky's software and services, the United States aims to mitigate risks associated with foreign entities that could compromise national security. It also sets a precedent for foreign institutions engaging in significant transactions with the Russian military-industrial sector, thereby serving as a warning to entities that facilitate or enable activities that could compromise national security. Amid ongoing geopolitical tensions, Russia has criticized the U.S. sales ban on Kaspersky software, calling it a typical effort to stifle foreign competition in favor of American products. However, Kaspersky has maintained its stance of not being associated with the Russian government.



## [CISA and Partners Explore Memory Safety in Critical Open Source Projects](#)



**What happened:** The Cybersecurity and Infrastructure Security Agency (CISA) has released [Exploring Memory Safety in Critical Open Source Projects](#) in partnership with the Federal Bureau of Investigation (FBI) and other agencies. This guidance aims to provide organizations with findings on the scale of memory safety risks in specific open source software (OSS). Memory safety vulnerabilities are among the most prevalent classes of software vulnerability and reportedly generate substantial costs for both software manufacturers and consumers related to patching, incident response, and other efforts. This joint guidance provides a starting point for software manufacturers to create memory-safe roadmaps—including plans to address memory safety in external dependencies, which commonly include OSS.

- **What this means:** OSS is often an integral part of critical infrastructure and enterprise software. This type of integration is occasionally observed to be under-maintained and secured, thereby presenting opportunities for bad actors to take advantage and cause significant damages. CISA has warned that even those open source projects written in memory-safe languages could contain memory safety vulnerabilities due to direct use of memory-unsafe languages or external dependency on projects that use memory-unsafe languages. Additionally, low-level functional requirements to disable memory safety could create opportunities for memory safety vulnerabilities in code written in otherwise memory-safe languages.

# | Deep and Dark Web Intelligence |

## | Deep and Dark Web Intelligence Key Findings

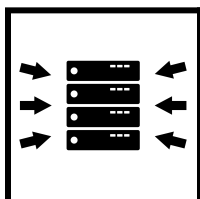
### Interpol Argentina's Data Leaked on the Dark Web

**What happened:** On June 23, 2024, threat actor "emocat" claimed to have leaked data associated with Interpol Argentina on the predominantly English-language dark web forum BreachForums. Emocat allegedly leaked sensitive operational data that includes internal communications and personal details of law enforcement officers. The threat actor did not disclose the initial source of the data breach or how it was exploited.



- **What this means:** This data leak could have various implications. Specifically, the leak of personally identifiable information (PII) can lead to identity theft, fraud, or other danger to the individuals involved. Additionally, the leak of operational data could compromise or disrupt any ongoing investigations, potentially leading to other legal repercussions. Moreover, this type of breach could undermine the public's trust in law enforcement by instilling doubt in the security of critical organizations.

### Threat Actor Group Announces Attacks in France, to Include Paris Olympics

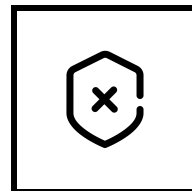


**What happened:** On June 24, 2024, the threat actor group "Cyber Army of Russia Reborn" announced an attack against the French Film Festival and the Grand Palace in Paris. The attack was carried out via DDoS in conjunction with other prominent pro-Russian hacktivist groups. Additionally, the group's Telegram post claimed the pro-Russian hacktivist collective is gearing up for a focused campaign targeting the upcoming Paris Olympics this summer.

- **What this means:** These attacks continue a series of DDoS strikes against NATO states over recent months. While Cyber Army of Russia Reborn claimed these attacks, the group gave credit to other hacktivists with whom it often cooperates, including "NoName(057)16", "Hacknet", "Cyber Dragon", and "UserSec"—each prominent, pro-Russian hacktivists in their own right. DDoS attacks, particularly against infrastructure, allow for a low-risk/high-reward strike against a nation that will draw attention to the hacktivist's cause. ZeroFox assesses with high confidence that these hacktivist groups will continue to carry out DDoS attacks with emphasis on European NATO nations. Cyber Army of Russia Reborn has made good on prior threats, and its claim of a pending campaign against France during the 2024 Olympic games should be taken seriously.

## Threat Actors Advertising New Chrome Zero-Day Exploit

**What happened:** On June 25, 2024, untested threat actor “Cas” claimed to be selling a zero-day Sandbox Escape RCE exploit for the Chrome browser on BreachForums. The next day, untested threat actor “ctf” (claiming to act as a broker) advertised the same exploit for sale on the predominantly Russian-language dark web forum xss. Both actors’ advertisements claim that the exploit was successfully tested on Chrome browser versions 126.0.6478.126 and 126.0.6478.127, as well as on Microsoft Windows versions 21H1 and 21H2. The actors are seemingly selling the exploit for USD 1 million, which can be accepted via exchanges of the cryptocurrencies XMR (Monero) and BTC (Bitcoin). The post also states that the buyer can utilize the threat actors “Aegis” or IntelBroker (discussed above in this report) as a middleman/escrow service.



- **What this means:** While Cas and ctf are untested threat actors for which ZeroFox has not identified any previous activity, the discovery and exploitation of a zero-day typically requires an advanced skill set. This, in combination with their alleged affiliation with the well-regarded and established threat actor IntelBroker, could indicate that the actors possess sophisticated capabilities. Moreover, on June 17, 2024, IntelBroker advertised a zero-day RCE exploit for Atlassian Jira in a post that also mentioned its relatively new escrow app (ZeroFox observed IntelBroker first advertising its escrow app in an April 2 post). This corroborates Cas and ctf’s claim they are using IntelBroker as an escrow service, which indicates that the sale of the exploit is likely legitimate.

# | 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 the industrial control system, networking, storage, and technology domains. Juniper has [released](#) patches for multiple vulnerabilities that affect Juniper Secure Analytics (JSA). A cyber threat actor could exploit one of these vulnerabilities to take control of an affected system. CISA has [added](#) three new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog: GeoSolutionsGroup JAI-EXT Code Injection Vulnerability (CVE-2022-24816), Linux Kernel Use-After-Free Vulnerability (CVE-2022-2586), and Roundcube Webmail Cross-Site Scripting (XSS) Vulnerability (CVE-2020-13965). Cybersecurity researchers have warned of a critical flaw ([CVE-2024-37032](#)) in Ollama's artificial intelligence (AI) platform that can potentially allow RCE. The issue, dubbed Problama, was fixed on May 7, 2024, after disclosure. [CVE-2024-6101](#) stems from an inappropriate implementation in V8 in Google Chrome that allows a remote attacker to perform out-of-bounds memory access via a crafted HTML page. Some [versions](#) of Dell PowerProtect DD have a buffer overflow vulnerability (CVE-2024-29176). An attacker with low privileges could exploit this to crash the application or execute arbitrary code on the underlying operating system with the application's privileges. [CVE-2024-5181](#) affects mudler/localai version 2.14.0 due to a command injection flaw. This vulnerability stems from how the application processes the backend parameter in its configuration file, potentially allowing malicious initialization process names. CVE-2024-5806 is a critical authentication bypass vulnerability in [Progress MOVEit Transfer](#), a managed file transfer (MFT) solution. Fortra FileCatalyst Workflow has a critical SQL injection vulnerability ([CVE-2024-5276](#)) that allows remote unauthenticated attackers to create unauthorized admin accounts and manipulate data in the application database. Apple has released a firmware [update](#) for its AirPods, addressing a vulnerability (CVE-2024-27867) that could allow attackers to spoof paired devices and eavesdrop on conversations. Siemens Energy automation products are affected by [multiple](#) vulnerabilities. An unauthenticated buffer-overread could leak information, while authenticated users could escalate privileges due to insufficient input sanitization.

### Notable vulnerabilities:

#### [CVE-2024-5655](#)



**What happened:** This vulnerability is present in certain versions of GitLab Community and Enterprise Edition products. It could allow an attacker to trigger a pipeline as another user under certain circumstances.

➤ **What this means:** This **CRITICAL**-severity vulnerability could allow an attacker to trigger a pipeline as another user. GitLab has informed users that

upgrading to the latest versions will cause pipelines to no longer run automatically when a

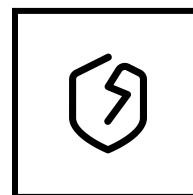
merge request is re-targeted after its previous target branch is merged. Users must manually start the pipeline to execute continuous integration (CI) for their changes.

➤ **Affected products:**

- GitLab CE/EE 15.8 to 16.11.4
- GitLab CE/EE 17.0.0 to 17.0.2
- GitLab CE/EE 17.1.0 to 17.1.0

## **CVE-2024-5276**

**What happened:** Cybersecurity researchers identified a **CRITICAL** SQL injection vulnerability (CVSS Score: 9.8) in Fortra's FileCatalyst Workflow, a web-based file exchange platform. This flaw allows remote, unauthenticated attackers to create rogue admin users and manipulate the application's database. Fortra has released a patch in FileCatalyst Workflow version 5.1.6 Build 139.

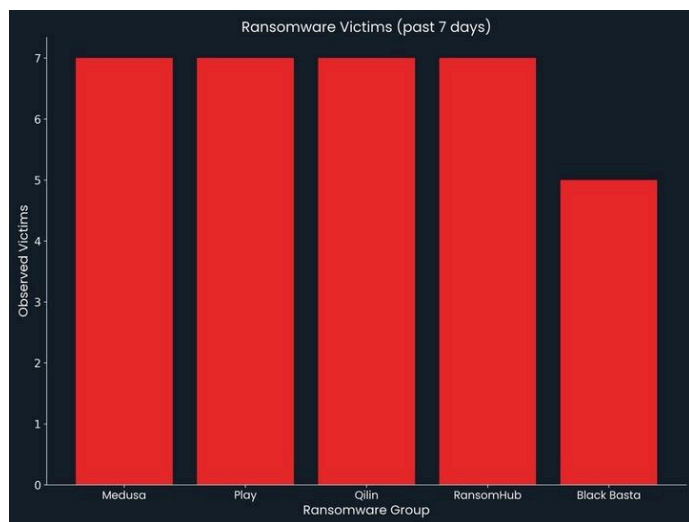


- **What this means:** The SQL injection vulnerability poses a severe risk, enabling attackers to modify application data and create unauthorized admin accounts—potentially compromising the platform's security integrity. Although data exfiltration is not possible, the availability of a public exploit increases the threat of active attacks. Users must promptly upgrade to the latest patched version to mitigate these risks and prevent unauthorized access.
- **Affected products:**
- Fortra's FileCatalyst Workflow versions 5.1.6 Build 135 and older

# | Ransomware and Breach Intelligence |

## **Ransomware and Breach Intelligence Key Findings**

### **Ransomware Intelligence: Ransomware Targets Governments and Critical Infrastructure Worldwide**



Source: ZeroFox Internal Collections

**What happened:** A cyberattack has severely impacted Indonesia's data centers, affecting nearly 200 government agencies and leaving many systems down, though some are now recovering. The attackers have [demanded](#) a USD 8 million ransom for the decryptor, which the Indonesian government has refused to pay. Meanwhile, cybersecurity experts have [linked](#) Chinese and North Korean state-sponsored actors to ransomware and data encryption attacks conducted from 2021 to 2023 that targeted global

government and critical infrastructure sectors. These sophisticated groups use tools like Cobalt Strike and custom malware to evade detection, destabilize services, and strain international relations. This blend of cybercrime and state-sponsored espionage complicates attribution, allowing states to claim plausible deniability while blaming independent cybercriminals for the attacks. In the past week, ransomware attacks have also targeted other industries, with the manufacturing, technology, and construction sectors suffering the most number of attacks according to ZeroFox metrics. CDK Global, a car dealership software provider, [experienced](#) two cyberattacks in June that disrupted its systems and customer support channels. The "BlackSuit" ransomware gang is suspected to be responsible, and CDK clients were left with limited support options during the outage.

- **What this means:** The ransomware used against Indonesia's government agencies is suspected to be LockBit 3.0, a variant that often targets governments and critical infrastructure. The recent surge in activity, including claims of an attack on a prominent U.S. financial organization, suggests LockBit is aiming to re-establish its pre-takedown status through high-profile attacks. Over the past year, ZeroFox has identified over 650 victims of LockBit ransomware, with around 20 percent affecting government and critical infrastructure sectors. The combination of sophisticated tools—like Cobalt Strike and custom malware—with ransomware to extort ransom, sabotage, distract, misattribute, and eliminate evidence used by Chinese and the North Korean actors reflects the evolving techniques and skills of state-sponsored cyber espionage groups. The deployed malware

allows these adversaries to cause significant damage to critical infrastructure and serve the broader strategic interests of adversarial states. Additionally, the blending of cybercrime and state-sponsored espionage tactics complicates attribution and allows states to claim plausible deniability by framing these attacks as the work of independent cybercriminals. Meanwhile, the quick restoration of services by CDK Global after its first breach has raised concerns about increased vulnerability to future attacks. CDK has warned clients about potential follow-on attacks from unauthorized contacts posing as CDK representatives, highlighting the need for cautious and staggered recovery approaches to enhance protection against cyber threats.

## **Breach Intelligence: Data Security Incidents Across the Globe**

**What happened:** This week, there have been multiple data breach incidents reported from the United States and other countries around the globe. [Levi Strauss & Co.](#), a well-known U.S.-based denim retailer, disclosed a security breach affecting more than 72,000 customers due to an automated credential-stuffing attack. Cybercriminals potentially accessed personal data stored in online accounts, including names, email addresses, delivery addresses, order histories, and partial payment card information. Levi Strauss & Co. assured customers that its internal systems remained secure and that there is currently no evidence of misuse of the compromised data. Affected customers have been notified, underwent password resets, and were advised to update passwords on other platforms as a precaution. Hacking group “ShinyHunters” claimed an attack on [Ticketek](#), an Australian-based event ticketing company, wherein the threat group allegedly stole 30 million users’ data. According to Ticketek’s [statement](#), no payment information has been breached, but other information like customer names, dates of birth, and email addresses are likely to have been impacted. [Neiman Marcus](#) has reported a data breach following attempted sales of its database by hackers involved in recent Snowflake data theft incidents. The American luxury retailer disclosed the breach in a notification to the [Office of the Maine Attorney General](#), revealing that personal information of 64,472 individuals was leaked. Threat actor “Sp1d3r” advertised Neiman Marcus’ data for sale on a hacking forum for USD 150,000 in exchange. Sp1d3r also claimed to have leaked a database associated with [Jollibee](#), a U.S.-based fast food delivery company, on BreachForums. The threat actor claimed to sell 32 million customers’ data (including names, addresses, phone numbers, email addresses, hashed passwords, sales orders, and transactions) priced at USD 40,000. [Bharat Sanchar Nigam Limited](#) (BSNL), a public telecommunications company in India, suffered a massive data breach exposing sensitive information of millions of users. The breach, carried out by a hacker known as “kiberphant0m,” involved critical data such as IMSI numbers and SIM details. Arkansas-based [Evolve Bank](#) has confirmed a cybersecurity incident wherein customer data was exposed on the



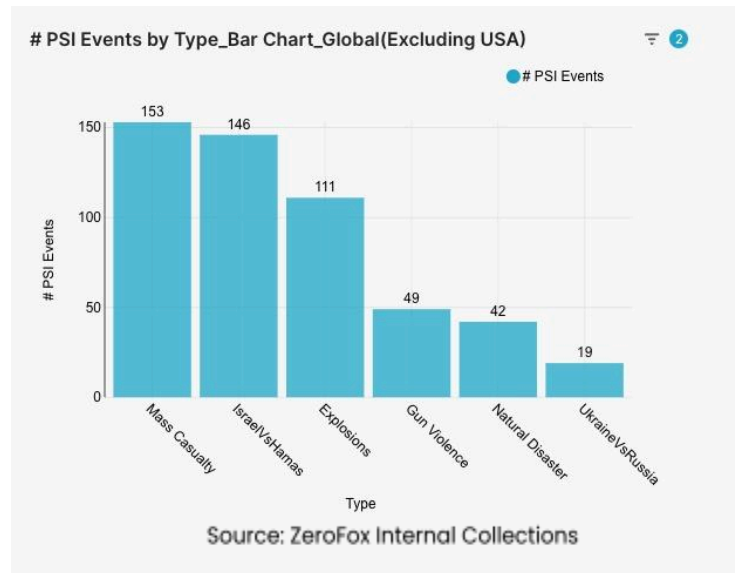
dark web. The breach included account numbers and deposit balances linked with the fintech company. Affected customers have been informed and advised on precautionary measures. The cybercriminal group Lockbit 3.0 reportedly claimed responsibility for the breach and threatened to publish sensitive data unless a ransom is paid. Meanwhile, a Chinese state-sponsored hacking group known as [RedJuliatt](#) intensified its cyberattacks targeting Taiwanese organizations, particularly in the government, education, technology, and diplomacy sectors. RedJuliatt exploited vulnerabilities in SoftEther VPN software to breach the networks of various institutions, including government agencies in multiple countries.

- **What this means:** The recent spate of data breaches affecting companies like Levi Strauss & Co., Ticketek, BSNL, Evolve Bank, and more poses significant risks to customers globally. For affected individuals, compromised personal information such as names, email addresses, delivery details, and (in some cases) partial payment card information can lead to identity theft, phishing attacks, and fraud. Threat actors such as ShinyHunters and various hacking groups can leverage this stolen data to perpetrate further credential-stuffing attacks, sell personal information on dark web forums, or conduct targeted phishing campaigns. Threat actors can re-sell the stolen financial details on the dark web, potentially inflicting further financial harm on victims beyond the initial fraudulent transactions. Furthermore, RedJulliet's hacking patterns are observed to be similar to those of Chinese state-sponsored groups; the group has been noted attempting cyberattacks against more than 70 Taiwanese organizations. Individuals are urged to remain vigilant, update their passwords not only for affected accounts but across all platforms, monitor financial statements for suspicious activity, and consider identity theft protection services as a precautionary measure.

# Physical and Geopolitical Intelligence

## Physical and Geopolitical Intelligence Key Findings

### Physical Security Intelligence: Global

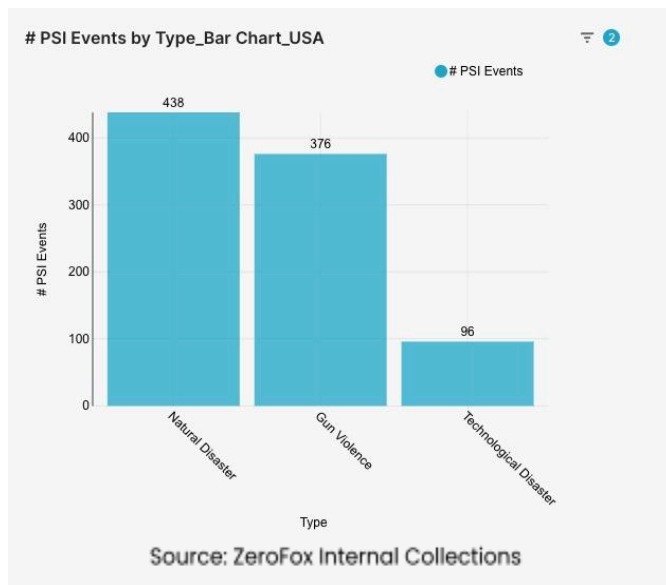


**What happened:** Excluding the United States, there was a 1 percent decrease in mass casualty events this week from the previous week, with the top contributing countries being Palestine, Russia, and Lebanon; approximately 73 percent of these events were explosions. General alerts related to the Israel-Hamas War (including protests, raids, and involvement in neighboring countries) increased by 11 percent from the previous week. Additionally, events related to Russia's war in Ukraine increased by 111

percent. The top three most-alerted subtypes were explosions, which saw an 11 percent increase from the previous week; gun violence, which decreased by 2 percent; and natural disasters, which increased by 17 percent. Notably, protest activity saw an increase of 15 percent.

- **What this means:** Russia had the second highest number of mass casualty events this week due to a series of terrorist attacks over the weekend in which 20 people were killed and 12 people were injured at a church, a synagogue, and a police post in [Dagestan](#). While there was no immediate claim of responsibility, it is important to note that this attack came three months after the ISIS-facilitated operation in Moscow that killed 145 people; additionally, Dagestan is known to be a hotbed of Islamic extremism, but no official connection can be made at this time. As for the Russia-Ukraine conflict, this weekend also saw a large-scale Russian [attack](#) on Ukrainian power grids, which may explain the increase in the usage of the UkraineVsRussia tag last week. It is the eighth time Russia has launched an attack on energy infrastructure facilities in the past three months. Finally, protest activity increased partly due to Kenyan [demonstrations](#) against a controversial tax bill; more than 20 people were killed. The bill was not signed into law, but protesters continued to demand that President Ruto step down.

## Physical Security Intelligence: United States



**What happened:** In the past week, the top three most-alerted incident subtypes were natural disaster, gun violence, and technological disaster (in that order). Natural disaster alerts typically involve fires and severe weather; gun violence alerts are instances in which there is a confirmed or likely confirmed victim; and technological disasters encompass large-scale man-made disasters, such as hazmat situations and train derailments. The top two states that had the most gun violence alerts were Illinois and California, which together made up one-third of this week's nationwide total (33 percent). Gun

violence across the United States overall decreased by 6 percent from the week prior. The top two contributors to natural disaster alerts this week were California and New York, and natural disaster alerts across the country increased by 17 percent. The top contributing states to technological disasters were Florida and Maryland.

- **What this means:** Natural disasters have once again become the most alerted subtype, as much of the nation has seen extreme heat waves, increased wildfires, and flood-inducing storms this week. The head of the Homeland Security Department said on [Friday](#) that the Federal Emergency Management Agency (FEMA), which is the agency tasked with responding to disasters across the country, is preparing as it goes into what is expected to be an intense hurricane and wildfire season caused by climate change. Interestingly, technological disasters were the third most alerted subtype this week, which may go hand in hand with the increased global warming and recent heat waves. A recent study determined that U.S. oil and natural gas wells, pipelines, and compressors are spewing three times the amount of the potent heat-trapping gas [methane](#) as the government has determined and that about 30 percent of the world's warming since pre-industrial times comes from methane emissions. As the climate continues to change, the United States and the rest of the world are likely to see more life-threatening disasters.

Interested in more ZeroFox Threat Intelligence? ZeroFox produces timely, relevant, and actionable [intelligence reporting](#) regularly to keep your team informed on developments in the threat landscape.

## | Appendix A: Traffic Light Protocol for Information Dissemination

|                         | Red                                                                                                                                                                                                    | Amber                                                                                                                                                                                                                                                                                                                        |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WHEN SHOULD IT BE USED? | <b>Sources may use</b><br><b>TLP:RED</b> 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. | <b>Sources may use</b><br><b>TLP:AMBER</b> 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?   | <b>Recipients may NOT share</b><br><b>TLP:RED</b> with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.                                     | <b>Recipients may ONLY share</b><br><b>TLP:AMBER</b> 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.<br><b>Note that</b><br><b>TLP:AMBER+STRICT</b> restricts sharing to the organization only. |
|                         | Green                                                                                                                                                                                                  | Clear                                                                                                                                                                                                                                                                                                                        |
| WHEN SHOULD IT BE USED? | <b>Sources may use</b><br><b>TLP:GREEN</b> when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.              | <b>Sources may use</b><br><b>TLP:CLEAR</b> when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.                                                                                                                                                      |
| HOW MAY IT BE SHARED?   | <b>Recipients may share</b><br><b>TLP:GREEN</b> information with peers and partner organizations within their sector or community but not via publicly accessible channels.                            | <b>Recipients may share</b><br><b>TLP:CLEAR</b> 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%         |