



Weekly Intelligence Brief

Classification: TLP:GREEN

June 17, 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 14, 2024**; 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 – Iranian Data Leak Advertised on the Dark Web	2
ZeroFox Intelligence Flash Report – Threat Actor Linked to ShinyHunters Advertises Extortionate Data Breach	2
ZeroFox Intelligence Assessment – UEFA Euro 2024 Tournament	2
ZeroFox Intelligence Brief – Underground Economist: Volume 4, Issue 12	3
 Cyber Intelligence Key Findings	5
Hacktivists Target EU Political Parties in DDoS Attacks	5
Pure Storage Discloses Data Breach Caused by Snowflake Workspace Compromise	5
Phone Scammers Impersonating CISA Employees	6
 Deep and Dark Web Intelligence Key Findings	8
New BreachForums–Associated Telegram Channels Appear Following Deletion of Prior One	8
Threat Actor Conducts Cyberattack Against German Government	8
Untested Threat Actor Advertised Access to a Taiwanese Telecommunication Company	9
 Exploit and Vulnerability Intelligence Key Findings	11
CVE-2023-50868	11
CVE-2024-32896	12
 Ransomware and Breach Intelligence Key Findings	14
Ransomware Intelligence: Eldorado and Play Account for Majority of Attacks	14
Breach Intelligence: 750,000 Individuals' Data Stolen in Frontier Communications Attack	15
 Physical and Geopolitical Intelligence Key Findings	17
Physical Security Intelligence: Global	17
Physical Security Intelligence: United States	18
 Appendix A: Traffic Light Protocol for Information Dissemination	19
 Appendix B: ZeroFox Intelligence Probability Scale	20

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Flash Report – Iranian Data Leak Advertised on the Dark Web

Untested English-speaking actor “irleaks” has announced the sale of a large leaked data set pertaining to an independent Iranian government agency, the Hajj and Pilgrimage Organization, on the dark web Onniforums community. The leaked data will very likely attract threat collectives with geopolitical or ideological motivations, including hacktivist and state-sponsored groups hostile to Iran. Additionally, financially motivated threat actors, such as ransomware groups, will likely be interested. The recent data leak is very likely related to the ongoing Israel-Hamas war and demand from geopolitically aligned actors for state-related data. It is likely that data leaks implicating both Israel and Iran will continue to be advertised by threat actors on dark web forums while the conflict persists.

ZeroFox Intelligence Flash Report – Threat Actor Linked to ShinyHunters Advertises Extortionate Data Breach

Untested threat actor “spld3r” has advertised the sale of a notably-large leaked data set in the Russian-speaking dark web forum xss. The breach allegedly contains 65,000 records of data stolen from a U.S.-based financial organization that purportedly include both personal financial information (PFI) and personally identifiable information (PII). The owner of this stolen data is likely a victim of the ongoing fallout from the alleged breach of cloud-based service provider Snowflake. Since the alleged breach on May 23, 2024, several of Snowflake’s assumed customers’ data have been advertised on deep and dark web (DDW) forums. Spld3r is almost certainly synonymous with, or heavily associated with, threat actor “ShinyHunters”, who is very likely responsible for recent attacks against Snowflake customers. In the coming weeks, it is very likely that additional Snowflake customers will be implicated in data breaches, with the stolen information being advertised for sale in DDW forums.

ZeroFox Intelligence Assessment – UEFA Euro 2024 Tournament

The 17th Union of European Football Associations (UEFA) European Championship (Euro 2024) soccer tournament is due to take place across Germany from June 14 to July 14. The quadrennial event comes with myriad logistics issues due to the influx of millions of fans from at least 24 countries attending 51 matches across 10 stadiums. Germany’s public transportation, accommodation, tourism, and security services will be put to the test. German authorities are most concerned with the transportation system, which has been beset by funding cuts and labor strikes in 2024, as well as a renewed terrorism threat posed by supporters and terror groups like al-Qaeda and the Islamic State.

Euro 2024 attendees may also experience issues related to crime, public drunkenness, and cyber scams targeting spectators at the matches and related events.

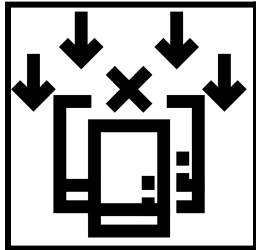
ZeroFox Intelligence Brief – Underground Economist: Volume 4, Issue 12

On June 9, 2024, the actor "wockstar" announced the sale of the source code for their custom-built ransomware-as-a-service (RaaS) project Rust, which includes both the management web panel and the affiliate panel, on the Russian-speaking DDW forum RAMP. On May 20, 2024, untested actor "Plifal" announced a new malicious tool named Plifal Software on the Russian-speaking dark web forum Exploit.

| Cyber Intelligence |

Cyber Intelligence Key Findings

Hacktivists Target EU Political Parties in DDoS Attacks

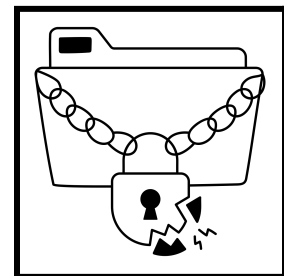


What happened: Hactivist group “HackNet” has claimed responsibility for distributed denial-of-service (DDoS) attacks on election-related sites and political parties, coinciding with the European Parliament elections. Network defenders have mitigated at least three DDoS attacks, including two significant attacks on June 5 and 6. The first attack peaked at 115 million requests per hour, while the second reached 44 million requests per hour. Both attacks targeted pro-Russian nationalist political parties Party for Freedom (PVV) and Forum for Democracy (FvD).

- **What this means:** The hactivist group’s focus on parties with pro-Russian stances suggests a strategic motive to target entities opposing its ideological views. Nonetheless, hactivist attacks are more likely to be a general nuisance than to directly meddle in the election process or interfere with the results. However, hactivists can influence political landscapes and voter opinions, in addition to inconveniencing people, thus besmirching the electoral process. DDoS attacks on election-related sites also reflect the potential for such disruptions to impact voter access to information and election integrity. More hactivists are likely to jump on the bandwagon and conduct such attacks during the election, reflecting the increasing trend of politically motivated cyberattacks targeting democratic processes.

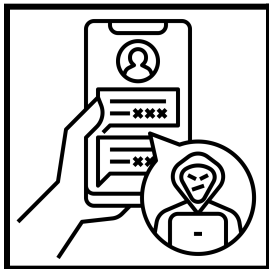
Pure Storage Discloses Data Breach Caused by Snowflake Workspace Compromise

What happened: Cloud storage systems and services provider Pure Storage has [confirmed](#) a data breach related to Snowflake, with a single data analytics workspace compromised. According to the security bulletin on its support page, the breach did not expose any customer data. The breach affected telemetry information used for customer support, including company names, email addresses, and software release versions. Pure Storage continues to monitor its systems and has found no further unusual activity or threats to its infrastructure. Researchers investigating the Snowflake credentials compromise have reported that the lack of multi-factor authentication (MFA) was a common factor in the breaches affecting Snowflake customers (including Santander and TicketMaster), although it is unclear if this was the case for Pure Storage.



- **What this means:** The Snowflake credentials compromise has been [attributed](#) to threat actor group “UNC5537” (potentially linked to Scattered Spider), which also reportedly hacked into 165 organizations with the help of stolen Snowflake credentials. The compromise is likely a direct consequence of vulnerabilities in cloud-based services and highlights the potential risks of not employing sufficient authentication methods. In a report released earlier this month, ZeroFox [assessed](#) that it is very likely that additional Snowflake customers will be implicated in data breaches, with the stolen information advertised for sale in DDW forums. Furthermore, the Snowflake-related breaches might set precedents for future digital extortion tactics, with a trend toward omitting payload encryption to attract more threat actors.

Phone Scammers Impersonating CISA Employees



What happened: The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has issued a warning against phone scammers utilizing names and titles to impersonate government employees, including CISA employees. CISA has emphasized that its staff will never request that individuals wire money, cash, cryptocurrency, or gift cards or issue instructions to keep a discussion secret.

- **What this means:** CISA’s warning reflects a concerning escalation in scam tactics, whereby fraudsters are leveraging the credibility of government agencies to trick individuals into financial losses. CISA recommends that individuals who suspect they are being targeted by a scammer impersonating a CISA employee take note of the phone number, hang up immediately, and validate the contact by calling CISA or report the call to law enforcement. Successful infiltration into systems with the scammed data can create opportunities for identity theft and fraud, potentially causing financial harm to affected individuals, or other forms of exploitation. Additionally, scammers may use the apparent legitimacy of government impersonations to further deceive individuals or perpetrate subsequent scams.

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

New BreachForums-Associated Telegram Channels Appear Following Deletion of Prior One



What happened: On June 12, 2024, the Telegram channel associated with prominent underground marketplace BreachForums, Jacuzzi, was removed and promptly replaced by Jacuzzi 3.0 and Jacuzzi 4.0. BreachForums was recently taken down in a multinational law enforcement operation that reportedly resulted in arrests of key figures. Jacuzzi 3.0 is reportedly being moderated by a threat actor called “Rose,” who has taken the place of previous moderator “ShinyHunters.”

- **What this means:** BreachForums has undergone a steady evolution following a series of takedowns and law enforcement operations aimed at curtailing the prominent underground marketplace. Following a takedown in 2023 that resulted in the arrest of then-moderator “Pompompurin,” the site reconstituted using a series of domains to evade scrutiny. In addition to utilizing Telegram and other social media platforms to reconstitute the marketplace, [prominent threat actor “USDoD” reportedly plans to launch Breach Nation on July 4, 2024](#), and has made a concerted effort to draw as many former members of BreachForums to the new planned site. This evolution of BreachForums exemplifies the challenges in attempting to curtail underground activity. It also highlights the need for a multi-faceted approach to cybersecurity that does not rely upon law enforcement action to safeguard systems and data.

Threat Actor Conducts Cyberattack Against German Government



What happened: On June 11, 2024, the pro-Russian hacktivist group “NoName057(16)” claimed to have conducted a DDoS attack against German government sites. According to oName057(16)’s claim, which was posted on the group’s Telegram channel, the attack was carried out in response to and during Ukrainian President Zelensky’s visit to Germany. The group claimed to have struck websites belonging to the Federal Office of Logistics and Mobility, as well as the Federal Ministry of the Interior and

Homeland of Germany. It is unclear how long these sites were taken offline or otherwise degraded.

- **What this means:** Hacktivist group NoName057(16) has been highly active in recent months, carrying out attacks on their own and in cooperation with other like-minded hacktivists. As was the case with this DDoS attack, NoName057(16) frequently targets NATO

nations—including the United States—in support of Russia’s operations in Ukraine. While the DDoS attacks have, to date, caused minimal disruption to critical functions, these attacks are an easy way to bring attention to the attacker’s cause. Thus, ZeroFox assesses this tactic will remain popular with hacktivist groups.

Untested Threat Actor Advertised Access to a Taiwanese Telecommunication Company

What happened: On June 9, 2024, untested threat actor “Kelentovich” posted an offer to sell webshell access to an unspecified Taiwanese telecommunications company on the xss forum. The initial access broker did not specify a charge for the access and instead stated the price was open to negotiation. According to Kelentovich, the access contains 910 GB of unspecified data for a Taiwanese telecommunications company with an annual revenue of USD 7.2 billion. Of note, Kelentovich does not have a strong track record on xss.



- **What this means:** Access to a Taiwanese telecommunications company could lead to the leak of large amounts of sensitive data. While there is no indication that Chinese nation-state or nation-state-affiliated actors are behind this access, a leak of this magnitude would benefit China in its ongoing efforts to penetrate Taiwan’s critical infrastructure—of which the telecommunications sector is a large part. While Kelentovich did not state the name of the company, [open sources indicate that Taiwan Semiconductor Manufacturing Company \(TSMC\) has a current annual revenue of USD 7.2 billion](#). TSMC produces over half the world’s semiconductors; any significant data leak or attack on TSMC could have an exponential impact on the global economy. It is unclear if Kelentovich has legitimate access to TSMC or any other Taiwanese telecommunications company. ZeroFox will continue to monitor the dark web for indications of a compromise.

| Exploit and Vulnerability Intelligence |

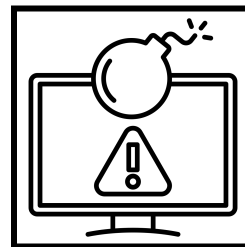
| Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox has observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in software solutions, networking, and government security domains. CISA has [added](#) three new vulnerabilities to its Known Exploited Vulnerabilities Catalog (KEV) based on evidence of active exploitation. These vulnerabilities could be attack vectors for malicious cyber actors and pose significant risks to federal enterprise. In its latest batch of Patch Tuesday updates, Microsoft has [released](#) fixes for 51 flaws (including one zero-day and five denial of service vulnerabilities). Additionally, threat actors have recently [exploited](#) a vulnerability patched by Microsoft in March. Meanwhile, discontinued Netgear WNR614 routers have been observed to contain [six](#) vulnerabilities that could allow threat actors to bypass authentication, intercept communications, and steal credentials. [Ivanti](#) has recently released a patch for CVE-2024-29824, a vulnerability that can allow remote attackers to execute arbitrary code on affected products of Ivanti Endpoint Manager.

Notable vulnerabilities:

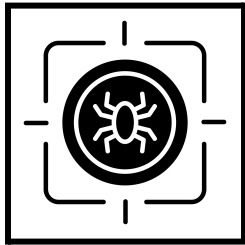
[CVE-2023-50868](#)

What happened: The Closest Encloser Proof aspect of the DNS protocol (in RFC 5155 when RFC 9276 guidance is skipped) allows remote attackers to cause a denial of service (CPU consumption for SHA-1 computations) via DNSSEC responses in a random subdomain attack, which is also known as the "NSEC3" issue.



- **What this means:** Microsoft assigned this **IMPORTANT**-severity vulnerability a score of 6.5. The RFC 5155 specification implies that an algorithm must perform thousands of iterations of a hash function in certain situations.
- **Affected products:**
 - Windows Server 2012 R2 (Server Core installation)
 - Windows Server 2012 R2
 - Windows Server 2012 (Server Core installation)
 - Windows Server 2012
 - Windows Server 2016 (Server Core installation)
 - Windows Server 2016
 - Windows Server 2022, 23H2 Edition (Server Core installation)
 - Windows Server 2022 (Server Core installation)
 - Windows Server 2022
 - Windows Server 2019 (Server Core installation)
 - Windows Server 2019

CVE-2024-32896



What happened: Google released a major Pixel security update warning that a patched vulnerability, CVE-2024-32896, has been exploited. This zero-day bug is a **HIGH**-severity elevation of privilege issue.

➤ **What this means:** Conform, a type-safe form validation library, allows the parsing of nested objects in the form of 'object.property'. Due to an improper implementation of this feature in versions prior to 1.1.1, an attacker can exploit the feature to trigger prototype pollution by passing a crafted input to 'parseWith...' functions. Applications that use Conform for server-side validation of form data or URL parameters are affected by this vulnerability. Version 1.1.1 contains a patch for the issue.

- **Affected products:**
- Pixel Firmware



ZEROFOX®

Weekly Intelligence Brief

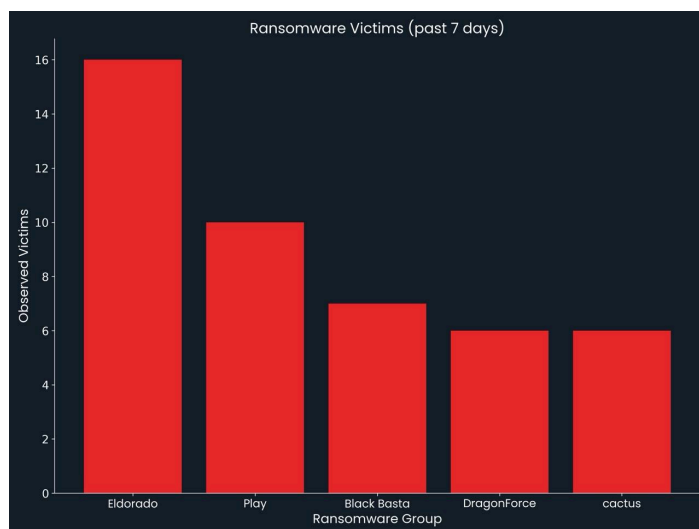
TLP:GREEN

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

Ransomware Intelligence: Eldorado and Play Account for Majority of Attacks

What happened: In the past seven days, ZeroFox has recorded over 85 ransomware attacks predominantly targeting the construction and manufacturing sectors. These attacks were primarily conducted by the Eldorado and Play ransomware groups; over 60 percent of the victims were located in North America and Europe. In other news, Panera Bread experienced a ransomware attack in late [March](#) that resulted in the encryption of its virtual machine systems. Besides [notifying](#) the employees, the company has also [informed](#) the office of California's Attorney General of the data breach and is currently investigating the incident with external cybersecurity experts. Meanwhile, RansomHub has



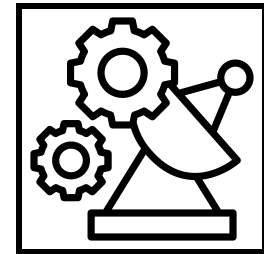
Source: ZeroFox Internal Collections

recruited "Scattered Spider" (a notorious actor associated with a string of attacks targeting popular casinos last year) into its ranks. The recruitment drive comes as an effort to capitalize on the situation caused by the collapse of the BlackCat/ALPHV RaaS operation, leaving affiliates without owed payments and infrastructure. A Ukrainian man was [arrested](#) for his role as a freelance developer for the Russian ransomware groups Conti and LockBit. The Toronto District School Board (TDSB) has [reported](#) a ransomware attack on its software testing environment and is currently investigating potential exposure of personal information.

- **What this means:** Panera's ransomware attack highlights the ongoing threat posed by cybercriminals to businesses, potentially disrupting operations and compromising sensitive data. With the stolen data, threat actors can potentially engage in identity theft, fraud, or sell the information on the dark web. Personal information like names and Social Security numbers can be used to open fraudulent accounts, apply for loans, or conduct other criminal activities. Panera is offering affected individuals a one-year membership to credit monitoring, identity detection, and identity theft resolution services. This step will help the affected individuals by providing continuous monitoring of their credit reports for any suspicious activity, early detection of identity theft attempts, and assistance in resolving any identity theft issues that may arise.

Breach Intelligence: 750,000 Individuals' Data Stolen in Frontier Communications Attack

What happened: American telecommunications company Frontier Communications has disclosed that a data breach (which was reported in the April 20 [issue](#) of ZeroFox's Cyber Intelligence Daily Brief) affected over 750,000 individuals and exposed sensitive customer data, such as Social Security numbers, addresses, dates of birth, credit scores, and phone numbers. Meanwhile, ZeroFox [observed](#) a post on the RansomHub ransomware leak site targeting Frontier Communications, with a claim to have stolen two million customers' data. In other news, Pure Storage [confirmed](#) a breach involving its Snowflake data analytics workspace, adding to the list of victims affected in the Snowflake cyberattack. Cybersecurity company Cylance is [investigating](#) reports of a data breach that allegedly exposed 34 million emails and other sensitive data relating to customers, partners, and employees. In the financial world, Truist has [confirmed](#) that its systems were breached in an October 2023 cyberattack.

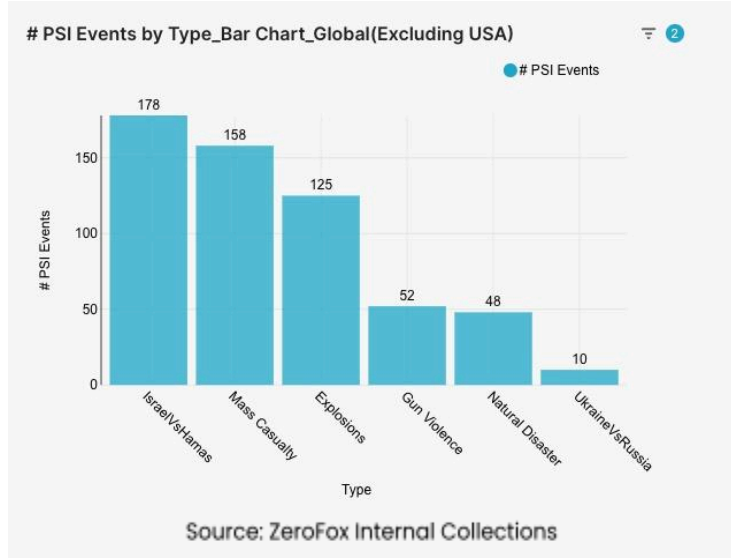


- **What this means:** The exposed personal data from Frontier Communications creates opportunities for identity theft and fraud, potentially causing financial harm to affected individuals. Additionally, the stolen data can be leveraged for future cyberattacks, including phishing scams, targeted malware distribution, and exploitation of the compromised information to gain unauthorized access to accounts or to perpetrate further breaches. Furthermore, the RansomHub ransomware group's approach to selling stolen data, similar to their tactics following the British auction house Christie's [attack](#) last month, indicates a pattern of criminal behavior aimed at monetizing illicitly obtained information. Meanwhile, the FCC has [proposed](#) new rules for internet routing security, requiring broadband providers to report their efforts in addressing vulnerabilities in the Border Gateway Protocol (BGP).

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

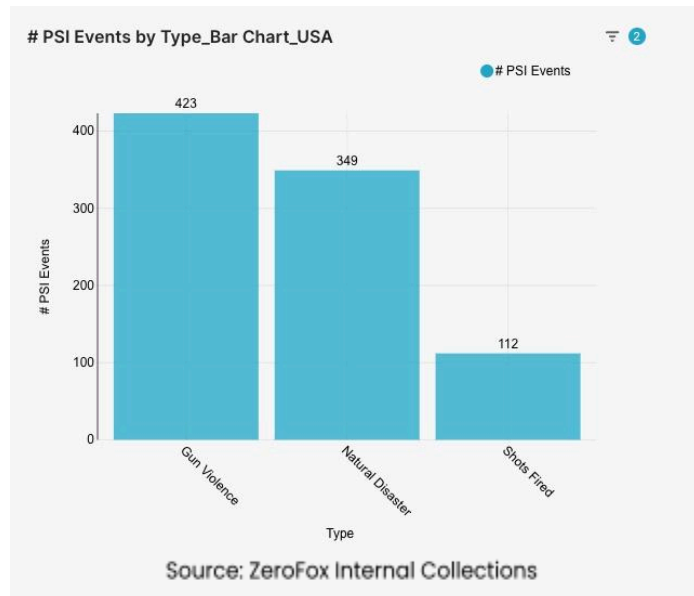
Physical Security Intelligence: Global



What happened: Excluding the United States, there was a 6 percent increase in mass casualty events this week from the previous week, with the top contributing countries being Palestine, Israel, and Lebanon (in that order); approximately 79 percent of these events were explosions. General alerts related to the Israel-Hamas War (including protests, raids, and involvement in neighboring countries) decreased by 12 percent from the

previous week. Additionally, events related to Russia's war in Ukraine remained static. The top three most-alerted subtypes were explosions, which saw a 10 percent increase from the previous week; gun violence, which decreased by 32 percent; and natural disasters, which increased by 26 percent.

- **What this means:** Both mass casualty alerts as well as explosions increased this week, which is understandable as explosions make up such a large portion of overall mass casualty events. This week, Israeli forces have [killed](#) Taleb Abdullah, the most senior Hezbollah commander; in response, Hezbollah fired more than 200 missiles and rockets across its southern border on Wednesday in one of its heaviest attacks on northern Israel since the 2006 war. These events and others explain why Israel and Lebanon are the second and third-leading countries in mass casualty events this week. Although gun violence decreased overall, Mexico is still the highest contributing country—despite its election season being over. This is likely due to the ongoing gang violence the country has seen; recently, there were mass [killings](#) in both Leon and Acapulco. Once again, [India](#) was the top contributing country this week in the natural disaster subtype, accounting for 19 percent of international natural disaster alerts. The country continues to experience both severe heat waves as well as monsoons, which are causing floods and other disruptions. The monsoon is expected to continue its expansion this week as well.



Physical Security

Intelligence: United States

What happened: In the past week, the top three most-alerted incident subtypes were gun violence, natural disaster, and shots fired. Gun violence alerts are instances in which there is a confirmed or likely confirmed victim, whereas shots fired alerts encompass shootings that did not result in a victim. The top two states that had the most gun violence alerts were Illinois and California, which together made up almost one-third of this week's nationwide total (29 percent).

Gun violence across the United States

overall increased by 3 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 decreased by 6 percent. The shots fired subtype encompasses confirmed shootings in which there are no human victims; these events increased by 30 percent from the previous week. Illinois and New York were the top two contributing states.

- **What this means:** While gun violence and natural disasters remained the top two alerted subtypes, shots fired took third place, with cities such as New York City and Los Angeles accounting for a significant number of such instances. Densely populated areas such as these are more likely to see higher crime rates; for gun violence, the highest contributing city was Chicago. Last weekend alone, 10 people were [shot](#) and killed in Chicago, and more than 30 were wounded by gunfire. Many agree that both stronger law enforcement and more resources for underprivileged parts of the city must play a role in improving the situation, but it is unclear how much change these strategies can successfully bring about. Record heat temperatures have been seen in California this week, causing [wildfires](#) that have prompted evacuations and shut down major highways. New York has also seen an increase in fire activity, but these are mainly structure fires in New York City primarily caused by electrical issues and appliances.

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?	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%