



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

July 15, 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 July 12, 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 July 2024 Geopolitical Brief	2
ZeroFox Intelligence Assessment – Threats to the Republican National Convention	2
 Cyber Intelligence Key Findings	4
Hackers Call It Quits After Releasing Data Allegedly Associated with the Heritage Foundation	4
CISA and Partners Release Advisory on PRC State-Sponsored Group APT 40	4
U.S. Justice Department Disrupts Covert Russian Government-Operated Social Media Bot Farm	5
 Deep and Dark Web Intelligence Key Findings	7
Actor Claims to be in Possession of Windows Local Privilege Escalation Vulnerability	7
Actor Claims DDoS Attack Against U.S.-Based Newspaper	7
Pro-Russian Hacker Claims DDoS Attacks Against NATO	8
 Exploit and Vulnerability Intelligence Key Findings	10
CVE-2024-4577	10
CVE-2024-5910	11
 Ransomware and Breach Intelligence Key Findings	13
Ransomware Intelligence: New Eldorado Ransomware Targets VMware ESXi VMs	13
Breach Intelligence: Breaches Target Commercial Websites and NATO Portals	14
 Physical and Geopolitical Intelligence Key Findings	16
Physical Security Intelligence: Global	16
Physical Security Intelligence: United States	17
 Appendix A: Traffic Light Protocol for Information Dissemination	18
 Appendix B: ZeroFox Intelligence Probability Scale	19

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence July 2024 Geopolitical Brief

Despite achieving concessions from the Kenyan government on avoiding tax increases, further protests are likely that threaten the leadership of President Ruto. Venezuelan President Nicolas Maduro is very likely to interfere in the late July elections, which increases the probability that the international community will not recognize the results. A continued low level of fighting in Gaza is more likely in the short term than a new war between Israel and Hezbollah. China's coast guard has become increasingly aggressive in targeting its neighbors over territorial disputes. China's Third Plenum will likely see economic stimulus to boost the struggling economy, as well as new efforts to protect Chinese industries from Western trade sanctions; however, major changes that please international investors are unlikely. The British elections saw the ruling conservatives lose power to the Labour party, but the bigger political development could involve smaller parties hoping to establish a footprint. The French elections look likely to result in an embarrassing loss for President Macron, but the expected political paralysis could benefit him in the long run. Security forces are concerned about terror attacks on the Paris Olympics, while the French public is largely disillusioned with hosting the Games.

ZeroFox Intelligence Assessment – Threats to the Republican National Convention

The Republican National Convention (RNC) will be held at the Fiserv Forum in downtown Milwaukee, Wisconsin, from July 15-18, 2024. According to local officials, approximately 50,000 delegates, guests, and media members are expected to visit the city for the event, in addition to thousands of protesters. Wisconsin is likely to be a hotly contested state in the upcoming November 2024 presidential election, with Milwaukee being a Democratic stronghold. In 2020, President Joe Biden carried the state by only slightly more than 20,000 votes after Trump won the state in 2016. In this heated political atmosphere, left-leaning protest groups have vowed to carry out demonstrations that could lead to confrontations with police and security personnel.

| Cyber Intelligence |

Cyber Intelligence Key Findings

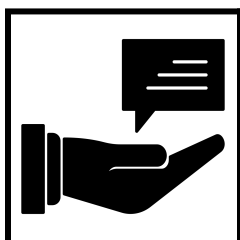
Hackers Call It Quits After Releasing Data Allegedly Associated with the Heritage Foundation

What happened: “SiegedSec”, a hacktivist collective, released 2 GB of data supposedly associated with the American conservative think tank Heritage Foundation. This data dump included full names, email addresses, passwords, and usernames of individuals linked to the organization. SiegedSec’s campaign, dubbed OpTransRights, targets entities supporting anti-trans and anti-abortion laws. The group targeted the Heritage Foundation supposedly due to its Project 2025 plans, perceived as a blueprint for far-right reforms under Donald Trump. Soon after announcing the leak, the group [posted](#) its plans for disbandment on its Telegram channel, adding it is trying to avoid the attention of law enforcement.



- **What this means:** SiegedSec has been implicated in attacks on the North Atlantic Treaty Organization (NATO) and [Idaho National Laboratory \(INL\)](#), a major nuclear lab in the United States. The collective has cited Project 2025—an initiative from the Heritage Foundation comprising a collection of conservative policy proposals—as the reason for targeting the think tank. The motivation and the nature of the attack showcase the increasing role of politically motivated hacktivism, whereby hackers target organizations to promote social and political agendas—in this case, purportedly trans rights and opposition to anti-abortion laws. The group seemingly declared its plan to disband after an online altercation between the admins and the executive director of Heritage Foundation. SiegedSec’s disbandment announcement, if genuine, may temporarily ease the pressure on targeted institutions. However, whether the group will disband is currently difficult to affirm. Additionally, the exposure of sensitive personal data, including names, emails, and passwords, can incite more politically motivated cyberattacks targeting the owners of the data.

CISA and Partners Release Advisory on PRC State-Sponsored Group APT 40



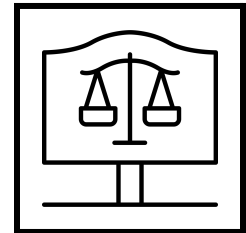
What happened: The Cybersecurity and Infrastructure Security Agency (CISA) and other global security agencies have [released](#) an advisory titled “People’s Republic of China (PRC) Ministry of State Security APT40 Tradecraft in Action.” The advisory provides information about PRC state-sponsored cyber group APT40 (also known as Kryptonite Panda, GINGHAM TYPHOON, Leviathan, and Bronze Mohawk). CISA urges all organizations and software

manufacturers to review the advisory to help identify, prevent, and remediate APT 40 intrusions.

- **What this means:** According to the advisory, this group appears to prefer exploiting vulnerable, public-facing infrastructure over techniques that require user interaction, such as phishing campaigns and places a high priority on obtaining valid credentials to enable a range of follow-on activities. The PRC state-sponsored cyber group has previously targeted organizations in various countries, including Australia and the United States, and the techniques highlighted in the advisory are regularly used by other PRC state-sponsored actors globally. The collaborating security agencies believe the group poses a threat to their countries' networks as well.

U.S. Justice Department Disrupts Covert Russian Government-Operated Social Media Bot Farm

What happened: The U.S. Department of Justice (DOJ) has announced the seizure of two domain names and investigated nearly 1,000 social media accounts linked to a Russian-operated, artificial intelligence (AI)-driven bot farm. This campaign utilized AI to fabricate fake social media profiles, often posing as Americans, to spread pro-Russian propaganda and disinformation. The Federal Bureau of Investigation (FBI) and the Cyber National Mission Force (CNMF), in collaboration with global allies, issued a joint cybersecurity [advisory](#) that outlines the technology used by the social media bot farm, including insights into how its operators utilized a customized AI system to advance its disinformation campaign. X (formerly Twitter) also suspended additional bot accounts identified in the operation for violating terms of service.

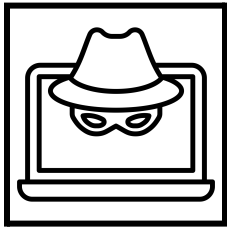


- **What this means:** The U.S. government's disruption of a Russian government-backed, AI-enabled propaganda campaign stopped a potentially significant threat posed by global disinformation campaigns. These operations undermine trust and security on widely used social media platforms, leading to potential financial losses and the widespread dissemination of false information. The infiltration of social media by AI-generated profiles can erode public confidence in the information they consume, which can destabilize trust in key systems. These efforts illustrate DOJ's readiness to confront misuse of AI by malign actors, emphasizing international cooperation and private sector collaboration.

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

Actor Claims to be in Possession of Windows Local Privilege Escalation Exploit



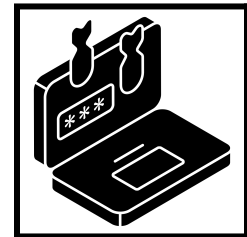
What happened: On July 6, 2024, threat actor “tikila” claimed to sell a Windows Local Privilege Escalation (LPE) vulnerability on the dark web forum BreachForums. The threat actor stated that the exploit has been tested and confirmed to work on Windows 10, Windows 11, and various Windows Servers (2008, 2012, 2016, 2019, 2022). The actor has requested interested parties to contact them via TOX.

- **What this means:** Windows operating systems account for approximately 27 percent of operating system market share globally.¹ A previously undisclosed LPE vulnerability can put systems at risk. Undisclosed vulnerabilities are particularly dangerous as there are no patches or mitigations available, allowing attackers to exploit them undetected. This particular vulnerability has a wide impact area as it affects Windows 10, Windows 11, and various Windows Servers (2008, 2012, 2016, 2019, 2022) operating systems.

Actor Claims DDoS Attack Against U.S.-Based Newspaper

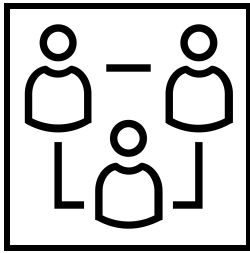
What happened: On July 8, 2024, threat actor group “SN_Blackmeta” claimed to have conducted a distributed denial-of-service (DDoS) attack against *The Washington Times*, a U.S.-based newspaper. The attack allegedly lasted between four and five hours.

- **What this means:** A DDoS attack on a U.S.-based news organization like *The Washington Times* has significant implications beyond the immediate disruption of services. As a prominent conservative daily in Washington, D.C., known for its influential political commentary, such an attack not only silences a voice in the media landscape but also exposes vulnerabilities in digital infrastructure critical to free speech and public discourse. The attack suggests a deliberate targeting of institutions pivotal in shaping political narratives and public opinion, potentially signaling a broader campaign to undermine information dissemination in a country that prides itself on democratic values and freedom of expression.



¹ [hXXps://gs.statcounter\[.\]com/os-market-share](https://gs.statcounter.com/os-market-share)

Pro-Russian Hacker Claims DDoS Attacks Against NATO



What happened: On July 10, 2024, pro-Russian hacktivist group “Noname057(16)” claimed to have conducted DDoS attacks on several NATO entities with the help of the group’s factions and alliances. The group allegedly carried out attacks on two direct NATO entities, the Northern European Command’s Command and Control Information System (NEC CCIS) and the Munition Safety Information Analysis Center (MSIAC), and one global think tank, Globsec. These entities are co-organizing the NATO Public

Forum set to take place at the NATO Summit on July 10-11, 2024.

- **What this means:** The recent claims by NoName057(16), “Russian Cyber Army”, and “UserSec” of targeting multiple NATO websites are significant due to the impact on critical NATO infrastructure and operations. These cyberattacks, which are predominantly DDoS attacks, aim to disrupt essential functions across various domains, including crisis management, scientific research, command and control systems, and munitions safety. The targeted websites represent key NATO capabilities and allied organizations spanning multiple countries, indicating a coordinated effort to undermine NATO’s digital presence and potentially compromise sensitive information.

| Exploit and Vulnerability Intelligence |

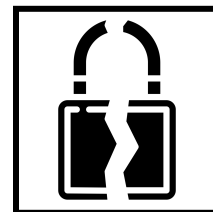
| Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox has observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in software solutions, networking, and government security domains. CISA has [added](#) three new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. Microsoft [released](#) its monthly security updates and addressed 143 security flaws, including two actively exploited vulnerabilities. The two exploited flaws are [CVE-2024-38080](#) (Hyper-V Elevation of Privilege) and [CVE-2024-38112](#) (MSHTML Platform Spoofing). Researchers have [observed](#) hackers exploiting CVE-2024-5441 in the Modern Events Calendar plugin on over 150,000 websites, aiming to upload files and execute remote code. A critical vulnerability in the Ghostscript document conversion toolkit, tracked as CVE-2024-29510, [affects](#) Ghostscript versions 10.03.0 and earlier. It is being exploited in the wild to conduct remote code execution (RCE). A new ransomware group is [exploiting](#) a high-severity bug, CVE-2023-27532, in the Veeam Backup & Replication component. GitLab has [issued](#) critical updates addressing security flaws in its platform, notably CVE-2024-6385 with a CVSS score of 9.6. CVE-2024-6409, present in select OpenSSH versions and distinct from the earlier CVE-2024-6387 (RegreSSHion), [poses](#) a significant RCE risk due to a race condition in signal handling within the privsep child process. Recently [disclosed](#) vulnerabilities in Gogs, a self-hosted Git service, reveal four unpatched security flaws, three of which are critical. Adobe has [released](#) security updates to address multiple vulnerabilities in Adobe software. Meanwhile, Citrix has also [released](#) security updates to address vulnerabilities in multiple Citrix products. Palo Alto Networks [issued](#) updates to fix five security flaws—including CVE-2024-5910 (CVSS 9.3), which allows attackers to take over admin accounts in the Expedition tool.

Notable vulnerabilities:

[CVE-2024-4577](#)

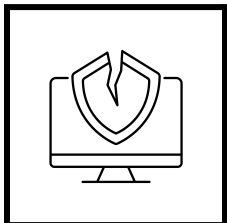
What happened: When using Apache and PHP-CGI on Windows in PHP versions 8.1. before 8.1.29, 8.2. before 8.2.20, and 8.3. before 8.3.8, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in the command line given to Win32 API functions. The PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run and thus reveal the source code of scripts, run arbitrary PHP code on the server, et cetera.



- **What this means:** This **CRITICAL**-severity vulnerability allows an attacker to remotely execute malicious commands on Windows systems using Chinese and Japanese language locales.
- **Affected products:**

- In PHP versions 8.1.
- before 8.1.29, 8.2.
- before 8.2.20, 8.3.
- before 8.3.8

CVE-2024-5910



What happened: Missing authentication for a critical function in Palo Alto Networks Expedition can lead to an Expedition admin account takeover for attackers with network access to Expedition. This vulnerability causes configuration secrets, credentials, and other data imported into Expedition to be at risk.

➤ **What this means:** The company has not detected any exploitation of this **CRITICAL** bug in the wild and has reportedly fixed this issue in Expedition 1.2.92 and all later versions. Palo Alto advises users to restrict access to authorized users, hosts, or networks.

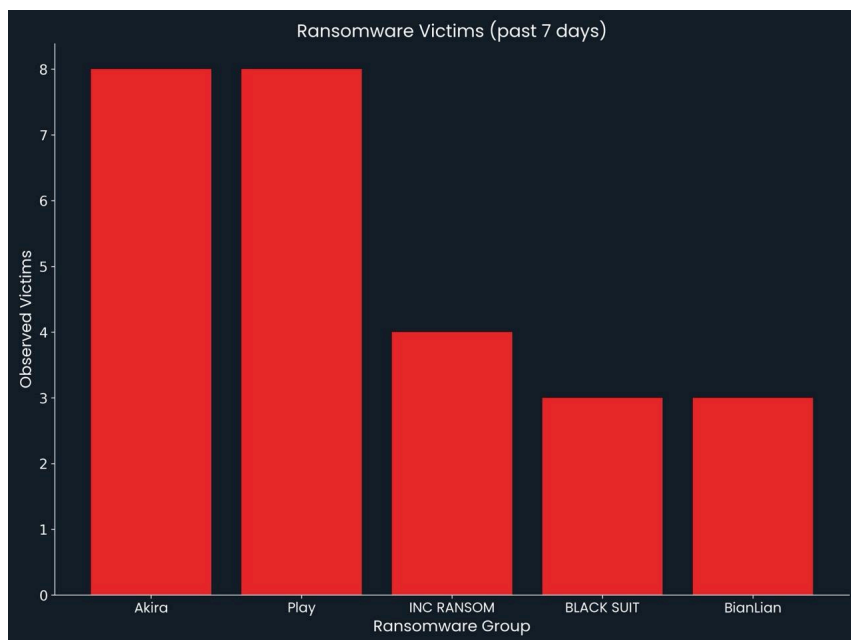
➤ **Affected products:** All versions of Expedition prior to version 1.2.92

| Ransomware and Breach Intelligence |

Ransomware and Breach Intelligence Key Findings

Ransomware Intelligence: New Eldorado Ransomware Targets VMware ESXi VMs, Among Other Ransomware Attacks

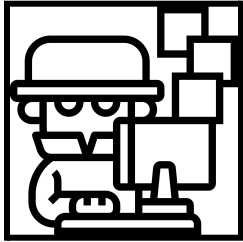
What happened: The “Eldorado” ransomware group has been observed targeting various systems (including VMware ESXi hypervisors) using ChaCha20 and RSA encryption, appending “.00000001” to encrypted files and leaving “HOW_RETURN_YOUR_DATA.TXT” ransom notes on the compromised systems. It encrypts network shares via SMB, deletes shadow copies, and self-deletes to evade detection. On June 7, ZeroFox [identified](#) Eldorado’s new leak site. In other news, the American Radio Relay League (ARRL) has confirmed that a ransomware attack in [May](#) resulted in the theft of data belonging to some of its employees. Evolve Bank & Trust [reported](#) in a recent submission to Maine’s attorney general that the data of over 7.6 million customers was compromised during the LockBit attack in late [May](#). ZeroFox has also observed over 45 ransomware attacks in the past seven days, mostly on the manufacturing sector and primarily conducted by the “Akira” and “Play” ransomware groups. Over 65 percent of these victims are located in North America.



Source: ZeroFox Internal Collections

- **What this means:** Eldorado's use of strong encryption algorithms and RSA for key management highlights the increasing sophistication of ransomware techniques, posing severe threats to organizations across multiple critical sectors. Its deliberate targeting of VMware ESXi environments underscores the ransomware's adaptation to enterprise infrastructures, potentially causing widespread operational disruptions and data loss. Furthermore, RansomHub, a ransomware-as-a-service (RaaS) operation, was also [observed](#) utilizing a Linux encryptor tailored for encrypting VMware ESXi environments in corporate attacks. Threat actors target VMware ESXi environments due to their prevalence in corporate infrastructures, aiming to maximize impact and ransom yield. This specialized focus disrupts critical operations, demands significant recovery efforts, and potentially results in substantial financial losses for affected organizations.

Breach Intelligence: Breaches Target Commercial Websites and NATO Portals



What happened: ZeroFox intelligence has observed threat actor SiegedSec claiming to have breached the NATO Consultation, Command, and Control (C3) portal. Additionally, several other adversaries have been observed forming alliances to target NATO amid the 2024 Washington summit held from July 9 to July 11. On July 9, threat actor “randomdev” [claimed](#) to have leaked a database associated with Angel One, an India-based stock brokering and online trading platform, on the predominantly

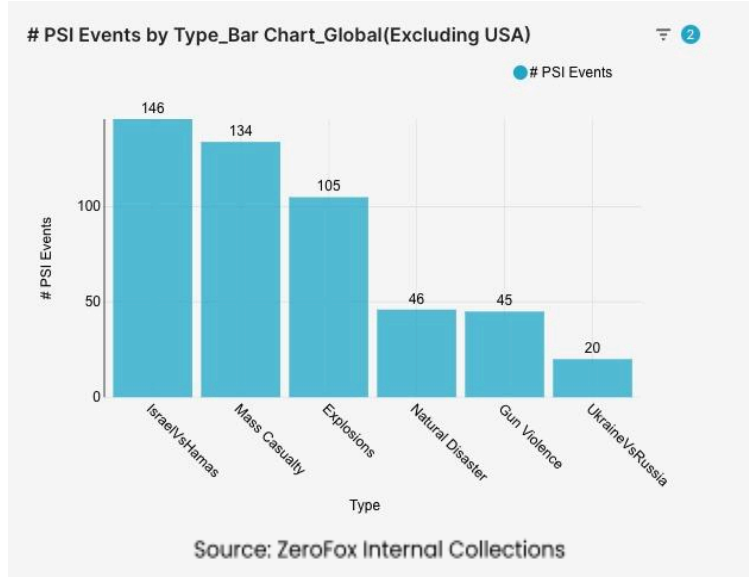
English-language dark web forum BreachForums. The leaked package contains data from 7,901,612 users, 1.2 million stock holding records, and 1.6 million users' profit and loss (PNL) information. Another notable data breach that made headlines [impacted](#) the United Arab Emirates' (UAE) Lulu Hypermarket, exposing the personal details of over 200,000 customers. ZeroFox intelligence [observed](#) threat actor “IntelBroker” claim responsibility for the breach, leaking email addresses and phone numbers allegedly associated with Lulu Hypermarket as proof. IntelBroker asserts it has possession of the full database, potentially containing millions of user and order details, and plans to release it later.

- **What this means:** Most of the actors, including hacktivists, targeting NATO are politically motivated. SiegedSec has stated its support for the Palestinian cause to be the motivation behind its attack. In a Telegram post, the group states it was apparently able to access “tens of thousands documents.” As for the Angel One incident, the exposure of such a large volume of sensitive financial data raises significant concerns about the security practices of Angel One and potentially other financial institutions. Similarly, the breach impacting Lulu Hypermarket poses a substantial risk to its customers. Both breaches can potentially lead to identity theft, fraud, extortion scams, spear-phishing attacks, and other malicious activities. The hackers might demand ransom, sell the data, or release it publicly, amplifying the threat.

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

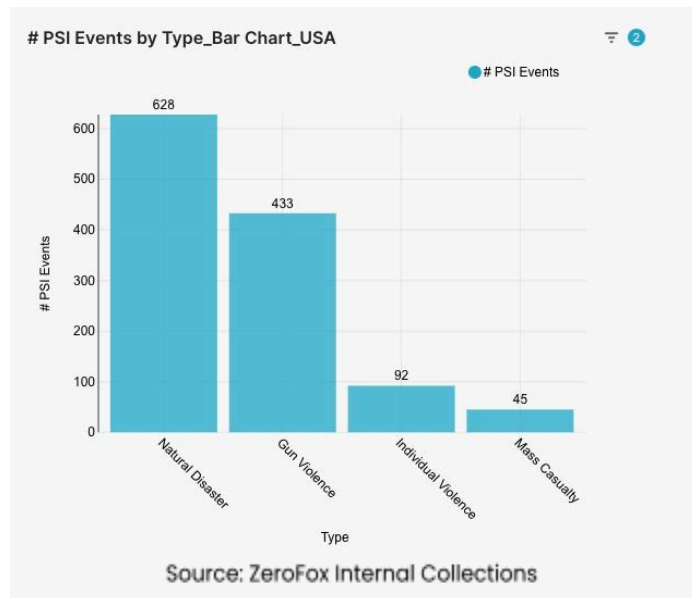
Physical Security Intelligence: Global



What happened: Excluding the United States, there was a 15 percent decrease in mass casualty events this week from the previous week, with the top contributing countries being Palestine, Israel, and Lebanon; approximately 78 percent of these events were explosions. General alerts related to the Israel-Hamas War (including protests, raids, and involvement in neighboring countries) decreased by 10 percent

from the previous week. Conversely, events related to Russia's war in Ukraine increased by 33 percent. The top three most-alerted subtypes were explosions, which saw a 19 percent decrease from the previous week; natural disasters, which increased by 28 percent; and gun violence, which decreased by 18 percent.

- **What this means:** The largest percentage increase this week pertained to events related to the Ukraine-Russia conflict, mainly due to Russia's escalation of attacks in civilian locations. This week saw the heaviest bombardment of [Kyiv](#) in four months, which killed at least 31 people, wounded 150, and hit a children's hospital. The Russian Defense Ministry has denied aiming at any civilian facilities and has claimed that the damage was instead caused by a Ukrainian air defense missile (although there is no evidence to corroborate this). On Tuesday, U.S. President Joe Biden announced plans to supply new air defenses to Ukraine in a speech opening the [NATO](#) summit. Natural disasters increased this week as well; while Hurricane Beryl has mostly moved into the United States, other areas of the world are still experiencing extreme weather. Landslides on [Indonesia](#)'s Sulawesi Island following torrential rain have killed at least 11 people and left dozens missing. Similarly, intense monsoon storms battered [India](#) on Monday, flooding parts of Mumbai, while lightning in Bihar killed at least 10 people. As climate change shows no signs of slowing, more such events are likely around the globe in the future.



Physical Security

Intelligence: United States

What happened: In the past week, the top three most-alerted incident subtypes were natural disasters, gun violence, and individual violence. 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 individual violence refers to instances of stabbing. The top two states that had the most gun violence alerts were Illinois and California, which together made up over one-third of this week's

nationwide total (34 percent; the week prior was 28 percent). Gun violence across the United States overall increased by 30 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 44 percent. Individual violence alerts decreased by 12 percent, and the top contributing states were California and New York as well.

- **What this means:** Gun violence this week increased significantly—as did the percentage of total gun violence alerts, which came from Illinois and California. This can largely be attributed to the Fourth of July holiday weekend, which historically has been associated with higher levels of crime; just in [Chicago](#) alone, 109 people were injured and 19 were killed in shootings from Wednesday to Sunday this week, and three of these instances were mass shootings. Similarly, [California](#) recorded 68 shooting instances over the holiday weekend. Across the country, there were a total of 20 mass shootings—a shooting in which four or more people are shot and/or killed, not including the shooter—over the Fourth of July week this year. Natural disaster alerts also increased significantly, as Hurricane Beryl has now made its way into the United States. Beryl made landfall in [Texas](#) as a Category 1 hurricane on Monday morning, killing six people, and has been the cause of flash flood and tornado warnings in several other states as well. Overall, it has resulted in the loss of electricity for more than three million U.S. homes and businesses.

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%