



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

May 20, 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 May 17, 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 – BreachForums Marketplace Seized by Law Enforcement	2
ZeroFox Intelligence Brief – LockBit Update: What Comes Next for the Extortion Collective?	2
ZeroFox Intelligence Flash Report – Fake Tether Cryptocurrency Tokens Announced for Sale	2
ZeroFox Intelligence Brief – Underground Economist: Volume 4, Issue 10	3
 Cyber Intelligence Key Findings	5
Europol: No Operational Information Stolen	5
Hack of French Sports Minister's X Account Highlights Olympics Cyberthreats	5
DOJ Indictment Charges Two Brothers for Stealing USD 25 Million in Ethereum Blockchain Attack	6
 Deep and Dark Web Intelligence Key Findings	8
Threat Actor Claims to Sell Zero-Day RCE Exploit for Microsoft Outlook	8
GhostSec Shifts from Cybercrime to Hacktivism	8
Pro-Russian Hacktivist Group Conducts DDoS Attack in Denmark	9
 Exploit and Vulnerability Intelligence Key Findings	11
CVE-2024-23296	11
CVE-2024-30051	12
 Ransomware and Breach Intelligence Key Findings	14
Ransomware Intelligence: MediSecure e-Script Firm Hit by Ransomware Data Breach	14
Breach Intelligence: WebTPA Hack Causes Sensitive Data Breach	14
 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 – BreachForums Marketplace Seized by Law Enforcement

On May 15, 2024, the popular English-language deep and dark web (DDW) forum BreachForums was seized in an operation likely coordinated by multiple international law enforcement (LE) agencies. Since mid-2023, BreachForums has been one of the most popular DDW marketplaces hosting discussions surrounding malicious network access and exploitation, as well as the trading of associated goods such as personally identifying information and personal financial information. ZeroFox can neither independently confirm nor deny that a spate of recent posts on the forum advertising the sale of highly sensitive information initiated the LE activity. ZeroFox notes the possibility that the LE operation is ongoing, with the potential for further disruption to occur.

ZeroFox Intelligence Brief – LockBit Update: What Comes Next for the Extortion Collective?

Increased pressure on LockBit's leadership following recent LE activity is likely to make the extortion operation more volatile and unpredictable in the short term and may have negative consequences for extortion victims. LockBit's ability to persuade other ransomware and digital extortion (R&DE) threat actors that one of its operation's purported leadership figures, "LockBitSupp," was incorrectly identified and that its affiliates' identities remain secure is very likely hindered by recent reputational damage and degraded credibility. LockBit's inability to maintain stable infrastructure will likely be perceived by many threat actors as evidence that LockBit's operation is on a declining trajectory and is indicative of its leadership focusing on brand restoration rather than operational efficacy. Should barriers persist and hinder LockBit's ability to restore its reputation—as well as continued degradation in operational output—the likelihood that leadership will seek to close down LockBit's operation will increase. R&DE operations of this nature have a history of ceasing activity via exit scams conducted by the operations' leadership teams.

ZeroFox Intelligence Flash Report – Fake Tether Cryptocurrency Tokens Announced for Sale

Since the beginning of May 2024, two advertisements for the sale of fake Tether ECR20 (also known as USDT) have been offered in DDW forums. Such announcements are historically uncommon, though there is a roughly even chance that demand for these services is increasing.

Threat actors seeking to acquire fake Tether ERC20 coins most likely intend to leverage them in malicious, fraudulent activity such as exchange or investment scams. These are often conducted via the establishment of a webpage imitating a legitimate cryptocurrency or investment platform. If threat actors are continually successful in leveraging fake cryptocurrencies for malicious purposes, it is likely that additional purchasing options will become available in DDW forums. This would very likely lead to an increased threat to both individuals and organizations that are either involved in cryptocurrency trading or accept it as tender.

ZeroFox Intelligence Brief – Underground Economist: Volume 4, Issue 10

On May 15, 2024, the popular English-language DDW forum BreachForums was seized in an operation likely coordinated by multiple international LE agencies. On May 8, 2024, threat actor “g77” stated in a post on the DDW community RAMP that they were seeking to obtain illicit access into the networks of global shipping entities. Since the beginning of May 2024, two advertisements for the sale of fake Tether ECR20 have been offered in DDW forums. On May 6, 2024, untested threat actor “Average” started a thread in the Russian-speaking DDW community Exploit advertising the development of a new artificial intelligence (AI)-powered one-time password (OTP) bot that can be leveraged in two-factor authentication (2FA) bypass attacks, as well as other social engineering activity.

| Cyber Intelligence |

Cyber Intelligence Key Findings

Europol: No Operational Information Stolen



What happened: Europol is investigating a data breach impacting its Europol Platform for Experts (EPE) wherein a threat actor exfiltrated For Official Use Only (FOUO) documents containing classified data. At the time of reporting, the website is offline and displays a message that the service is “not available at the moment due to maintenance activities.” A threat actor going by the moniker “IntelBroker” has claimed responsibility for the breach. The agency revealed that the threat actor reportedly gained access to the data using stolen credentials and not by exploiting a vulnerability or a misconfiguration. Europol has also conveyed to news outlets that “only a small and limited part of the EPE (closed user group) could be accessed” utilizing the stolen credentials.

- **What this means:** Europol has confirmed that the breach has had no impact on Europol core networks and exposed no operational data. However, as the European Union’s LE agency, classified Europol data exposed to threat actors could pose serious risks to the upcoming European Parliament elections. Adversaries might use the exposed data for spear phishing attacks targeting political entities or for misinformation or disinformation campaigns. The threat actor behind this attack, IntelBroker, is a cybercriminal group known for exfiltrating sensitive data. It has also allegedly orchestrated the recent hacks of General Electric and stolen sensitive military files belonging to the U.S. Defense Advanced Research Projects Agency (DARPA).

Hack of French Sports Minister’s X Account Highlights Olympics Cyberthreats

What happened: French Sports Minister Amélie Oudéa-Castéra’s X account (formerly Twitter) was hacked. Her profile photo was changed and bizarre messages were sent out, prompting concerns and intervention from both X and France’s cybersecurity agency (ANSSI) as Paris prepares to host the 2024 Olympics. The hack was immediately detected, and the account has been restored.



- **What this means:** The takeover of the French Sports Minister’s X account amid Olympic preparations sheds light on the potential vulnerabilities that major events like the Olympics face in the digital age. Hacktivists and threat actors across the world view these events as prime targets to disrupt proceedings and leave a mark on the global stage, aiming to steal sensitive data, conduct distributed denial-of-service (DDoS) or ransomware attacks paralyzing key systems, carry out phishing schemes targeting officials and participants, or

make political statements. The Olympics hosts a convergence of world players in a single location, providing threat actors of all political causes a chance to vie for attack vectors and make a global impact.

DOJ Indictment Charges Two Brothers for Stealing USD 25 Million in Ethereum Blockchain Attack



What happened: The U.S. Department of Justice (DOJ) has arrested two brothers for attacking the Ethereum blockchain and stealing USD 25 million of cryptocurrency. In an indictment released on May 15, the DOJ has charged them with conspiracy to commit wire fraud, wire fraud, and conspiracy to commit money laundering.

➤ **What this means:** The Pepaire-Bueno brothers exploited a flaw in MEV-Boost code, allowing them to see the contents of blocks before validators officially received them. Maximal extractable value (MEV) refers to the practice of extracting additional profits by manipulating transaction ordering and execution on blockchain networks such as Ethereum. This gave the Pepaire-Bueno brothers a strategic advantage in executing their attack, enabling them to steal USD 25 million in cryptocurrency from the Ethereum blockchain within a remarkably short timeframe of just 12 seconds. This indictment represents the first instance of the U.S. government taking legal action against MEV exploitation and indicates that MEV practices not only pose risks to users' assets but also challenge the foundational principles of decentralized systems.

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

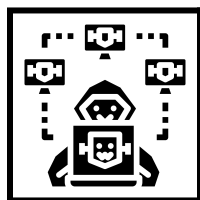
Threat Actor Claims to Sell Zero-Day RCE Exploit for Microsoft Outlook



What happened: On May 14, 2024, threat actor “Cvsp” claimed to be selling a zero-day Remote Code Execution (RCE) exploit for Microsoft Outlook on the predominantly English-language dark web forum BreachForums. The exploit reportedly targets x86/x64 versions of Microsoft Office 2016 and 2019, Microsoft Long-Term Servicing Channel (LTSC) 2021, and Microsoft 365 Apps for Enterprise. Cvsp offered to sell the exploit for USD 1.7 million, facilitated through escrow, and requested that any interested parties contact them via Telegram for additional details.

- **What this means:** ZeroFox has observed previous activity by Cvsp on only one other occasion: on April 18, 2024, the actor advertised the sale of a zero-day Local Privilege Escalation (LPE) exploit for Microsoft Windows for USD 150,000. While little is currently known about the actor’s intentions, capabilities, or credibility, individuals should ensure that they are running the most updated versions of all Microsoft products at all times out of an abundance of caution. This is especially true for those associated with U.S. government systems in light of the recent disclosure of breaches compromising the Outlook accounts of numerous top federal officials.

GhostSec Shifts from Cybercrime to Hacktivism



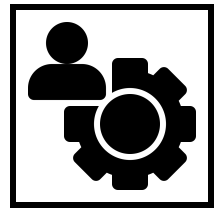
What happened: On May 15, 2024, threat actor group GhostSec, which has previously been involved in financially motivated cybercrimes, announced it would be returning to its original focus on hacktivism. As part of this transition, the group will discontinue its services; close its ransomware product, GhostLocker; and provide its code to its ally Stormous, ensuring a smooth exit without scams.

The threat actor announced that it has gathered sufficient funds through its past activities to support its operations moving forward. GhostSec stated it may offer a hacking course in the future as well.

- **What this means:** GhostSec will likely have an uptick in hacktivist attacks due to its shift in focus and having more time to dedicate to that type of attack. The group may also use new tactics in its hacktivist attacks to enhance its operations and set them apart from other hacktivist groups. It is also possible that Stormous may utilize the GhostLocker code to create its own variant for ransomware operations.

Pro-Russian Hacktivist Group Conducts DDoS Attack in Denmark

What happened: On May 15, 2024, the pro-Russian threat actor and hacktivist group “Cyber Army of Russia Reborn” claimed a DDoS attack against the European Conference of Postal and Telecommunications Administrations (CEPT) in Denmark. This attack is in line with recent hacktivist attacks whereby primarily European nations’ infrastructure is being targeted by DDoS attacks.



- **What this means:** Cyber Army of Russia Reborn is a new iteration of a group that became active at the outset of Russia’s invasion of Ukraine. The group, along with a number of others that work in concert against Russia’s adversaries, favors DDoS attacks against infrastructure targets in countries that support Ukraine. This and other like-minded hacktivist groups are likely to maintain a steady pace of similar attacks in the near term. While this attack was targeted against the Danish office of CEPT, it is noteworthy that CEPT has a role in coordinating telecommunications organizations throughout Europe, thus expanding the possible scope of the attack. ZeroFox has not observed any significant disruption to telecommunications in Denmark but will continue to monitor for effects from this attack.

| Exploit and Vulnerability Intelligence |

| Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox has observed vulnerabilities, exploits, and updates disclosed by prominent entities in software solutions, network security domains, and U.S. national security. After a hacking competition revealed notable vulnerabilities in widely used software systems, companies have been releasing security updates to address and patch these bugs. Microsoft has [documented](#) around 60 flaws in several of its software products and two actively exploited zero-day bugs ([CVE-2024-30040](#) and [CVE-2024-30051](#)) in its May Patch Tuesday updates. Apple has [released](#) security updates to address vulnerabilities in Safari, iOS, iPadOS, macOS, watchOS, and tvOS. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system. VMware has [disclosed](#) several vulnerabilities in VMware Workstation Pro / Player and VMware Fusion. Updates and workarounds are available to remediate these vulnerabilities in the affected VMware products. Cacti, an open-source network monitoring and fault management framework, has addressed a dozen security flaws, of which one (CVE-2024-25641) is a critical [remote](#) code execution bug and another (CVE-2024-29895) is a critical command [injection](#) vulnerability. Google has [rolled](#) out security updates addressing several security issues in its Chrome browser, including two zero-day vulnerabilities, CVE-2024-4671 and CVE-2024-4947. Intel has [published](#) 41 new security advisories addressing more than 90 vulnerabilities found in the company's products, of which CVE-2024-22476 has a severity score of 10 and allows an unauthenticated attacker to enable escalation of privilege via remote access. SSD has [released](#) an advisory addressing security vulnerabilities in DIR-X4860 allowing remote unauthenticated attackers to access the HNP port to gain elevated privileges and run commands as root.

Notable vulnerabilities:

[CVE-2024-23296](#)



What happened: CVE-2024-23296 is a memory corruption issue that was addressed with improved validation. This issue is fixed in iOS 17.4 and iPadOS 17.4. This **HIGH** severity vulnerability has been assigned a CVSS score of 7.8.

➤ **What this means:** An attacker with arbitrary kernel read and write capability may be able to bypass kernel memory protections. Apple is aware of a report that this issue may have been exploited. Users are required to either apply mitigations as per vendor instructions or discontinue use of the product if mitigations are unavailable.

Affected products:

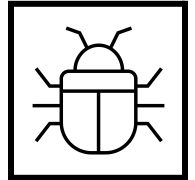
- Apple iPad OS versions below 17.4
- Apple iPhone OS versions below 17.4
- Apple macOS from version 14.4 to below 14.4

- Apple tvOS versions below 17.4
- Apple visionOS versions below 1.1
- Apple watchOS versions below 10.4

CVE-2024-30051

What happened: CVE-2024-30051 is an actively exploited Windows DWM Core Library flaw that lets an actor gain SYSTEM privileges. This vulnerability is actively being abused by several QakBot actors. The **HIGH** severity bug carries a CVSS score of 7.8.

➤ **What this means:** CVE-2024-30051 is a Windows DWM Core Library elevation of privilege (EoP) vulnerability enabling local attackers on a network to escalate to system privileges. When combined with an initial code-execution bug, it facilitates complete takeover of a target and lateral movement, often exploited by ransomware actors.



Affected products:

- Windows Server 2016 (Server Core installation)
- Windows Server 2016
- Windows 10 Version 1607 for x64-based Systems
- Windows 10 Version 1607 for 32-bit Systems
- Windows 10 for x64-based Systems
- Windows 10 for 32-bit Systems
- Windows 11 Version 23H2 for x64-based Systems
- Windows 11 Version 23H2 for ARM64-based Systems
- Windows 10 Version 22H2 for 32-bit Systems
- Windows 10 Version 22H2 for ARM64-based Systems
- Windows 10 Version 22H2 for x64-based Systems
- Windows 11 Version 22H2 for x64-based Systems
- Windows 11 Version 22H2 for ARM64-based Systems
- Windows 10 Version 21H2 for x64-based Systems
- Windows 10 Version 21H2 for ARM64-based Systems
- Windows 10 Version 21H2 for 32-bit Systems
- Windows 11 version 21H2 for ARM64-based Systems
- Windows 11 version 21H2 for x64-based Systems
- Windows Server 2022 (Server Core installation)
- Windows Server 2022
- Windows Server 2019 (Server Core installation)
- Windows Server 2019
- Windows 10 Version 1809 for ARM64-based Systems
- Windows 10 Version 1809 for x64-based Systems
- Windows 10 Version 1809 for 32-bit Systems



ZEROFOX®

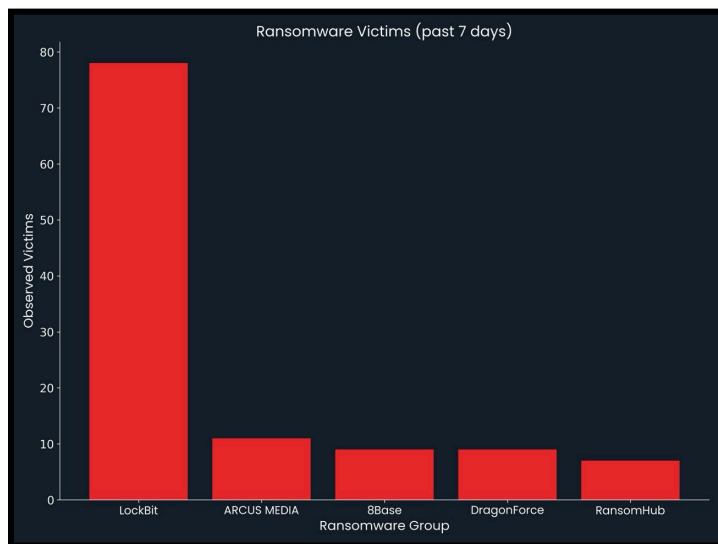
Weekly Intelligence Brief

TLP:GREEN

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

Ransomware Intelligence: MediSecure e-Script Firm Hit by Ransomware Data Breach



Source: ZeroFox Internal Collections

What happened: MediSecure shut down its operations due to a ransomware attack originating against a third-party vendor. Personal and health information of individuals has been compromised, and the extent of the breach is still unclear. The Australian Federal Police are investigating the incident. Meanwhile, CISA and its partners have released a joint cybersecurity [advisory](#) on BlackBasta that provides organizations with the tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) used by known Black Basta ransomware affiliates.

➤ **What this means:** MediSecure is one of Australia's main electronic prescription providers, issuing millions of electronic prescriptions; a ransomware attack compromising its systems with malicious software could likely lead to unauthorized access to sensitive personal and health information. With the increasing frequency of ransomware attacks targeting healthcare organizations, this breach could result in significant disruptions to healthcare services, potential loss or theft of personal data, and increased risks of identity theft or fraud for individuals whose information was compromised.

Breach Intelligence: WebTPA Hack Causes Sensitive Data Breach

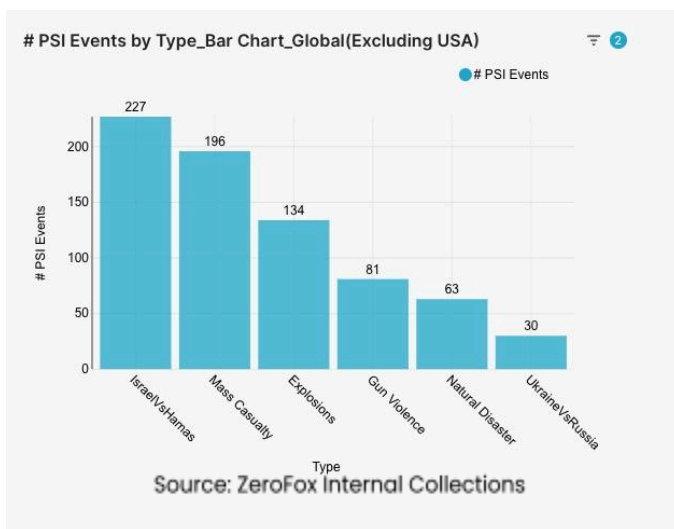
What happened: WebTPA Employer Services, a claims administrator for medical services, has disclosed a data breach on certain systems that affects more than 2.4 million patients. Discovered in 2023, the [breach](#) may have exposed personal information such as names, contact details, dates of birth and death, Social Security numbers, and insurance information. Financial and medical treatment information was not impacted, and clients have been notified.



➤ **What this means:** WebTPA is a third-party medical claims administrator that works in collaboration with other financial and insurance services. According to the breach notice,

WebTPA provides services to “certain benefit plans and insurance companies whose information was impacted in this incident.” The Hartford, a client of WebTPA, [confirmed](#) that its data for insureds enrolled in some of its services was stored in some of the affected systems.

| Physical and Geopolitical Intelligence |



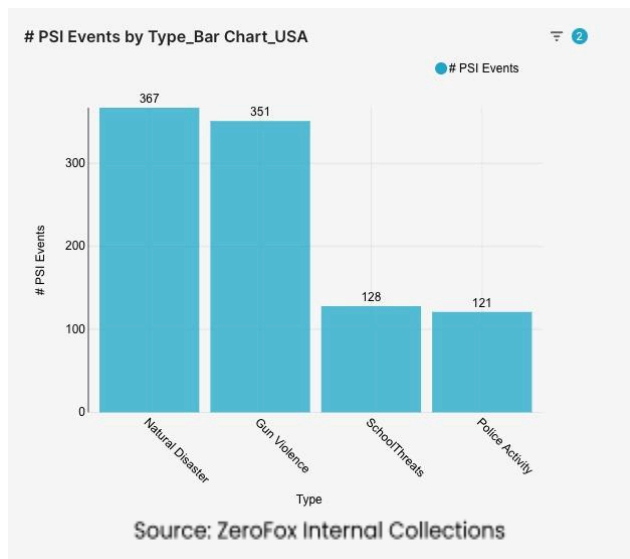
Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 2 percent decrease in mass casualty events this week from the previous week, with the top contributing countries being Palestine, Ukraine, and Israel (in that order); approximately 68 percent of these events were explosions.

General alerts related to the Israel-Hamas war (including protests, raids, and involvement in neighboring countries) increased by 3 percent from the previous week; notably, Palestine and Israel accounted for just under one half of all international explosions alerted (46 percent). Additionally, events related to Russia's war in Ukraine increased by 43 percent. The top three most-alerted subtypes were explosions, which saw a 11 decrease from the previous week; gun violence, which increased by 31 percent; and natural disasters, which increased by 21 percent.

- **What this means:** While mass casualty event numbers and Israel-Hamas war-related alerts remained relatively stable in the last two weeks, events related to Russia's war in Ukraine saw a definitive upward spike. This may be due to Russia's renewed [offensive](#) efforts in Kharkiv and Kyiv this week, which have caused Ukrainian troops to partially retreat from these areas as they do not have adequate weapons to defend themselves. Gun violence has also increased quite significantly since the previous week, with the top contributing country being Guatemala. Due to the prevalence of gang violence, as well as the upcoming presidential election of neighboring country, Mexico, both shootings and general instances of violence have increased; gangs with territory in both countries are using intimidation tactics to ensure that their favored political candidates have advantages. Finally, natural disasters saw an increase as well, with the top contributing country this week being Canada; this is due to numerous [wildfires](#) burning across the nation (over 130 total) that are causing air quality issues in both Canada and the United States.



Physical Security Intelligence: United States

What happened: In the past week, the top three most-alerted incident subtypes were natural disasters, gun violence, and police activity, in that order; this is the second week in a row that natural disasters have outnumbered gun violence alerts. Gun violence alerts are instances in which there is a confirmed or likely confirmed victim (i.e., not simply shots fired). The top two states that had the most gun violence alerts were California and Illinois, which together made

up almost one quarter of this week's nationwide total. Gun violence across the United States decreased by 10 percent from the week prior. The top two contributors to natural disaster alerts this week were Florida and California, and natural disaster alerts across the country decreased by 10 percent. The police activity subtype is used to alert evacuations, lockdowns, and heavy police presence for which the reason is not yet known at the time of alerting; California and Texas were the top two contributing states this week for this subtype, and police activity across the country as a whole increased by 3 percent. Alerts related to schools, excluding protests, decreased by 5 percent.

- **What this means:** Natural disasters outnumbering gun violence as the most alerted incident type this week is likely due to several instances of severe weather; [Florida](#) was the top contributor to this incident subtype due to several powerful thunderstorms, strong winds, and tornado warnings throughout the week. Gun violence events nationwide did decrease to some degree, but California and Illinois continue to be some of the top contributing states on a consistent basis due to their populated cities, like Los Angeles and Chicago. Both police activity and school-related threats showed a small decrease this week. The two subtypes are closely correlated, as a large portion of the police activity alerts are school-related instances (including events such as preemptive shooting threats and lockdowns); it is likely that both have decreased somewhat due to the school year coming to an end.

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%