



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

April 22, 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 April 19, 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
Flash Report – Bassterlord Returns to Sell Third Malicious Publication	2
Flash Report – Access to U.S. Web Hosting Organization Advertised in Deep and Dark Web Forum	2
Flash Report – Geopolitical and Cyber Risks of Iranian Attack on Israel	2
Intelligence Brief – Lengthy Indian Elections Present Cyber and Physical Threats	3
Intelligence Brief – Underground Economist: Volume 4, Issue 8	3
 Cyber Intelligence Key Findings	6
LockBit Strikes Unidentified Organization in West Africa with a New Variant	6
Hackers Hide Malicious Codes in Images to Target 320 Organizations Globally	6
Cisco Warns of Large-Scale Brute Force Attacks Against VPN Services	7
 Deep and Dark Web Intelligence Key Findings	9
Threat Actor Groups Announced Attack Against BreachForums	9
Threat Actor noob_iab Auctioning Network Access Bundle to 4,000 Servers Worldwide	9
Threat Actor Group “Red Evil” Claims Cyberattack Against Iran	10
 Exploit and Vulnerability Intelligence Key Findings	12
CVE-2024-3817	12
CVE-2024-20295	12
 Ransomware and Breach Intelligence Key Findings	16
Optics Giant Hoya Hit with USD 10 Million Ransomware Demand	16
Breach Intelligence: Actor Leaks Data from Ministry of Defense Israel	16
 Physical and Geopolitical Intelligence Key Findings	19
Physical Security Intelligence: Global	19
Physical Security Intelligence: United States	20
 Appendix A: Traffic Light Protocol for Information Dissemination	22
 Appendix B: ZeroFox Intelligence Probability Scale	23

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Flash Report – Bassterlord Returns to Sell Third Malicious Publication

On April 7, threat actor “Bassterlord” posted an advertisement on the deep and dark web (DDW) forum xss for a new educational manual, which allegedly assists threat actors in “organizing” mass brute force–targeting of corporations. The thread addresses multiple topics but was locked shortly after it was posted upon the author’s request. Bassterlord claims that, following the February 2024 law enforcement disruption of LockBit, their associated group, the National Hazard Agency (NHA), was under surveillance by the Federal Bureau of Investigation (FBI). This led to the seizure of all of NHA’s funds (including those stored in Monero, known as XMR) and the cessation of NHA’s operations.

ZeroFox Intelligence Flash Report – Access to U.S. Web Hosting Organization Advertised in Deep and Dark Web Forum

On April 8, 2024, an untested threat actor, “synthetic,” posted on the deep and dark web platform RAMP advertising access to a U.S.-based web hosting organization. Threat actor synthetic claims that the buyer will receive administrative access to all hosted web pages, which could number in the hundreds of thousands and belong to hundreds to thousands of separate organizations. The asking price for the initial access was USD 80,000, which is significantly higher than the typical price tag for initial access to an organizational network. This is almost certainly due to the notably high potential financial return for the successful exploitation of such significant access. Synthetic is not an active user in RAMP, but the advertisement indicates that sales will take place using the forum’s escrow service—significantly increasing the credibility of both the sale and the actor.

ZeroFox Intelligence Flash Report – Geopolitical and Cyber Risks of Iranian Attack on Israel

On April 13, Iran launched a massive, yet calibrated, attack on Israel in retaliation for an earlier Israeli strike on an Iranian consulate in Syria. Negative economic, geopolitical, and supply chain effects have been muted because markets already factored in the strike, which came with a two-week warning and deliberately avoided mass casualties. An immediate Israeli response that would widen the Israel-Hamas war is unlikely, but limited strikes against military positions belonging to Iranian allies across the Middle East are well within the realm of possibility. Ahead of the retaliation, ZeroFox identified cyber threat actors forming alliances with both Israel and Iran, which could escalate to cyberattacks on organizations on each side of the conflict. An Israeli-backed cyberattack on Iran is less likely, as Israel has historically focused its targeting on threats to its physical security.

ZeroFox Intelligence Brief – Lengthy Indian Elections Present Cyber and Physical Threats

India will hold a national parliamentary election from April 19 to June 1, with results expected on June 4. Prime Minister Narendra Modi is heavily favored to win a rare third term at the head of the Bharatiya Janata Party. Modi's pursuit of a landslide win against the fragmented opposition has led to accusations that he is intimidating political rivals and critics through the use of tax probes and legal cases. In the cyber realm, the election has been marked by the use of online influence campaigns and generative artificial intelligence (AI) to spur support for certain candidates. Several existing protest movements are unlikely to significantly interfere with the election but could spur heightened security and localized internet disruptions if they escalate during the drawn-out voting period. High tensions between India and its major neighbors, China and Pakistan, will likely play out through online influence campaigns, election-related hacktivism, and cyber infiltration rather than through direct physical conflict. At the same time, insurgents in both the Jammu and Kashmir territory and India's forested central belt could seek to stage small-scale attacks on electoral infrastructure.

ZeroFox Intelligence Brief – Underground Economist: Volume 4, Issue 8

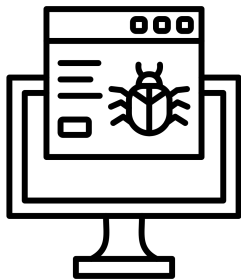
On April 15, BreachForums' surface web domain was taken down. Threat actor "R00TKIT", in alleged coordination with "CyberArmyofRussia", declared responsibility for the site's disruption several hours later in a Telegram post. On April 8, 2024, hacktivist group "SiegedSec" posted on its Telegram channel announcing the start of a new campaign dubbed Operation Trans Rights 2.

| Cyber Intelligence |

Cyber Intelligence Key Findings

LockBit Strikes Unidentified Organization in West Africa with a New Variant

What happened: According to researchers, LockBit has targeted an unidentified organization in



West Africa with a sophisticated attack leveraging a new variant of the LockBit 3.0 builder. Under the guise of being a system administrator, threat actors infected several of the victim's systems with the LockBit 3.0 builder variant. This new variant can generate custom, self-propagating ransomware to disable defense software on target systems, encrypt network shares, and bypass detection by deleting Windows Event Logs. The malware strain can also orchestrate attacks on select systems and corrupt documents or spreadsheets..

➤ **What this means:** Researchers came across the new variant in late March, initially labeling it Trojan-Ransom.Win32.Lockbit.gen, Trojan.Multi.Crypmod.gen, and Trojan-Ransom.Win32.Generic. It allows attackers to take over victims' systems using leaked privileged credentials. The incident in West Africa marks the only victim of this ransomware variant in this area. However, similar incidents have been detected elsewhere since the leaked builder surfaced in 2022. As the debate continues over the prevalence of LockBit in ransomware attacks, organizations can defend against such incidents by enforcing multifactor authentication, listing permitted applications, and establishing well-defined incident response plans.

Hackers Hide Malicious Codes in Images to Target 320 Organizations Globally

What happened: Researchers have observed threat actor "TA558" using images infected with malicious code to deploy malware tools on targeted systems in over 320 organizations globally. The campaign initiates with emails containing seemingly harmless attachments that exploit a seven-year-old patched remote control execution (RCE) vulnerability in Microsoft Office. The attachments comprise a Visual Basic Script (VBS) that fetches an image file (JPG). The image comes with PowerShell code that downloads the final payload, delivering a diverse range of malware families. One way to fortify against this malware-delivery campaign is to update Microsoft Office to the latest versions.



- **What this means:** This particular malware delivery campaign makes use of Steganography, a sophisticated method for embedding data covertly within files that seemingly appear innocuous. Emails are dispatched from compromised SMTP servers, bypassing security measures by masquerading as authentic communications. Exploiting vulnerabilities in outdated Microsoft Office versions, the attack retrieves a VBS from a trusted source, initiating a process that fetches a JPG file containing encoded payloads. PowerShell within the image then accesses a text file housing a reversed base64-encoded executable. To further hide its activities, the malware strain utilizes popular cloud platforms such as Google Drive. The stolen data is disguised as ordinary traffic and is stealthily transmitted to compromised FTP servers.

Cisco Warns of Large-Scale Brute Force Attacks Against VPN Services

What happened: Cisco has warned of a large-scale credential brute-forcing campaign that is targeting VPN and SSH services on devices worldwide. The attackers use a combination of valid



and generic employee usernames related to specific organizations in order to gain access to the internal network or hijack a device. The affected devices are manufactured by multiple companies, including Cisco, CheckPoint, Fortinet, SonicWall, and Ubiquiti.

- **What this means:** According to researchers, the attack is not specific to any particular industry or region and seems to employ a random, opportunistic strategy. Some of the tools used to conduct the attacks include TOR, VPN Gate, IPIDEA Proxy, BigMama Proxy, Space Proxies, Nexus Proxy, and

Proxy Rack. Meanwhile, Cisco has cautioned its customers about a social engineering [cyberattack](#) targeting a third-party telephony provider for its Duo multi-factor authentication (MFA) service. Threat actors allegedly compromised employee credentials to access the provider's systems and downloaded SMS logs for specific users within a certain period. Cisco has advised impacted users to stay vigilant against follow-on phishing attacks.



ZEROFOX®

Weekly Intelligence Brief

TLP:GREEN

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

Threat Actor Groups Announced Attack Against BreachForums

What happened: On April 15, 2024, threat actor groups R00TKIT and CyberArmyofRussia (aka People's CyberArmy) claimed on Telegram to have conducted a coordinated attack against the English-language internet forum BreachForums. While the groups did not disclose the type of attack they carried out, they did reveal that the attack allegedly brought down BreachForums' servers and crashed its surface web [.]cx domain. The attack did not disrupt BreachForums' [.]onion site, and its moderator, "Baphomet," later announced the resumption of the surface-level site under the [.]st top level domain (TLD). The groups further announced in this Telegram post their plan to publish a list of BreachForums' user data, including email addresses and IP addresses, on an undisclosed date.



- **What this means:** As an English-language forum, BreachForums does not have the same community restrictions on attacking Russian and former Soviet entities as Russian-language forums typically do. As a result, anti-Russia content is frequently posted on the site, giving R00TKIT and CyberArmyofRussia—who are largely motivated by pro-Russia ideology—the motivation to disrupt BreachForums. Additionally, the available details of the attack align with both groups' regular use of distributed denial-of-service (DDoS) attacks, of which ZeroFox has observed a recent uptick in from CyberArmyRussia. However, in a subsequent post to the forum's Telegram channel, Baphomet disputed the groups' involvement in the attack and instead placed blame on the Five Eyes network (an intelligence alliance between the United States, United Kingdom, Canada, Australia, and New Zealand), though it does not provide corroborating evidence. While ZeroFox cannot definitively confirm attribution at this time, it assesses that there is a roughly even chance that the attack on BreachForums was conducted by either of the aforementioned actors. ZeroFox will continue to monitor for any further updates.

Threat Actor noob_iab Auctioning Network Access Bundle to 4,000 Servers Worldwide

What happened: On April 15, 2024, ZeroFox observed the untested threat actor "noob_iab" advertising an auction for a network (VPN, SSH, Shell) access bundle with root rights to 4,000 corporate servers of undisclosed companies worldwide on the predominantly Russian-language dark web forum Exploit. Noob_iab first made the post on April 10, 2024; according to the actor, many companies on the list are engaged in the IT services and telecommunications industries.

The starting bid for the access bundle was USD 150,000, with a minimum bid of USD 20,000 and an instant purchase price of USD 400,000.



➤ **What this means:** As the actor is untested, ZeroFox cannot confirm their credibility as to whether they actually have the access bundle to a high number of servers to sell. An actor could purchase all of these accesses and conduct a large number of attacks in quick succession. This could also be beneficial for ransomware groups, as they could gain access to potential victim companies for a low cost compared to what they might receive for each ransom to increase their profit margin. As the price is so high and the actor's credibility cannot be verified, there is a low likelihood of the bundle being purchased.

Threat Actor Group “Red Evil” Claims Cyberattack Against Iran

What happened: On April 13, 2024, pro-Israel threat actor group “Red Evil” announced a campaign against an unspecified Iranian system. The attack reportedly included the successful distribution of text messages to over 20 million Iranian users claiming to be from the Government of Iran. The texts were designed to appear as if coming from the Iranian Passive Defense Organization and warned citizens to prepare for an attack from Israel. According to Red Evil, this attack caused enough panic that residents began withdrawing money from banks, and the Iranian government addressed the “electronic and psychological warfare” via a news release.



- **What this means:** Red Evil has operated since at least the onset of the Israel-Hamas war and primarily focuses its attacks against Iran. While the group does not appear to be very active, they have successfully conducted attacks against critical infrastructure such as the power grid and telecommunications networks in Iran. Attacks such as this that appear to be geopolitically motivated carry the risk of escalating the conflict. The group's ability to emulate the Iranian government agency responsible for warning citizens of an attack demonstrates a relatively sophisticated capability. ZeroFox assesses the recent escalation in the regional conflict will likely result in increased activity by third-party hacktivist groups.

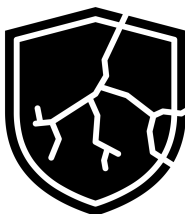
| Exploit and Vulnerability Intelligence |

| Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox has observed vulnerabilities, exploits, and updates disclosed by prominent companies in the software solutions, asset management, and network security domains. Oracle released its [Critical Patch Update](#) and made available hundreds of security patches for vulnerabilities, more than 30 of which are critical. Ivanti disclosed patches for more than [20 vulnerabilities](#) in its Avalanche enterprise mobile device management (MDM) product. The fixes involve critical bugs CVE-2024-24996 and CVE-2024-29204, which can be exploited remotely. Cisco recently published an [advisory](#) addressing software updates for a command injection vulnerability (CVE-2024-20295) in the command line interface (CLI) of the Cisco Integrated Management Controller (IMC). Google and Mozilla have released security updates this week. In [Chrome 124](#), Google announced fixes for 22 bugs, including three that are high-severity issues, and rolled out 124.0.6367.60/.61 for Windows and macOS and version 124.0.6367.60 for Linux. Mozilla released a [security advisory](#) for patches that fixed 15 vulnerabilities, including high-severity bugs that could allow attackers to execute arbitrary code.

Notable vulnerabilities:

[CVE-2024-3817](#)



What happened: HashiCorp's go-getter library is vulnerable to argument injection when executing Git to discover remote branches. This **CRITICAL** vulnerability does not affect the go-getter/v2 branch and package and is assigned a CVSS score of 9.8.

➤ **What this means:** When go-getter is performing a Git operation, it will try to clone the given repository. If a Git reference is not passed along with the

Git url, go-getter will then try to check the remote repository's HEAD reference of its default branch by passing arguments to the Git binary on the host on which it is executing.

- **Affected products:**

- go-getter 1.5.9 up to 1.7.3

[CVE-2024-20295](#)

What happened: CVE-2024-20295 has been discovered in the CLI of the Cisco IMC, which could be exploited by an authenticated, local attacker to execute command injection attacks on the underlying operating system and gain root privileges. The attacker needs read-only or higher privileges on the affected device. This vulnerability is tracked as **HIGH** and is assigned a CVSS score of 8.8.



➤ **What this means:** The vulnerability arises from inadequate validation of user-supplied input. An attacker can exploit it by submitting a specially crafted CLI command. Successful exploitation could lead to the elevation of privileges to root. Cisco has released software updates to fix this vulnerability, and there are no workarounds available.

● **Affected products:**

- 5000 Series Enterprise Network Compute Systems (ENCS)
- Catalyst 8300 Series Edge uCPE
- UCS C-Series Rack Servers in standalone mode
- UCS E-Series Servers
- 5520 and 8540 Wireless Controllers
- Application Policy Infrastructure Controller (APIC) Servers
- Business Edition 6000 and 7000 Appliances
- Catalyst Center Appliances, formerly DNA Center (DNAC)
- Cloud Services Platform (CSP) 5000 Series
- Common Services Platform Collector (CSPC) Appliances
- Connected Mobile Experiences (CMX) Appliances
- Connected Safety and Security UCS Platform Series Servers
- Cyber Vision Center Appliances
- Expressway Series Appliances
- HyperFlex Edge Nodes
- HyperFlex Nodes in HyperFlex Datacenter without Fabric Interconnect (DC-NO-FI) deployment mode
- IEC6400 Edge Compute Appliances
- IOS XRv 9000 Appliances
- Meeting Server 1000 Appliances
- Nexus Dashboard Appliances
- Prime Infrastructure Appliances
- Prime Network Registrar Jumpstart Appliances
- Secure Email Gateways
- Secure Email and Web Manager
- Secure Endpoint Private Cloud Appliances
- Secure Firewall Management Center Appliances, formerly Firepower Management Center
- Secure Malware Analytics Appliances
- Secure Network Analytics Appliances
- Secure Network Server Appliances
- Secure Web Appliances
- Secure Workload Servers
- Telemetry Broker Appliances



ZEROFOX®

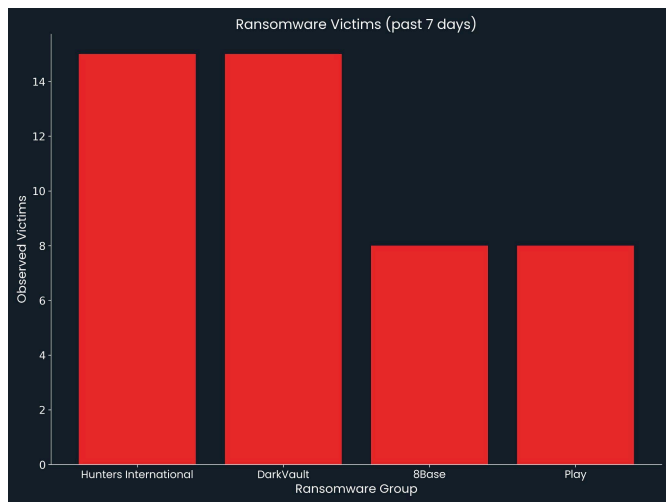
Weekly Intelligence Brief

TLP:GREEN

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

Optics Giant Hoya Hit with USD 10 Million Ransomware Demand



Source: ZeroFox Internal Collections

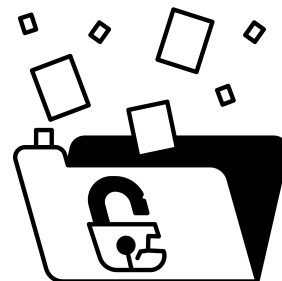
What happened: Hoya Corporation (Hoya) recently suffered a cyberattack conducted by “Hunters International.” The threat actor demanded a USD 10 million ransom to not leak Hoya’s records, which allegedly contained 1.7 million stolen files comprising 2 TB of data. Hunters International took a “No Negotiation / No Discount” stance towards Hoya in this attack. The Hunters International and “DarkVault” ransomware groups have been the most active groups in the past week.

➤ **What this means:** The cyberattack on Hoya impacted the production and order process, with multiple of its business divisions experiencing IT outages; remediation efforts are reportedly ongoing.

Breach Intelligence: Actor Leaks Data from Ministry of Defense Israel

What happened: Threat actor “APExploits” has leaked a database allegedly associated with Israel’s Ministry of Defense. APExploits claims that it breached the Ministry’s systems in January 2023. The leaked data includes dates of birth, email addresses, genders, groups, phone numbers, names, and projects.

- **What this means:** Tensions in the Middle East have been rising in the past few days, with repercussions spreading in the cyber realm as well. Several actors have claimed to target Israel and its allies, while some others are attacking Iranian websites. APExploits leaking Israel’s Ministry of Defense data on the dark web is likely aligned with these geopolitical developments. Affected individuals and companies should be wary of unsolicited communication involving targeted emails or calls from unknown sources, as threat actors might use the leaked information for spear phishing attacks.

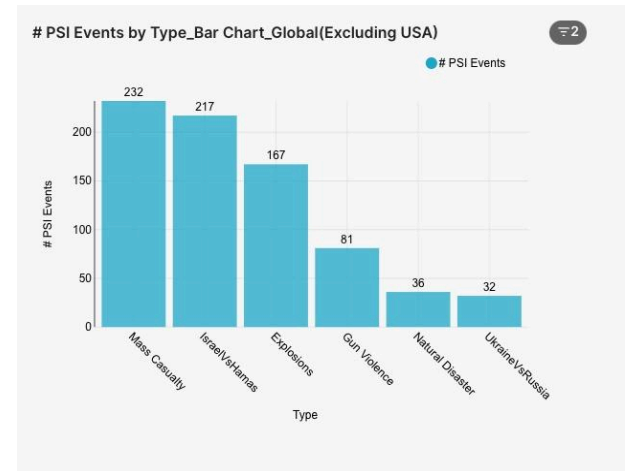


Physical and Geopolitical Intelligence

| Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

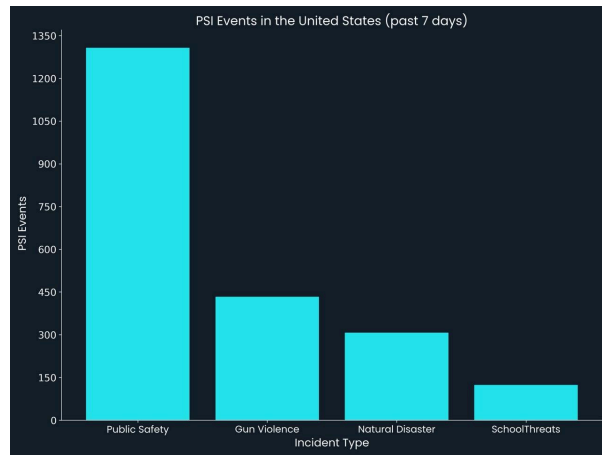
What happened: Excluding the United States, there was a 25 percent increase in mass casualty events alerted this week, with the top contributing countries being Palestine, Israel, and Lebanon; notably, approximately 72 percent of these events were explosions. Additionally, there were over 200 alerts related to the Israel-Hamas war (including protests, raids, and involvement in neighboring countries), as opposed to a little over 30 alerts related to the conflict in Ukraine. Following explosions, the most alerted incident sub-types were gun violence and natural disasters.



Source: ZeroFox Internal Collections

- **What this means:** Tensions surrounding the Israel-Hamas war continue to rise as neighboring countries such as Lebanon, Iran, and Syria increase their involvement in the conflict. Iran's attack on Israel over the weekend was mostly intercepted; however, Iran has warned that any retaliation from Israel will result in even larger attacks, including the targeting of U.S. military bases. Lebanon is a top contributor to mass casualty alerts due to Hezbollah's growing participation in the conflict; Hezbollah are also backed by Iran and have many more resources than Hamas. While the number of attacks are fewer in Ukraine, they are still lethal, as seen by the recent Chernihiv bombing that killed 18 people and wounded over 60. President Volodymyr Zelensky has claimed that Ukraine did not have enough air defense equipment and has recently lowered the Ukrainian draft age to 25. Under the gun violence category, many of these alerts were from North and South American countries such as Guatemala, Mexico, and the Bahamas and are possibly related to ongoing gang violence in those regions. The natural disasters alerted globally this week were mostly fires; notably, Indonesia is currently under a tsunami warning due to a volcano erupting, and Dubai saw unprecedented amounts of rain this week that led to city-wide flooding.

Physical Security Intelligence: United States



Source: ZeroFox Internal Collections

What happened: In the past week, the top three most-alerted incident subtypes were gun violence, natural disasters, and police activity. 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 which had the most gun violence alerts were Illinois and Pennsylvania, which together made up over 20 percent of this week's nationwide total. Gun violence across the United States increased by approximately 9 percent from the week prior. As structure fires and wildfires currently fall under the

natural disaster scope, the majority of natural disasters alerted this week consist of these events. The top two

contributors to the natural disaster alerts this week were California and Texas. 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 Wisconsin were the top two contributing states this week. Both nationwide school-related threats (including all incident types except protests) as well as nationwide protest activity increased by 34 percent from last week.

- **What this means:** Multiple researchers have correlated warmer temperatures with higher levels of reported crime. This is not necessarily due to more crimes being committed when it is warm; it is likely because more crimes then occur outdoors in view of the public as well as law enforcement, which may explain the rise in both gun violence and police activity subtype alerts. Gun violence often occurs in major cities such as Chicago and Philadelphia, which elucidates why Illinois and Pennsylvania contribute a significant amount to overall gun violence instances. The spring season also brings on a rise in fires, as drier climates, higher temperatures, and forceful winds become more abundant. Both California and Texas, the top two contributors to this week's natural disaster alerts, have experienced wildfires as well as structure fires this week. Protest activity may have increased due to tensions regarding domestic politics (particularly in relation to the upcoming presidential election) as well as international conflict (most notably, the ongoing Israel-Hamas war) causing calls to action. It is difficult to assess why school-related threats have increased this week; however, as many school-related instances fall under the police activity umbrella, it becomes more clear that these numbers may correspond.

Interested in more ZeroFox Threat Intelligence? ZeroFox researchers produce 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%