



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN
August 26, 2024

Scope Note

ZeroFox's Weekly Intelligence Briefing highlights the major developments and trends across the threat landscape, including digital, cyber, and physical threats. 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 August 23, 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 – RansomHub Extortion Activity on Sharp Upward Trajectory	2
ZeroFox Intelligence Brief – An Introduction to Stealer Logs	2
 Cyber Intelligence Key Findings	4
OpenAI Disrupts Covert Iranian Influence Operation Leveraging ChatGPT to Target U.S. Elections	4
Cyber Threats to U.S. Critical Food Infrastructure	5
Blind Eagle Hackers Exploit Spear Phishing to Deploy RATs in Latin America	6
 Deep and Dark Web Intelligence Key Findings	8
Meow Ransomware Targets Zydus Pharmaceuticals	8
Akira Ransomware Targets Transit Authority of Northern Kentucky	8
CyberDragon Claims Attack on AT&T	9
 Exploit and Vulnerability Intelligence Key Findings	11
CVE-2024-5932	11
CVE-2024-6089	12
 Ransomware and Breach Intelligence Key Findings	14
Ransomware Attacks and Operational Setbacks	14
Data Breaches Target Various Sectors	15
 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	21
 Appendix B: ZeroFox Intelligence Probability Scale	22

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Flash Report – RansomHub Extortion Activity on Sharp Upward Trajectory

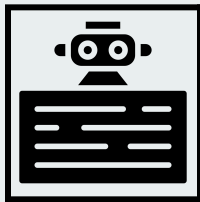
The ransomware-as-a-service (RaaS) operation “RansomHub” has almost certainly significantly increased its operational tempo in recent weeks, having conducted more attacks so far in Q3 2024 than in Q1 and Q2 2024 combined. RansomHub was first observed in approximately February 2024 and exhibited a higher tempo of attacks during those initial weeks than is usually observed from new ransomware operations. RansomHub’s activity as a proportion of all ransomware activity observed by ZeroFox is also on a sharp upward trajectory, with the group accounting for approximately 2 percent of all attacks in Q1, 5.1 percent in Q2, and 14.2 percent so far in Q3. There is a likely chance that RansomHub will remain the most prominent ransomware collective for the coming months and continue to attract affiliates. The collective will almost certainly continue to target a highly diverse array of sectors, and the proportion of attacks targeting organizations located in North America will very likely increase.

ZeroFox Intelligence Brief – An Introduction to Stealer Logs

In this brief, ZeroFox provides an introduction to info-stealing malware and the stealer logs that they produce, the cyber threat actors providing both the information supply and demand for them, and the threats that such stealers pose to individuals and organizations. A stealer log is a series of data files generated and compiled by malicious software known as “infostealers.” The log contains personal and sensitive information that has been collated and extracted by a cyber threat actor. Numerous data-stealing techniques are leveraged by infostealers; form grabbing, keylogging, credential dumping, and screen scraping are all commonly used to uncover and extract information from the target endpoints. Threat actors responsible for the production of stealer logs often seek to sell the stolen data in deep and dark web (DDW) forums, supplying cybercriminals with a constant trove of stolen information. The information found in stealer logs (such as credentials, personal financial details, browser information, and hardware specifications) is used to enable and enhance a broad array of cyberattacks. The mitigation strategies of individuals and organizations must be as diverse as the stealer logs themselves and address the full scope of network access vectors that can be targeted by an attacker in possession of credentials, cookies and tokens, or other browser data.

| Cyber Intelligence |

| Cyber Intelligence Key Findings

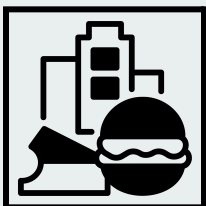


OpenAI Disrupts Covert Iranian Influence Operation Leveraging ChatGPT to Target U.S. Elections

What happened: OpenAI has taken down a set of ChatGPT accounts generating content used to further a covert Iranian influence operation dubbed Storm-2035 that is targeting the upcoming U.S. elections. OpenAI [states](#) the action is part of its ongoing efforts to detect and stop covert influence operations (IO). It identified 12 X (formerly Twitter) accounts contributing to Storm-2035 that purported to represent both sides of the U.S. political spectrum. The majority of social media posts the campaign published received few or no likes, shares, or comments and, hence, did not achieve any meaningful engagement. The operation ranked at the low end of Category 2 of the Brookings' Breakout Scale, which assesses the impact of covert IO on a scale from one (lowest) to six (highest). Additionally, an extensive operation was observed in the past week in which pro-Russia websites [masquerading](#) as U.S. news outlets are posting incendiary, misleading disinformation, such as unsubstantiated claims of the Democratic Party's involvement in a plot to kill former President Donald Trump, ahead of the high-stakes U.S. elections. The content is re-posted in various languages across several social media platforms and repeated by AI chatbots, increasing the operation's reach and engaging a diverse audience.

- **What this means:** OpenAI's investigation revealed that the campaign used ChatGPT to generate long-form content and short social media comments. The first workstream produced articles on U.S. politics and global events and was published on five websites that posed as news outlets catering to either side of the political spectrum. The second workstream created short comments in English and Spanish for social media posts. The generated content addressed various topics, including the conflict in Gaza, Israel's presence at the Olympic Games, and—to a lesser extent—Venezuelan politics, the rights of Latinx communities in the United States (both in Spanish and English), and Scottish independence. With the U.S. presidential elections on the horizon, the escalating tensions in the Middle East, and the ongoing Russia-Ukraine war, foreign actors are increasingly weaponizing generative artificial intelligence (AI) to fuel influence campaigns. Such operations allow actors to further their agenda while hiding their true identity or intentions. Consequently, hundreds of fake news outlets, such as the pro-Russia ones, have been proliferating over recent months. The fake sites also leverage easily accessible AI tools to produce inflammatory content, intending to promote controversial or inaccurate

narratives. Deepfakes associated with elections in Asia and the European Union have already [raised](#) concerns and prompted social media companies to take preventive measures. Notably, authorities have [issued](#) warnings ahead of the U.S. presidential elections about foreign influence campaigns primarily aimed at spreading disinformation, sowing discord, and undermining confidence in democratic institutions and values.



Cyber Threats to U.S. Critical Food Infrastructure

What happened: The Federal Bureau of Investigation (FBI)'s second annual Agriculture Threats Symposium in Omaha, Nebraska, focused on rising cyber threats to the U.S. agriculture sector, (including ransomware attacks, intellectual property theft, and bioterrorism) exacerbated by increased digital connectivity in farming operations. Over 400 farmers, cybersecurity experts, and policymakers from 30 states attended the symposium. In the past year, ZeroFox has observed more than 200 cyber incidents against agriculture and food-related entities. The attacks were primarily conducted by the LockBit and Play ransomware groups; 45 percent of the attacked entities were in the North American region.

- **What this means:** The FBI is monitoring major threats to the nation's agriculture sector, which—like water, power, and transportation—is considered part of the nation's critical infrastructure. The agriculture sector, which is integral to national security, is increasingly vulnerable due to its reliance on digital technologies; any degree of disruption in the agricultural sector affects U.S. rural life because of its dependency on this critical sector. As foreign adversaries, particularly China, target this critical infrastructure, the potential impact extends beyond farms to the broader economy. Examples of imminent cyber threats mentioned in the symposium included ransomware attacks that cripple operations, network hacks that take control of systems, and the theft of seeds worth millions of dollars in intellectual property and research. Additionally, the symposium highlighted the urgency for stronger partnerships between the public and private sectors to bolster cybersecurity defenses. Threat actors may have a vested interest in targeting a vital element of a nation's critical infrastructure (such as food and agriculture) in hacktivism attacks and other forms of hybrid warfare. Such attacks are likely to have an impact on food supply and logistics while also endangering other allied industries and sectors. The symposium highlighted that threats to agriculture are only growing and becoming more complex. Food systems are also [vulnerable](#) to hybrid warfare tactics of

both state and non-state actors. Networked systems interacting together amplify threats and vulnerabilities that exist in any of the major systems, as well as risk to other dependent systems. This gives way to risks that are highly relevant for food safety and supply, manufacturing, banking, finance, commodities, insurance, and other sectors.



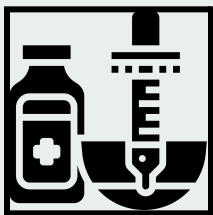
Blind Eagle Hackers Exploit Spear Phishing to Deploy RATs in Latin America

What happened: Cybersecurity researchers have identified a threat actor group called “Blind Eagle” (aka APT-C-36) that has consistently targeted organizations and individuals across Latin American countries, including Colombia, Ecuador, Chile, and Panama. This group, suspected to be Spanish-speaking, has been active since at least 2018. Its attacks affect various sectors (including government, financial services, and energy) and primarily involve spear phishing to distribute various remote access trojans (RATs), including AsyncRAT, BitRAT, Lime RAT, NjRAT, Quasar RAT, and Remcos RAT.

What this means: Blind Eagle’s attack method begins with phishing emails that impersonate legitimate institutions, urging recipients to click on a link leading to a fake website or download a malicious attachment. These emails direct targets to actor-controlled sites where an initial dropper is deployed, which then fetches further malicious payloads from various remote servers. The final stage malware, often obfuscated and using modified open-source RATs, can capture sensitive information or install additional plug-ins for enhanced functionality. Recent updates include using Hijack Loader for distributing AsyncRAT, indicating the group’s adaptability and evolving tactics. The use of spear phishing and publicly available RATs by Blind Eagle poses significant risks to organizations. Successful attacks can lead to unauthorized access to sensitive systems, data breaches, and the compromise of critical infrastructure. The infiltration of the government, financial, and energy sectors can disrupt operations, damage reputations, and result in financial losses. Blind Eagle’s sophisticated phishing and malware techniques highlight the group’s capability to evade detection and continuously adapt its methods, making the actor a persistent and evolving threat. This shows that even publicly available tools can be leveraged for serious cyber espionage and data theft. Organizations must prioritize advanced threat detection, employee training, and incident response strategies to mitigate these risks and protect their assets from such adaptable cyber threats.

| Deep and Dark Web Intelligence |

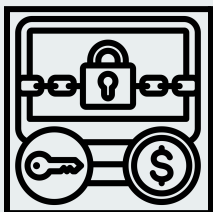
| Deep and Dark Web Intelligence Key Findings



Meow Ransomware Targets Zydus Pharmaceuticals

What happened: On August 19, 2024, ZeroFox observed an update on the “Meow” ransomware leak site targeting U.S.-based pharmaceuticals company Zydus Pharmaceuticals. According to the post, the threat actors claim to be selling over 200 GB of confidential data, including financial documents, client and employee information, and details pertaining to pharmaceutical research and development. The post further assures potential buyers that this data provides insight into the company’s operations, research activities, and strategic plans. The threat actors are reportedly selling the data to one individual for USD 7,500 or to multiple individuals for USD 2,500 each.

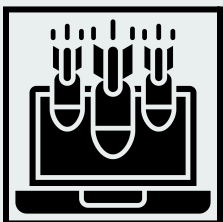
- **What this means:** This breach has the potential to threaten Zydus Pharmaceuticals’ operational continuity and result in a disruption to drug production and sales. As the company currently offers more than 500 products on the U.S. market, this attack could severely jeopardize the healthcare needs of a large portion of the U.S. population. The company is also a U.S.-based subsidiary of Zydus Lifesciences, a multinational pharmaceutical company headquartered in India. The breach of the U.S.-based entity could lead to additional breaches of subsidiaries in other countries, as well as of the main company itself. This highlights the need for robust cybersecurity measures, such as network segmentation.



Akira Ransomware Targets Transit Authority of Northern Kentucky

What happened: On August 20, 2024, ZeroFox observed an update on the “Akira” ransomware leak site targeting the Transit Authority of Northern Kentucky (TANK). According to the post, the threat actors are in possession of personal information of employees and customers, confidential agreements, contracts, and incident data. The post does not specify whether the data is being sold, or at what price, but mentions that it will be available on the leak site “soon.” The threat actors did not specify any further information, including how the data was obtained.

- **What this means:** This attack has the potential to disrupt transportation operations in the Northern Kentucky area, possibly leading to financial losses, service delays, and a lack of public trust in local transportation that may see customers seek alternatives. Additionally, the compromised personal data of employees and customers raises concerns about possible identity theft, financial fraud, and privacy violations that the company will have to remediate. Akira Ransomware is a positive-reputation threat actor with a history of committing highly sophisticated attacks. Therefore, ZeroFox assesses the group's claimed attack against TANK is likely true.



CyberDragon Claims Attack on AT&T

What happened: On August 21, 2024, threat actor group “CyberDragon” claimed on its Telegram channel to have conducted a distributed denial-of-service (DDoS) attack against AT&T, a U.S.-based internet service and mobile phone provider. The post includes a graph that shows the attack leading to at least 263 outages over its first 24 hours.

- **What this means:** While DDoS attacks do not typically result in significant or lasting damage, this one will almost certainly lead to widespread discontent, as AT&T is one of the largest telecommunications providers in the United States. AT&T users' inability to contact others or use the internet for both professional and personal reasons could result in disruptions to other sectors. The attack could also lead to reputational damage and subsequent financial loss for AT&T. Additionally, this attack underscores CyberDragon's ongoing efforts to disrupt major industry players and highlights its capacity for targeting high-profile organizations.

| **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, operating systems, industrial automation, and government security domains. Last week, the Cybersecurity and Infrastructure Security Agency (CISA) added five vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog based on evidence of active exploitation. Two of these ([CVE-2021-33044](#) and [CVE-2021-33045](#)) are Dahua IP Camera authentication bypass vulnerabilities that can let attackers bypass device identity authentication by constructing malicious data packets. [CVE-2022-0185](#) is a high-severity heap-based buffer overflow bug in the Filesystem Context functionality of the Linux kernel. [CVE-2021-31196](#) is another high-severity bug added to the KEV in the past week. It is a remote code execution (RCE) vulnerability in the Microsoft Exchange Server. [CVE-2024-23897](#) is a critical Jenkins vulnerability that can allow RCE. Microsoft has released the patch for [CVE-2024-38193](#), an exploited bug which, if successfully exploited, can let an attacker gain SYSTEM privileges. [CVE-2024-6800](#) is a critical (CVSS score: 9.5) bug that could allow an attacker to bypass authentication and gain administrator access to the system. It was fixed in GitHub Enterprise Server versions 3.13.3, 3.12.8, 3.11.14, and 3.10.16. [CVE-2024-6079](#) exists in the Rockwell Automation Emulate3D™, which could be leveraged to execute a DLL Hijacking attack. The application loads shared libraries, which are readable and writable by any user. If exploited, a malicious user could leverage a malicious DLL and perform an RCE attack. Another Rockwell vulnerability addressed in a CISA ICS Advisory is [CVE-2024-6089](#), a high severity input validation vulnerability. SolarWinds has released a hotfix for [CVE-2024-28986](#), rated 9.8 on the CVSS scale. The vulnerability could enable attackers to execute arbitrary commands on the host machine. While it was first reported as an unauthenticated flaw, SolarWinds' testing revealed that authentication is required. Despite this, it is strongly recommended that users promptly apply the patch.



CRITICAL

CVE-2024-5932

What happened: The GiveWP – Donation Plugin and Fundraising Platform for WordPress has a serious vulnerability that affects all versions up to and including 3.14.1. This flaw involves PHP Object Injection, which is a type of security flaw wherein an attacker can manipulate the data sent to the

server in such a way that it results in the execution of malicious PHP code. This vulnerability has a CVSS score of 10.

- > **What this means:** This vulnerability allows unauthenticated attackers to inject malicious PHP objects into the system. Exploiting this vulnerability can lead to RCE and the ability to delete arbitrary files on the server. If left unpatched, this could enable attackers to take control of the server, disrupt site operations, or cause data loss. To address the risks posed by this vulnerability, it is recommended that users upgrade to version 3.14.2 or a later version that includes the necessary security fixes.
- > **Affected products:**
 - Versions <= 3.14.1



HIGH

CVE-2024-6089

What happened: An input validation vulnerability exists in the Rockwell Automation 5015 – AENFTXT when a manipulated PTP packet is sent, causing the secondary adapter to result in a major nonrecoverable fault. If exploited, a power cycle is required to recover the product.

- > **What this means:** CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability, including minimizing network exposure for all control system devices and/or systems, ensuring they are not accessible from the internet, and locating control system networks and remote devices behind firewalls and isolating them from business networks, as well as implementing the risk [mitigation steps](#).
- > **Affected products:** Rockwell Automation 5015 – AENFTXT: Version 2.011

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

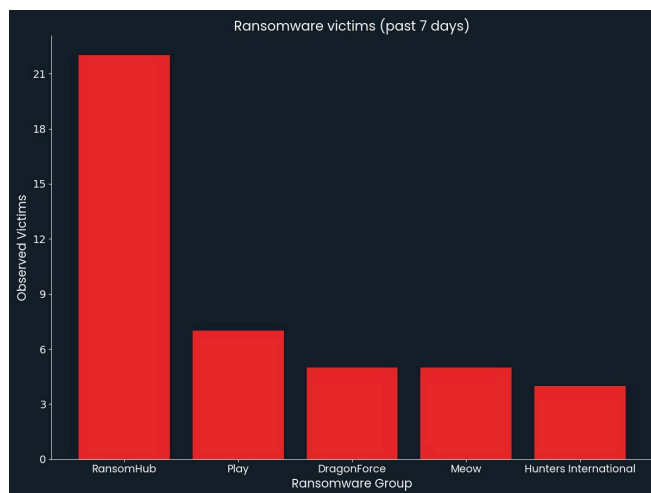


Ransomware Attacks and Operational Setbacks

What happened: Researchers have [observed](#) that ransomware groups have raked in the highest amount of funds while conducting fewer high-profile attacks in the first half of 2024. The city of Flint experienced a ransomware attack that affected the city's payment and communication services and is currently working towards bringing its network systems backup and restoring its online services. The attack did not affect emergency services but did impact billing systems and global information systems (GIS).

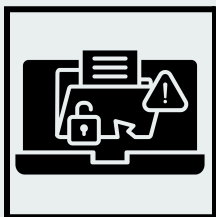
The official [notification](#) confirms that Flint experienced a ransomware attack and that investigations are still underway to establish if any sensitive data was stolen.

Flint is one of the several Michigan ransomware attacks targets. The U.S. Department of Health and Human Services (HHS) is [warning](#) the healthcare sector that ransomware group "Everest" is now targeting hospitals. The group is an RaaS adversary that accesses systems through compromised user accounts and RATs. Everest appears to have shifted its operations to function as an initial access broker within the underground Russian ransomware economy. Its primary role is to facilitate ransomware attacks by first gaining unauthorized access to victim organizations through methods like credential theft. The RansomHub ransomware gang has been [observed](#) in various campaigns involving new malware dubbed "EDRKillShifter" that disables endpoint detection and response (EDR) security software. Investigations suggest that the malware's language property can be traced back to Russian origins. CannonDesign is notifying its customers of a data breach that exposed and resulted in data being stolen. The company has not yet confirmed who breached and stole the data, but it is [suspected](#) that "Avos Locker" ransomware group may be behind the attack. The data reportedly includes database dumps, schematics, hiring documents, client details, and IT and infrastructure details.



Source: ZeroFox Internal Collections

- **What this means:** Ransomware attacks on healthcare facilities are often critical because of the confidentiality and possible time-sensitivity of the stolen medical data. This places significant financial burdens on care units responsible for their patients' health and well-being, and delays in accessing data can put patients at risk. Threat actors are now exploiting this to target healthcare facilities, as hospitals and other healthcare entities are more likely than other non-essential industries to pay ransoms in order to minimize patient risks and bring systems back online quickly. Since hospitals are more apt to pay, threat actors are incentivized to keep attacking these institutions, creating a vicious cycle. The EDRKillShifter malware is said to deploy legitimate but vulnerable drivers to disable security and take control of systems. Researchers suspect that the drivers are exploited by copying portions of proofs-of-concept available on GitHub and are modified to suit the attack. EDRKillShifter malware has been observed in various attack campaigns ranging from those leveraged by hacktivists to prominent ransomware groups like RansomHub. The RaaS operation RansomHub has almost certainly significantly [increased](#) its operational tempo in recent weeks, having conducted more attacks so far in Q3 2024 than in Q1 and Q2 2024 combined. "AvosLocker" [operates](#) under an RaaS model. AvosLocker affiliates, in the past, have compromised organizations across multiple critical infrastructure sectors in the United States, affecting Windows, Linux, and VMware ESXi environments. AvosLocker affiliates compromise organizations' networks by using legitimate software and open-source remote system administration tools. AvosLocker affiliates then use exfiltration-based data extortion tactics with threats of leaking and/or publishing stolen data.



Data Breaches Target Various Sectors

What happened: Toyota has [confirmed](#) that a third-party data breach exposed customer data. On August 19, ZeroFox Intelligence observed threat actor "ZeroSevenGroup" [claiming](#) responsibility for a cyberattack against Toyota's U.S. branch, where it accessed 240 GB of data. ZeroSevenGroup leaked the data on the dark web marketplace BreachForums. The dataset included details on Toyota employees, customers, contracts, and financial records. National Public Data (NPD) has now [confirmed](#) it experienced a cyberattack after threat actors leaked a stolen database

comprising millions of Social Security numbers (SSNs) and other sensitive personal information. Threat actor “SXUL” reportedly took credit for breaching NPD in April 2024 and priced the sale of the stolen database at USD 2 million. On April 7, threat actor “USDoD” posted a sample of the stolen data on BreachForums, followed by threat actor “Fenice”, who posted a link to download the dataset on August 6. USDoD was reportedly a middleman for the initial posting. In other news, a member of the Massachusetts Air National Guard was [arraigned](#) around mid-August on charges of violating military laws related to leaking classified U.S. national security documents. The accused, arrested in April 2023, deferred entering a plea until the court-martial trial started in March 2024. The Air Force has accused the individual of obstructing justice and ignoring orders related to classified information. Meanwhile, cybersecurity researchers [revealed](#) that wind measurement towers near classified locations in China have been used to collect and transmit sensitive data abroad, posing a national security risk. Investigations showed that some towers, built by companies with ties to foreign entities, were not legally registered and had complex data transmission methods. Authorities have intervened to prevent data leaks.

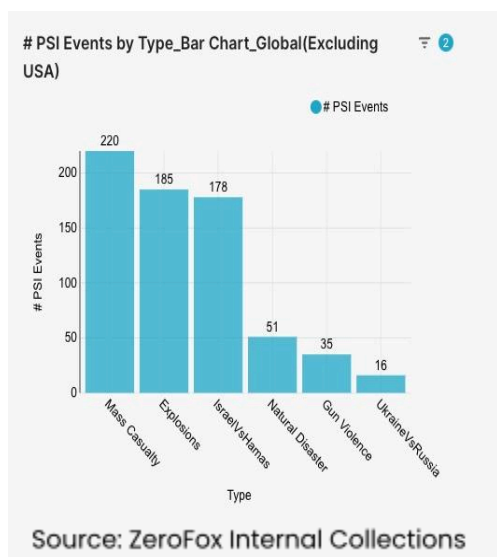
- **What this means:** The Toyota breach has exposed a wide range of sensitive information, including customer and employee data, financial records, and network details. Attackers reportedly used ADRecon (which extracts extensive information from Active Directory environments) to gather comprehensive information from Toyota’s network, potentially increasing the risk of future attacks. Toyota has not yet disclosed when the breach was detected, how the attacker gained access, or the extent of data exposure. The NPD breach presents severe long-term risks, like fraudulent credit accounts, loans, and tax returns that could lead to significant financial losses and potential legal battles, especially for Jerico Pictures. The background check company has recently been served a class action lawsuit for [failing](#) to properly secure the personally identifiable information (PII) of 2.9 billion people. Exposed SSNs are particularly concerning because they are important identifiers in financial and governmental transactions and can be a [target](#) for identity scammers. Additionally, leaked contact details, such as email addresses, can be used in phishing attacks to gather more personal information for further fraudulent activities. On the other hand, the individual with top-secret clearance in the Air Force was accused of mishandling classified information, including details on Russia’s invasion of Ukraine. Despite being ordered to stop accessing unrelated classified data, the individual allegedly obstructed justice by disposing of devices and instructing someone to delete online messages. The leaks, which were shared on the messaging app Discord, indicate a possibility others were involved or aware of the air guard’s leaks, potentially broadening the scope of the breach. This breach could expose strategic details, compromise intelligence sources, and potentially endanger lives, highlighting the severe impact of mishandling and leaking classified information. Meanwhile, in China, the discovery of wind measurement towers being used for covert data collection suggests that foreign entities are finding new, less

obvious ways to gather intelligence. As geopolitical tensions rise, China's response—tougher counter-espionage laws and stricter rules on meteorological data—reflects a more aggressive stance in protecting against foreign threats.

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global



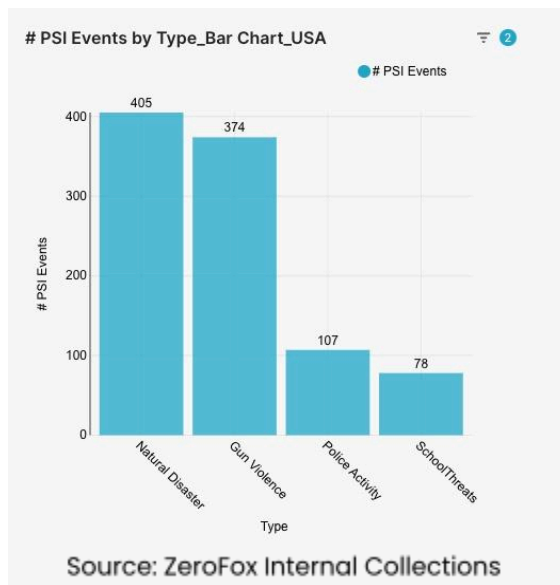
What happened: Excluding the United States, there was a 7 percent increase in mass casualty events this week from the previous week, with the top contributing countries being Palestine, Israel, and Lebanon. Approximately 84 percent of these events were explosions, and the three aforementioned countries accounted for approximately 56 percent of all mass casualty alerts. General alerts related to the Israel-Hamas War (including protests, raids, and involvement in neighboring countries) increased by 8 percent from the previous week. Additionally, events related to Russia's war in Ukraine decreased by 43 percent. The top three most-alerted subtypes were explosions, which saw a 6 percent increase from the

previous week; gun violence, which decreased by 26 percent; and natural disasters, which increased by 6 percent.

- **What this means:** This week, mass casualty, explosions, and alerts regarding the Israel-Hamas conflict all saw a very similar rate of increase, which correlates with the fact that these tags are often used together in one alert. The increase from this week may be due to the Israeli military stepping up [operations](#) and ordering evacuations in Deir el-Balah in central Gaza and Khan Younis in the south of Palestine; additionally, Hezbollah from Lebanon has recently attacked Israeli army positions in the Israeli town of Kiryat Shmona with several drones. As no peace agreement has yet been reached, these escalations are likely to persist. However, alerts related to the Ukraine-Russia war have decreased—possibly due to the slowing of Ukraine's Kursk [offensive](#), with its troops making only marginal gains around territory they already control. Natural disasters have also increased somewhat this week, as several parts of Asia continue to experience life-threatening damages from the monsoon season. For instance, earlier this week 14 people were [killed](#) in a 24-hour period in the Punjab province of Pakistan, and at least 209 people in the country have died from rain-related incidents since the beginning of July. As the monsoon season does not conclude until September, ZeroFox anticipates seeing more incidents related to this in countries across Asia.

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. Natural disaster alerts typically involve fires and severe weather; gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim; and police activity refers to law enforcement presence for a generalized threat or unknown reasons. The top two states that had the most gun violence alerts were Illinois and Ohio, which together made up one-quarter of this week's nationwide total (25 percent). Gun violence across the United States overall increased by 22 percent from the week prior. The top two contributors to natural disaster alerts this week were California and Texas, and natural disaster alerts across the country increased by 5 percent. Police activity alerts increased by 18 percent, and the top contributing states were California and Texas as well. Notably, all alerts (excluding protests) involving schools increased by 20 percent, with California and Texas again being the top contributors.



- **What this means:** Police activity and school-related threats both saw a similar rate of increase this week and had the same highest-contributing states. As more and more students are coming back from their summer break, generalized threats against schools have increased, which results in law enforcement presence (i.e., police activity alerts). Typically, this occurs when there is a suspected weapon on campus or a lockdown due to a nearby incident. Gun violence saw a fairly significant increase from the previous week, including a mass [shooting](#) of six people in Chicago, IL, as well as a triple [shooting](#) at a bar in Colerain Township, OH. Both of the aforementioned incidents took place in the states with the highest contributions to gun violence alerts this week. California continues to lead the way in natural disaster alerts as well, as firefighters are working to contain several wildfires, including the Park Fire, the Boise Fire, and the Canyon Fire.

| 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%