



Weekly Intelligence Brief

Classification: TLP:GREEN

September 2, 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 30, 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 Brief – Underground Economist: Volume 4, Issue 16	2
ZeroFox Intelligence Flash Report – Israeli Defense Organization Targeted in New Data Breach	2
 Cyber Intelligence Key Findings	4
Iranian Hackers Posing as Recruitment Firms in Sophisticated Espionage Campaign	4
Telegram Channels Propagating Deepfake Pornographic Material Terrorize South Korean Women	5
Secret Service and FBI Collaboration Places USD 2.5 Million Bounty on Information on Prolific Cybercriminal	6
 Deep and Dark Web Intelligence Key Findings	8
Threat Actor LulzSec Muslims Allegedly Hacks Argentine Air Force Website	8
IntelBroker Claims Breach of Advanced Micro Devices' Internal Communications	8
CloAk Ransomware Claims Attacks on U.S. and European Physical Supply Chain Entities	9
 Exploit and Vulnerability Intelligence Key Findings	11
CVE-2024-39717	11
CVE-2024-31214	12
 Ransomware and Breach Intelligence Key Findings	15
Ransomware Attacks Target Industries and Critical Sectors	15
Data Breaches Hit a Range of Key Industries	17
 Physical and Geopolitical Intelligence Key Findings	20
Physical Security Intelligence: Global	20
Physical Security Intelligence: United States	22
 Appendix A: Traffic Light Protocol for Information Dissemination	23
 Appendix B: ZeroFox Intelligence Probability Scale	24

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Brief – Underground Economist: Volume 4, Issue 16

On August 20, 2024, threat actor “goodluck” posted in the dark web forum Exploit, announcing that a new version of their Octo 1 malware, Octo 2, is now available. Octo 1 is a popular Android remote access banking trojan that has been highly sought after amongst threat actors since a similar bot named “Sova” ceased to be available following a 2021 exit scam. On August 18, 2024, positive-reputation threat actor “D3M0N” posted in the dark web forum Exploit advertising a new loader malware with an allegedly limited availability. On August 12, 2024, positive-reputation actor “Oxel” announced in the deep and dark web (DDW) forum xss that they are now offering a new stealer malware named “Banshee”, which is designed to steal data from MacOS users. On August 11, 2024, positive-reputation actor “streetsphinx” posted in the popular hacking forum BreachForums advertising over 2,000 alleged zero- and one-day vulnerabilities for sale.

ZeroFox Intelligence Flash Report – Israeli Defense Organization Targeted in New Data Breach

On August 22, 2024, the hacktivist collective “Handala” posted in DDW forums announcing a data breach targeting an Israel-based organization that specializes in the design and development of embedded electronic systems for industrial and military customers. On August 25, 2024, Handala posted a subsequent thread revealing a number of allegedly top-secret design schematics related to electronic equipment used by what they referred to as the “Zionist Air Force.” Since it was first observed in December 2023, Handala has allegedly conducted attacks against a wide range of organizations based in Israel and other countries perceived as sympathetic to Israeli strategic objectives. If the stolen information is as described, it is very likely to attract interest from an array of threat actors, from politically impartial cybercriminals seeking to enhance their social engineering campaigns to state-aligned or state-associated actors able to exploit data relating to military hardware and pursue a strategic advantage.

| Cyber Intelligence |

| Cyber Intelligence Key Findings



Iranian Hackers Posing as Recruitment Firms in Sophisticated Espionage Campaign

What happened: Cybersecurity researchers have uncovered a sophisticated espionage operation linked to a threat actor with alleged ties to the Iranian Revolutionary Guard that used a fake professional recruiting business to ensnare national security officials from Iran, Syria, and Lebanon. The threat actor, identified as loosely connected to “APT42” or “Charming Kitten,” has been engaging in this operation since at least 2017 and is involved in creating several counterfeit Human Resources (HR) companies, such as VIP Human Solutions and Optima HR, to lure military and intelligence personnel. These fronts were promoted through fake profiles across social media platforms like Telegram, X (formerly Twitter), and Virasty. The aim was to identify individuals willing to collaborate with Israel and Western governments. The Federal Bureau of Investigation (FBI) is investigating APT42’s broader efforts to influence the 2024 U.S. election.

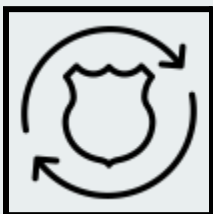
- **What this means:** The sophistication demonstrated via fake recruiting firms to target high-level military and intelligence personnel points to the adversary’s malicious intentions. By disguising themselves as Israeli-controlled entities, the Iranian hackers sought to create a false sense of trust among their targets, potentially extracting sensitive information about individuals interested in cooperating with adversarial countries. The operation is likely aimed at exposing and persecuting individuals engaged in intelligence activities against Iran, as the collected data includes personal and contact details. With the current geopolitical scenario dotted with increasing hostilities against Iran, more and more nation-state actors are turning to deceptive tactics to infiltrate sensitive networks and extract valuable intelligence. The operation is likely to aid Iran’s efforts in obtaining strategic intelligence to be used in broader operations against states that oppose its ideologies. Additionally, the alleged nexus between the threat actor and Charming Kitten indicates that the espionage operation is likely not an isolated operation but, rather, a part of APT42’s ongoing efforts to interfere with the upcoming U.S. elections. The FBI is investigating APT42’s activities, including its previous attempts to breach U.S. presidential campaigns. In May and June, APT42 [targeted](#) about a dozen people linked to the campaigns of former President Donald Trump and current President Joe Biden, including current and former government officials and campaign staffers from both political parties.



Telegram Channels Propagating Deepfake Pornographic Material Terrorize South Korean Women

What happened: Numerous Telegram chat rooms in South Korea have recently been discovered creating and distributing deepfake pornographic material featuring doctored photos of women, including minors, students, teachers, and military personnel. Many of these chat rooms, some with over 133,000 members, are organized by university names and linked to social media platforms where perpetrators illicitly obtain victim photos. Police investigations have revealed that these groups share bot programs for generating deepfake videos.

- **What this means:** These chat rooms exploit and victimize women from diverse age groups and backgrounds through deepfake pornographic material. The use of doctored images to create such content not only invades personal privacy but may also have psychological and emotional repercussions for the victims. The fact that minors, university students, teachers, and even military personnel are being targeted underscores the widespread nature of this abuse and the disregard for personal boundaries. South Korean authorities have been [addressing](#) similar cases, which appear to be increasing due to the growing availability of artificial intelligence (AI) tools. Social media posts reveal that victims of these chat rooms and those speaking out against the deepfakes are now being doxxed on various platforms, with their identities and personal information being exposed. This exposure poses significant risks, as malicious individuals could use this sensitive information for targeted attacks, potentially leading to serious physical threats. Meanwhile, following the incident, South Korean [authorities](#) have called on Telegram and other social media platforms to cooperate in removing and blocking sexually explicit deepfake content to address growing public and political concerns. The Korea Communications Standards Commission will establish a 24-hour hotline for victims and increase its regulatory personnel from 70 to 140 to better monitor digital sex crimes. The Korean National Police Agency plans to launch a seven-month campaign to combat online sex crimes.



Secret Service and FBI Collaboration Places USD 2.5 Million Bounty on Information on Prolific Cybercriminal

What happened: The Secret Service, in collaboration with the U.S. Department of State, has announced a reward of up to USD 2.5 million for information instrumental in arresting or convicting a Belarusian national suspected of several cybercrimes. The individual is reportedly involved in a decade-long malvertising scheme that deployed malware via online ads, compromising millions of devices. In addition to deploying the Angler Exploit Kit (AEK) and other forms of malware, the individual also allegedly engaged in "scareware" ad campaigns. These ads were reportedly aimed at tricking internet users by displaying alarming false messages that claimed to have detected a virus or other critical issue on their devices.

What this means: This individual is highly sought after because they are suspected of being involved in a decade-long cybercrime operation that has inflicted widespread harm on millions of unsuspecting users, including the deployment of the AEK and "scareware" ads. The scare tactics were intended to panic victims into taking immediate action, such as purchasing or downloading harmful software, granting remote access to their devices, or revealing sensitive personal or financial information. The suspected cybercriminal's activities involved a sophisticated and malicious campaign involving the transmission of the AEK and other malware through deceptive online advertisements known as malvertising. From October 2013 to March 2022, the individual and his collaborators deployed these malicious but legitimate-looking ads, enticing millions of unsuspecting internet users to click on them. Once clicked, the ads often redirected victims to malicious websites or servers, where their devices were compromised with malware. By deploying the AEK and other malware through seemingly legitimate online advertisements, the individual and his collaborators compromised countless devices, leading to financial losses, data breaches, and the unauthorized access and control of personal information. Their malvertising campaigns not only defrauded individuals but also likely contributed to a broader ecosystem of cybercrime, whereby access to compromised devices and stolen data is sold on cybercriminal forums. Law enforcement activity in taking down such cybercriminals and groups has likely played an essential role in limiting global cyber activities that cause millions in losses and reputational damage. AEK malware campaigns are likely enough of a global concern that law enforcement has zeroed in on them, as seen in the extradition and [charge](#) of the "Ransom Cartel" owner this month.

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings



Threat Actor LulzSec Muslims Allegedly Hacks Argentine Air Force Website

What happened: On August 23, 2024, threat actor group “LulzSec Muslims” claimed to have compromised the Argentine Air Force’s website in retaliation for the ongoing casualties in Gaza. The group managed to breach the server, delete all files, and replace the site with a message denouncing countries that support Israel. This attack is part of the group’s broader campaign against entities it perceives as aligned with Israel. LulzSec Muslims vowed to continue these digital assaults, targeting organizations it believes are complicit in the ongoing Israel-Hamas conflict.

- **What this means:** This incident illustrates the growing trend of cyberattacks being used as tools for political and ideological protest, especially in response to international conflicts. LulzSec Muslims’ attack highlights the ease with which hacktivist groups can target national entities to draw attention to global issues. The breach not only compromises national security but also sets a precedent for similar groups to use cyber operations as a form of digital protest. Threat actors might exploit this approach to gain publicity, further polarize conflicts, or pressure governments indirectly through cyber sabotage.



IntelBroker Claims Breach of Advanced Micro Devices’ Internal Communications

What happened: On August 25, 2024, threat actor groups “IntelBroker” and “EnergyWeaponUser” claimed to have breached Advanced Micro Devices (AMD), a U.S.-based multinational information technology (IT) company and semiconductor provider. The attackers claimed to have accessed sensitive data from AMD’s platforms, including case numbers, user credentials, and internal review statuses. The attackers also allegedly obtained data from the company’s internal Okta platform. The attackers have shared samples of the breached data and have indicated their willingness to provide further proof upon request. This breach is reportedly unrelated to previous cyber incidents associated with AMD.

- › **What this means:** This breach highlights the increasing sophistication of threat actors targeting critical technology firms. By compromising internal communications, attackers could potentially gain insights into AMD's internal processes, intellectual property, or customer-related issues, which could be exploited for further attacks or sold on dark web forums. The involvement of platforms like Okta suggests that the attackers may have obtained access to highly sensitive identity and access management data, which could be leveraged to impersonate users or escalate privileges within AMD's network. This incident underscores the necessity for robust security controls around internal communication and identity management systems—especially for entities in the technology and semiconductor industries.



CloAk Ransomware Claims Attacks on U.S. and European Physical Supply Chain Entities

What happened: On August 27, 2024, ZeroFox observed several new victims' data published on "CloAk Ransomware"'s leak site. Among the alleged victims are HVB Ingenieurgesellschaft, a Germany-based company focused on transport infrastructure, civil engineering, electrical engineering, and landscape planning; Dunlop Aircraft Tyres, an England-based manufacturer and supplier of aircraft tires; St. James Place, a U.S.-based retirement care community; and Westermans International, an England-based company that provides refurbished welding machinery and plasma-cutting equipment services. The alleged victims have not yet confirmed the leaks.

- › **What this means:** This recent string of ransomware attacks demonstrates the continued prevalence of financially motivated cybercrime. Emerging between the end of 2022 and the beginning of 2023, CloAk Ransomware initially focused most of its targeting on German and European entities. However, the group appears to be expanding to other areas of the world such as the United States and the United Kingdom, as seen in the above victims. As is typical with most ransomware groups, CloAk's first step in its attack chain is to gain access to a victim's network, most likely through a form of phishing. While ZeroFox cannot definitively confirm if the initial access vectors in the above breaches were via phishing, ensuring employees are able to identify phishing emails is critical for companies to maintain hardened cybersecurity defenses. Additionally, threat actors are increasingly targeting the physical supply chain in an effort to make quick money, attacking critical manufacturing companies and healthcare providers in particular. As such, these companies should practice a heightened level of cyber hygiene.

| **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, and government security domains. Cybersecurity researchers [found](#) another critical-severity vulnerability in the widely used WPS Office applications ([CVE-2024-7263](#)) that is exploited in the wild by a South Korea-linked advanced persistent threat (APT) actor. What makes this vulnerability dangerous is that the app is used by both major Chinese entities and civilians, making them vulnerable to spying and having sensitive data stolen. The Russian state-sponsored hacking group “[APT29](#)” has been using iOS and Android exploits from commercial spyware vendors in cyberattacks between November 2023 and July 2024. In July 2024, APT29 utilized exploits for CVE-2024-5274 and CVE-2024-4671 to attack Android users visiting the website [mga.gov\[.\]mn](#). Hitachi recently [released](#) an advisory addressing several vulnerabilities affecting the Hitachi Energy MicroSCADA X SYS600 product. The company released patches for five vulnerabilities, including two critical vulnerabilities (CVE-2024-4872 and CVE-2024-3980). Fortra FileCatalyst Workflow (web-based file exchange and sharing platform) has a critical SQL injection [vulnerability](#) (CVE-2024-5276) that allows remote unauthenticated attackers to create unauthorized admin accounts and manipulate data in the application database. FileCatalyst Workflow, utilized globally for large file transfers and private cloud collaboration, is impacted by this flaw. The Cybersecurity and Infrastructure Security Agency (CISA) recently [added](#) a known vulnerability to its catalog (CVE-2024-7965) based on evidence of active exploitation. Inappropriate implementation in V8 in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise.



HIGH

CVE-2024-39717

What happened: CVE-2024-39717 is a high-severity flaw that allows attackers to hijack credentials and infiltrate downstream customer networks. Versa Networks disclosed this bug and stated that the exploit occurs when firewall guidelines are not properly implemented. CISA [added](#) CVE-2024-39717 to its Known Exploited Vulnerabilities Catalog based on evidence of active exploitation on August 23.

- **What this means:** Cybersecurity researchers have observed Chinese APT group “Volt Typhoon” exploiting the bug as a zero-day. Volt Typhoon is known to exploit bugs to target key organizations across the globe. It [breached](#) the Dutch Ministry of Defence last year and deployed the COATHANGER RAT on compromised devices. The group exploited FortiOS vulnerabilities to target Dutch systems for information-gathering purposes. It is likely that the group will leverage this bug to target crucial entities.
- **Affected products:**
 - Versa Director GUI version 22.1.4
 - Versa Director GUI version 22.1.3
 - Versa Director GUI version 22.1.2
 - Versa Director GUI version 22.1.1
 - Versa Director GUI version 21.2.3
 - Versa Director GUI version 21.2.2



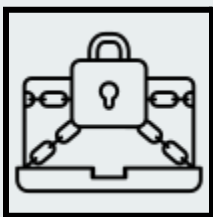
CRITICAL **CVE-2024-31214**

What happened: Traccar, an open-source GPS tracking system, has a critical vulnerability (CVSS score: 9.7) in versions 5.1 through 5.12 that allows arbitrary file uploads via the device image upload API. Attackers can fully control the file contents, directory, and file extension and partially control the file name. Although existing files cannot be overwritten, attackers can create new files with chosen names and extensions anywhere on the file system, potentially leading to remote code execution, cross-site scripting (XSS), or denial-of-service (DoS) attacks. This issue is exacerbated by Traccar's default settings, which enable self-registration and run with root/system privileges, increasing the risk of exploitation. Version 6.0 addresses this vulnerability, and disabling self-registration by default can significantly reduce its severity.

- **What this means:** This critical vulnerability in Traccar poses a significant security risk, as it allows attackers to upload arbitrary files with controlled names and extensions, potentially leading to severe consequences like remote code execution, XSS, or DoS attacks. If left unpatched, the flaw could enable malicious actors to exploit the system's default settings, which run with elevated privileges and permit self-registration. This could compromise the entire server, expose sensitive data, and disrupt services, making it crucial to update to version 6.0 and adjust default settings to mitigate these risks.
- **Affected products:** Traccar versions 5.1 to 5.12

Ransomware and Breach Intelligence

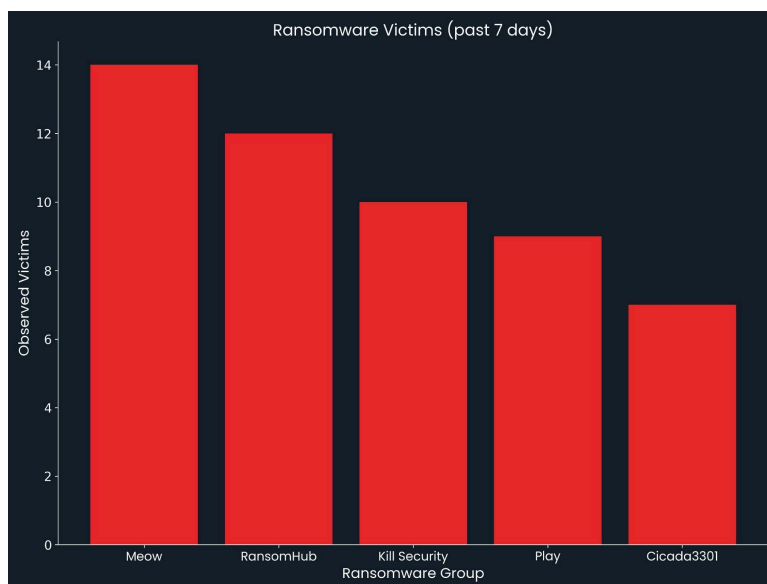
Ransomware and Breach Intelligence Key Findings



Ransomware Attacks Target Industries and Critical Sectors

What happened: Cybersecurity researchers have [identified](#) a new tactic used by “Qilin” ransomware in a July 2024 attack, wherein it not only deployed ransomware but also stole credentials stored in browsers across victim networks. The attackers accessed a VPN portal using compromised credentials, likely bought from an initial access broker, and then moved laterally to compromise the network. Patelco Credit Union confirmed that 726,000 customers were [affected](#) by a data breach resulting from a “[RansomHub](#)” ransomware attack on June 29, 2024.

The attackers gained unauthorized access to Patelco's network in May, stole sensitive personal information, and leaked it online on August 15, 2024, after negotiations failed. CISA has [released](#) an advisory about RansomHub this week to disseminate its known Indicators of Compromise (IOCs) and tactics, techniques, and procedures (TTPs). Young Consulting (now Connexure) is [notifying](#) 954,177 individuals of a data breach resulting from a “BlackSuit” ransomware attack on April 10, 2024. The breach, discovered three days after the attack, exposed sensitive data, including full names, Social Security numbers, dates of birth, and insurance claim information. ZeroFox intelligence had [observed](#) BlackSuit leaking a dataset allegedly associated with Young Consulting on its darknet portal in May. In other news, ZeroFox Intelligence also observed Play ransomware [claiming](#) responsibility for the recent attack on Microchip Technology, a prominent U.S. semiconductor manufacturer. The attack disrupted Microchip's servers and operations, leading to system isolation and an ongoing investigation. The “BlackByte” ransomware group has been [exploiting](#) a recently patched bug to escalate privileges and control virtual machines. BlackByte



Source: ZeroFox Internal Collections

used a mix of vulnerable drivers to bypass security measures and leveraged valid VPN credentials for initial access. Meanwhile, CISA and the FBI have [released](#) an advisory warning that Iranian cyber actors, known in the private sector as “Pioneer Kitten,” are targeting and exploiting U.S. and foreign organizations across multiple sectors in the United States. A significant percentage of the group’s U.S.-focused cyber activity is obtaining and maintaining technical access to victim networks to enable future ransomware attacks.

- **What this means:** The Qilin group’s strategy of stealing Chrome credentials during a ransomware attack signals a dangerous evolution in cybercrime tactics. By harvesting browser credentials, the attackers can access additional sensitive systems and accounts within the victim’s network, extending the impact beyond the initial ransomware infection. This approach could lead to further breaches, long-term access, or even future attacks on new targets, making it crucial for organizations to bolster their security measures, especially around credential storage and access controls. With Patelco officially confirming that 726,000 customers were impacted, the breach’s scale is now clear. The significantly high number of victims indicates the extensive exposure of personal data, raising serious concerns about identity theft and fraud. Patelco’s mitigation measures will aid affected individuals by enrolling them in complimentary identity protection and credit monitoring services for two years. In the #StopRansomware: RansomHub advisory, CISA states RansomHub has encrypted and exfiltrated data from at least 210 victims representing the water and wastewater, information technology, government services and facilities, healthcare and public health, emergency services, food and agriculture, financial services, commercial facilities, critical manufacturing, transportation, and communications critical infrastructure sectors. One of its latest victims is Halliburton, an oil and gas services giant, which [disclosed](#) the attack in late August. Similar to Patelco, the Young Consulting breach poses significant risks to those affected, as their personal information is now publicly exposed. Individuals should promptly utilize the offered credit monitoring service and stay alert for phishing and scamming attempts. The ransomware attack on Microchip Technology could severely impact the semiconductor supply chain, affecting industries reliant on its products, including automotive and defense. The disruption may delay production and deliveries, exacerbating the ongoing semiconductor shortage. Additionally, the public release of stolen data could compromise sensitive intellectual property and trade secrets, undermining industry security and competitiveness. Meanwhile, the rapid exploitation by BlackByte of a recently patched bug indicates the group’s agility in adapting to new vulnerabilities. By using valid VPN credentials and vulnerable drivers, the adversary effectively circumvents traditional security defenses. In the “Iran-based Cyber Actors Enabling Ransomware Attacks on U.S. Organizations” advisory, the FBI has stated that a significant percentage of Iranian threat actors’ operations against U.S. organizations are intended to obtain and develop network

access to collaborate with ransomware affiliate actors to deploy ransomware. The FBI further assesses these Iran-based cyber actors to be associated with the Government of Iran (GOI) and—separate from the ransomware activity—they are known to conduct computer network exploitation activity in support of the GOI (such as intrusions enabling the theft of sensitive technical data against organizations in Israel and Azerbaijan).



Data Breaches Hit a Range of Key Industries

What happened: Data breaches are increasingly prevalent, targeting a broad spectrum of key industries and exposing critical sectors to significant security risks and operational disruptions. The Iranian hacking group “APT33” (aka “Peach Sandstorm” and “Refined Kitten”) has [utilized](#) a newly developed Tickler malware in an intelligence campaign targeting U.S. and UAE organizations across the government, defense, satellite, oil, and gas sectors from April to July 2024. Park’N Fly, a major Canadian off-airport parking provider, [suffered](#) a data breach in July 2024 that exposed the personal and account information of approximately one million customers. The breach occurred through stolen VPN credentials. The company has reportedly confirmed that no financial or payment card information was affected. ZeroFox Intelligence observed “IntelBroker,” in conjunction with “EnergyWeaponUser,” [leaking](#) a database allegedly associated with AMD, a well-known U.S.-based semiconductor manufacturing company, on BreachForums. The actor claims that AMD suffered a data breach recently, leading to the exposure of information related to its internal communications. The actor also claimed that the data came from multiple sources, including [idmprod.xilinx\[.\]com](#) and [amdsso.okta\[.\]com](#). Dick’s Sporting Goods, an American sporting goods retailer, recently [discovered](#) that an unauthorized third party accessed its information systems, including confidential data. The company promptly involved external cybersecurity experts to investigate and address the issue and has notified federal law enforcement (LE). It is not yet known if the incident has impacted business operations.

- **What this means:** Affiliated with the Iranian Islamic Revolutionary Guard Corps (IRGC), APT33 used Tickler malware and exploited popular cloud services for command-and-control (C2) operations as part of an intelligence-gathering campaign. The group used fake cloud service subscriptions for C2, aiming to access multiple accounts without triggering security alerts or account lockouts by employing common passwords. Its targets included sectors such as government, defense, satellite, oil, and gas, which are valuable due to their sensitive and strategic information crucial to national

security and infrastructure. This suggests that APT33 was likely motivated by political interests or aimed to attract politically motivated actors with the intelligence it gathered. The breach at Park'N Fly impacts a substantial number of customers by exposing their full names, email addresses, physical addresses, Aeroplan numbers, and CAA numbers, which significantly increases the risk of identity theft and fraud. The exposed personal information can facilitate targeted phishing and scam attempts, while the compromised Aeroplan and CAA numbers may lead to account hijacking and fraudulent activity within loyalty and membership programs. Additionally, this incident also raises broader concerns about the security of customer data and the need for companies to minimize data retention to mitigate such risks. Attacks on semiconductor companies are significant because these firms produce key components used in a wide range of technology, from everyday gadgets to critical defense systems. Given the semiconductor industry's role, stolen internal communications can be leveraged for various malicious activities, including sabotaging supply chains, stealing cutting-edge technology, threatening national security, undermining market positions, and manipulating financial markets. Additionally, the stolen data from AMD can be used for corporate espionage, phishing attacks, operational disruption, or ransom demands. The alleged data from various sources suggests a more extensive and damaging breach, offering a broader view of an organization's operations and vulnerabilities. The breach at Dick's Sporting Goods is concerning as it involves the theft of confidential data, potentially exposing customers to identity theft or fraud. For the company, this incident could lead to reputational damage, loss of customer trust, and potential financial repercussions from legal and regulatory consequences. To reduce the risks associated with data breaches, customers and companies should adopt strong security practices, such as multi-factor authentication, regular system updates, and data encryption. Additionally, they should remain vigilant for any unusual activity and limit the retention of unnecessary data.

| Physical and Geopolitical Intelligence |

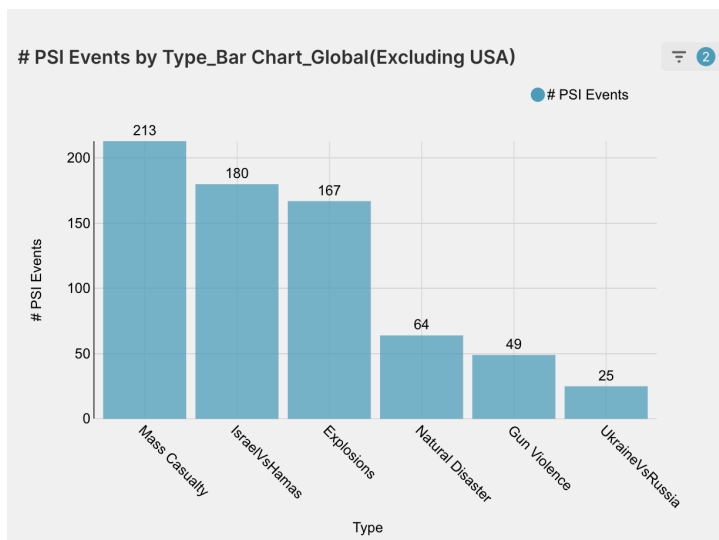
Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

What happened: Excluding the United States, the world saw a 3 percent decrease in Mass Casualty incidents perpetrated across the globe, with Palestine, Lebanon, and Israel being the largest contributors in this category this week; 47 percent of the events in those countries were Mass Casualty incidents. General Alerts pertaining to the Israel-Hamas conflict increased by 6 percent this week. Both Israel and Hamas contributed to 43 percent of all the total explosions incidents this week.

Additionally, with regard to the ongoing Russia-Ukraine conflict, the stats showed

a 50 percent increase in the events this week. The top three most alerted subtypes this week were Explosions, Natural Disaster, and Gun Violence. Of those, Explosions showed a 6 percent decrease, and Natural Disaster and Gun Violence increased by 14 percent and 55 percent, respectively, compared to the previous week.



Source: ZeroFox Internal Collections

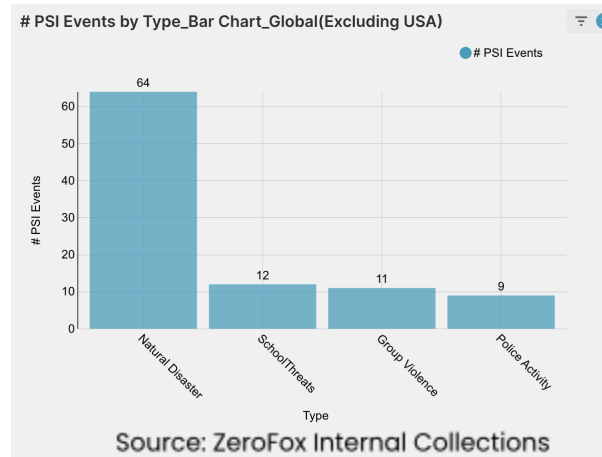
- What this means:** This week, the alerts related to the Israel-Hamas conflict showed a significant increase owing to the continued escalating tensions in the region. The week saw an increase in shooting incidents, with multiple casualties and several cases of explosion incidents in the region. More than 70 people were killed across Gaza in incidents across the week. Over the weekend, Lebanon's Hezbollah and the Israeli Defense Forces engaged in [rocket attacks across the border](#). Most of these bombings were concentrated in the Northern Israel region. ZeroFox saw coordinated attacks on Gaza, Khan Yunis, Tulkarm, Ramallah, and Jenin on Wednesday night. With a peace agreement yet to be signed, the violence will continue to persist. Alerts related to the ongoing war in Ukraine have also increased significantly this week. Both Russia and Ukraine saw increased bombing and airstrikes on its cities this week. There was a major hostage incident at the [IK19 prison](#) in Surovikino, Russia, which resulted in the death of four prison officials; ISIS is suspected of being responsible for the attacks. Natural Disaster incidents increased by a small percentage this week as rains continued to hit the Western Coast of [India and Pakistan](#)

due to cyclones forming in the Arabian Sea. Twenty-eight people have lost their lives this week due to the rains in the coastal states of both India and Pakistan. As stated in last week's Weekly Intelligence Brief, ZeroFox anticipates further incidents related to rains in the South Asian region, as monsoon season is expected to continue until the end of September.

Physical Security Intelligence: United States

What happened: In the past week, the three most alerted subtypes were Natural Disaster, Gun Violence, and Police Activity. The top two states that had the highest number of Gun Violence alerts were Illinois and California, which made up 37 percent of the total alerts in the category. Gun Violence across the United States showed a 12 percent decrease compared to the previous week. The top two states contributing to the Natural Disaster alerts were California and Florida; the alerts showed a negligible

decrease of 0.5 percent compared to last week. Similarly, the two states with the highest contribution to the Police Activity subtype were California and Texas. This subtype showed a 57 percent increase compared to the previous week. There were 105 alerts relating to school (excluding protests), an increase of 34 percent over last week.



- **What this means:** With schools reopening in the United States after the summer break, the generalized threat of violence towards the schools has shown an increase compared to last week. As per ongoing trends, this number may increase as cases of threats and swatting calls made to schools will likely continue to increase in the upcoming weeks. With police response to the incidents, both the School Threats and Police Activity tags are going to proportionally increase. Gun Violence showed a significant decrease; however, shooting incidents continued, with Chicago, Illinois, reporting [33 cases](#) of shooting and a [double shooting](#) on Carson Street in Los Angeles, CA over the weekend. Both the aforementioned incidents took place in states with the highest contribution to Gun Violence this week. Natural Disaster continued to be the most alerted subtype this week, with [Idaho and Oregon](#) having the highest number of active wildfires now followed by Montana, Washington, and Wyoming.

| 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%