



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

March 3, 2025

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 6:00 AM (EST) on February 28, 2025**; 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 5, Issue 4	2
ZeroFox Intelligence March 2025 Geopolitical Brief	2
 Cyber and Dark Web Intelligence Key Findings	4
North Korea's Lazarus Steals from Bybit in Major Attack	4
New Backdoor Targets Government and Educational Institution	5
Crypto Firm Gotbit Founder Charged for Market Manipulation and Wire Fraud	5
 Exploit and Vulnerability Intelligence Key Findings	7
CVE-2025-1751	7
CVE-2023-27853	8
 Ransomware and Breach Intelligence Key Findings	10
Ransomware Watch: Top Groups, Industry Trends, and Key Events	10
Prominent Data Breaches Observed in the Past Week	13
 Physical and Geopolitical Intelligence Key Findings	15
Physical Security Intelligence: Global	15
Physical Security Intelligence: United States	16
 Appendix A: Traffic Light Protocol for Information Dissemination	18
 Appendix B: ZeroFox Intelligence Probability Scale	19

| This Week's ZeroFox Intelligence Reports

[ZeroFox Intelligence Brief – Underground Economist: Volume 5, Issue 4](#)

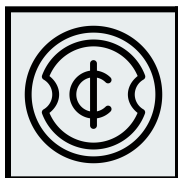
The Underground Economist is an intelligence-focused series illuminating dark web findings from our ZeroFox Dark Ops intelligence team.

[ZeroFox Intelligence March 2025 Geopolitical Brief](#)

U.S. tariffs are expected to start in March before progressing throughout April, very likely leading to supply chain disruptions. The new U.S. administration has telegraphed its desire to end both Russia's war in Ukraine and the Israel-Hamas war quickly. However, several powerful actors stand to lose from the security re-arrangements and will likely undercut U.S. aims. The ceasefire between Israel and Hamas negotiated by the Biden administration is likely to continue into March 2025 but collapse before being fully implemented, with the United States and Israel likely to pursue alternatives. The U.S. proposal to end Russia's war in Ukraine will likely include an implicit security guarantee for Ukraine, closer U.S.-Russia ties, billions in new European Union (EU) defense spending, and a U.S. military focused on China.

| **Cyber and Dark Web Intelligence** |

| Cyber and Dark Web Intelligence Key Findings



North Korea's Lazarus Steals from Bybit in Major Attack

What we know:

- North Korea's Lazarus Group stole USD 1.4 billion Ethereum (ETH) from a major global cryptocurrency exchange, Bybit.
- Investigations found that over 920 wallet addresses were involved in the laundering process.
- A coordinated effort by crypto security teams led to the freezing of USD 42.89 million in stolen assets.
- Bybit warned users about scammers impersonating employees and said that they would never request personal information, deposits, or passwords.
- The company also assured users that deposits and withdrawals have resumed despite the major hack.

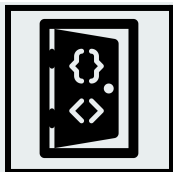
What is next:

- The stolen assets are likely being converted into Bitcoin and dispersed across thousands of addresses to evade law enforcement efforts in recovering them.
- [North Korea can launder the funds](#) and eventually convert them into fiat currency, bypassing international sanctions.
- The United States and its allies could impose additional sanctions or financial countermeasures targeting North Korean cyber operations.
- Proceeds will likely fund North Korea's nuclear and ballistic missile programs and expand its research and development, procurement of foreign components, and infrastructure capabilities.

Background:

- The Lazarus Group is a North Korean government-backed hacking organization that has been active since the early 2010s.
- It operates under the Reconnaissance General Bureau (RGB), North Korea's primary intelligence agency.
- Its attacks focus on stealing funds to bypass sanctions and finance military programs.

- The group has been observed using social engineering / phishing campaigns to target employees and executives with fake job offers and malware-infected files, as well as exploiting security vulnerabilities in crypto platforms, banks, and financial institutions.



New Backdoor Targets Government and Educational Institution

What happened: A newly discovered Linux backdoor dubbed “Auto-Color” has been targeting government and education institutions in North America and Asia. The backdoor is capable of running with and without root privileges, while being highly evasive and persistent; is difficult to remove from affected devices; and provides threat actors remote control.

- **What this means:** Given the backdoor’s features, government data is highly vulnerable to compromise by threat actors looking for financial gain and state-linked actors intent on achieving persistence to exfiltrate confidential information. This backdoor is likely particularly effective against government and educational institutions that use legacy systems like end-of-life routers and devices that have not patched past vulnerabilities, making them more susceptible to cyberattacks such as malware and phishing scams.



Crypto Firm Gotbit Founder Charged for Market Manipulation and Wire Fraud

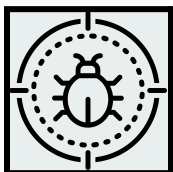
What happened: The founder of cryptocurrency financial services firm Gotbit has been charged for allegedly orchestrating a wide-ranging conspiracy to manipulate cryptocurrency markets on behalf of client cryptocurrency companies. The charges include wire fraud and conspiracy to commit market manipulation.

- **What this means:** Gotbit allegedly provided market manipulation services to create artificial trading volume for multiple cryptocurrency companies, including U.S.-based companies, resulting in proceeds of tens of millions of dollars. The firm allegedly marketed wash trading tactics to potential clients and explained how it utilized multiple accounts to evade detection of wash trading on the public blockchain. Such deceptive and fraudulent practices could endanger the financial assets of customers who have invested in these schemes and expose them to legal liabilities.

| **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 technology, software development, and critical infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA) released a total of four industrial control system (ICS) advisories on [February 24](#) and [February 25](#). CISA also has added four [vulnerabilities](#) to its Known Exploited Vulnerabilities ([KEV](#)) [catalog](#). The most recent version of [Parallels Desktop virtualization software for macOS](#) has an unpatched zero-day vulnerability that could enable root access. The [Cardealer theme for WordPress](#) is vulnerable to privilege escalation in versions up to, and including, 1.6.4 due to a missing capability check on the “save_settings” function. In [MITRE Caldera](#) through 4.2.0 and 5.0.0 before 35bc06e, a Remote Code Execution (RCE) vulnerability was found in the dynamic agent (implant) compilation functionality of the server. CVE-2025-26201 is a [credential disclosure vulnerability](#) via the /staff route in GreaterWMS <= 2.1.49 that allows remote unauthenticated attackers to bypass authentication and escalate privileges. [Adobe Commerce versions](#) 2.4.8-beta1, 2.4.7-p3, 2.4.6-p8, 2.4.5-p10, 2.4.4-p11, and earlier are affected by an Improper Authorization vulnerability that could result in privilege escalation.



CRITICAL

CVE-2025-1751

What happened: An SQL injection vulnerability has been identified in Ciges 2.15.5 by ATISoluciones. This flaw enables an attacker to retrieve, create, update, and delete database entries via the \$idServicio parameter in the /modules/ajaxBloqueaCita[.]php endpoint.

- **What this means:** This vulnerability allows attackers to execute unauthorized SQL queries against the database. By exploiting the \$idServicio parameter, attackers can retrieve sensitive data, add new data, modify existing records, or delete data. This could lead to severe consequences such as data breaches, service disruptions, or unauthorized access to private or business-critical information. It enables an attacker to manipulate the database by bypassing the usual security checks.
- **Affected products:**
 - ATISoluciones Ciges 2.15.5

**CRITICAL****CVE-2023-27853**

What happened: The NETGEAR Nighthawk Router WiFi6 prior to V1.0.10.94 has a format string vulnerability within one of its SOAP services. A format string vulnerability occurs when user input is improperly handled, allowing an attacker to inject malicious input that can be interpreted as code by the device. The SOAP service in this case did not adequately sanitize user input, potentially allowing attackers to execute arbitrary code remotely on the router.

- **What this means:** This vulnerability exposes users of the affected routers to the risk of RCE. If exploited, an attacker could gain control over the router, potentially compromising the security of the entire network. This would allow the attacker to access sensitive data, alter router configurations, or perform malicious activities without the user's knowledge. Since routers often serve as the gateway for home or small business networks, their compromise could lead to broader security risks for connected devices and sensitive personal or corporate information.

Affected products:

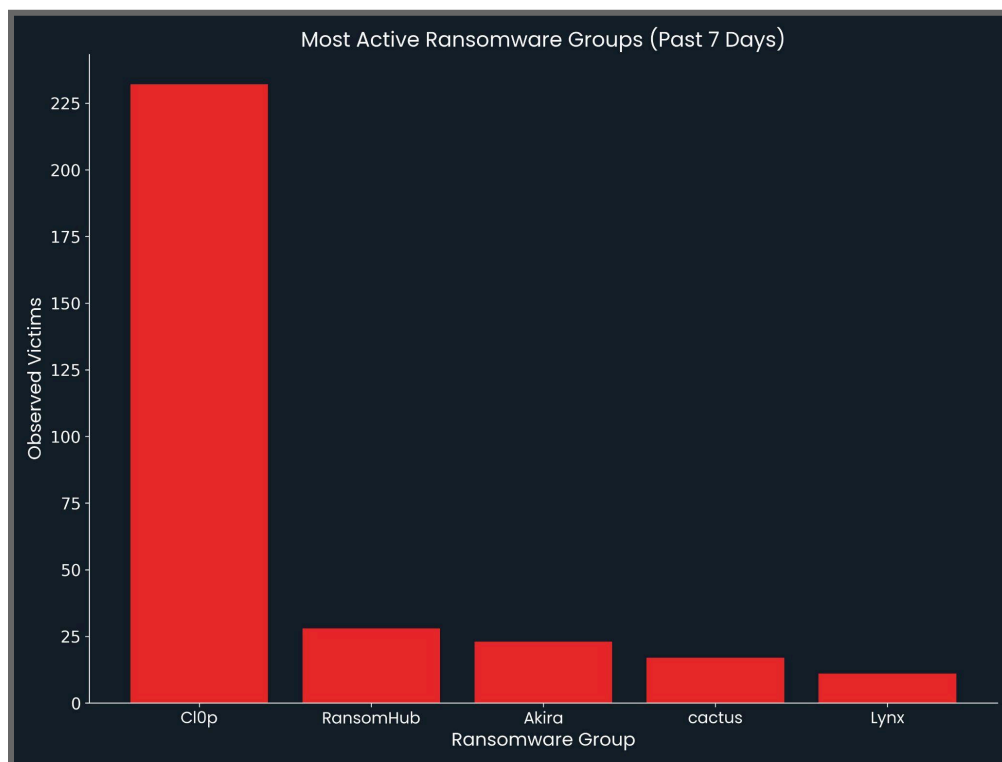
- NETGEAR Nighthawk WiFi6 Router prior to V1.0.10.94

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

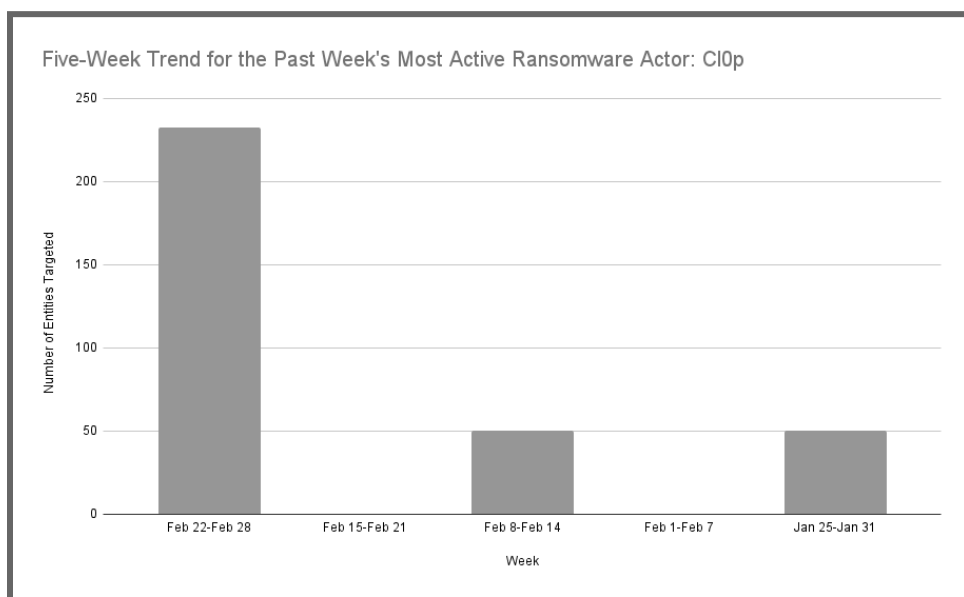


Ransomware Watch: Top Groups, Industry Trends, and Key Events



Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, ZeroFox observed at least 353 ransomware victims disclosed, most of which were located in North America; the manufacturing sector was the most affected, followed by retail. Cl0p remained the most active ransomware collective, unveiling its fourth (comprising 50 victims' names in the alphabetical range of E to H) and fifth list of victims (comprising 182 victims' names in the alphabetical range of H to W).

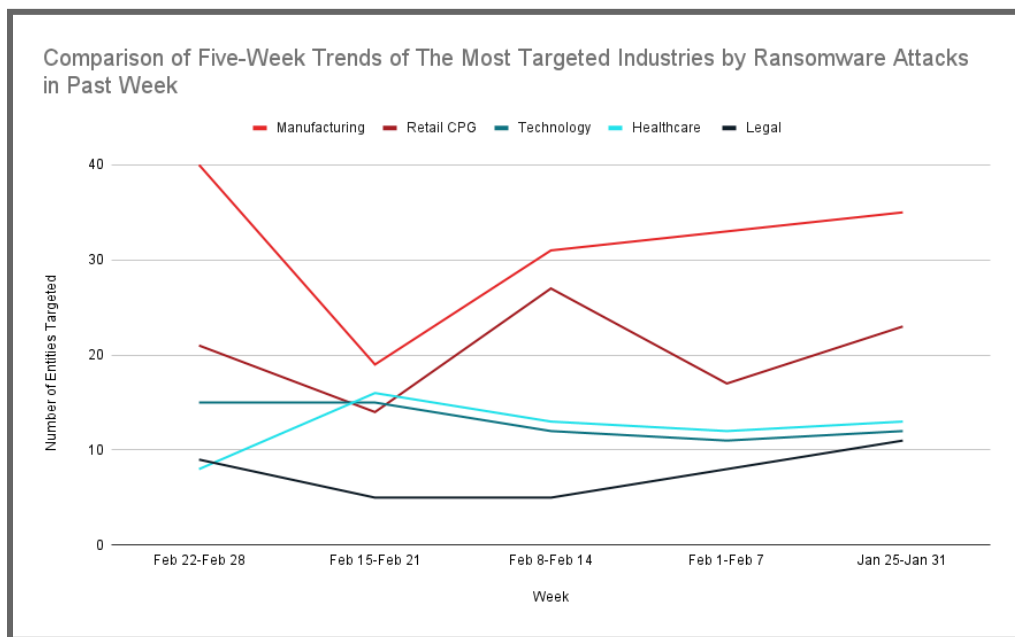


Source: ZeroFox Internal Collections

- **What this means:** In the past five weeks, CI0p has continued to make headlines with its list of victims, all of whom are likely victims of the same Cleo vulnerability exploit attack. Given the number and the alphabetical order of the victims in the fifth list, it is likely to be either the last or the next-to-last list of victims supposedly associated with the Cleo vulnerability exploit attack. CI0p also seemingly broke its pattern and has skipped the step of teasing a list, directly revealing the victim names.

Ransomware event in focus: Southern Water, a major UK water supplier, spent approximately GBP 4.5 million (USD 5.7 million) responding to a cyberattack by the Black Basta ransomware gang, which stole data from a limited part of its servers.

- **What this means:** This incident highlights the heavy financial toll ransomware attacks can have on firms involved in critical infrastructure. Additionally, Black Basta's internal chat logs were allegedly leaked last week, making it likely that law enforcement (LE) will be able to zero in on the group's tactics and operators. If the chats contain sensitive information about the group, Black Basta could pause its activities and re-build its operations to avoid LE disruption.



Source: ZeroFox Internal Collections

Ransomware trends in industries: In the past five weeks, ZeroFox has consistently observed most of the ransomware victims to be from the manufacturing sector. The number of ransomware victims observed from the retail industry is almost always higher than healthcare, except in the week of February 15 to February 21, when the number of observed healthcare targets surpassed those in the retail sector.



Prominent Data Breaches Observed in the Past Week

Targeted Entity	DISA Global Solutions	Various organizations	Genea
Number of Firms/Victims Affected	3.3 million individuals	90 organizations	Not disclosed
Compromised Data Fields	Social Security numbers, financial account information, credit card numbers, government-issued identification documents	Personal information	Contact details, Medicare card numbers, medical histories, test results, and medications (alleged)
Suspected Threat Actor	Yet to be determined	Aliases: DESORDEN Group, ALTDOS	Yet to be determined
Region	North America	Global	APAC
Industry	Professional services	Various industries	Healthcare
Possible Repercussions	Extortion, ransom demands, identity theft, and phishing attacks	Extortion, blackmail, and dark web sale	Privacy violations, blackmail, intimidation, and extortion

Three major breaches observed in the past week

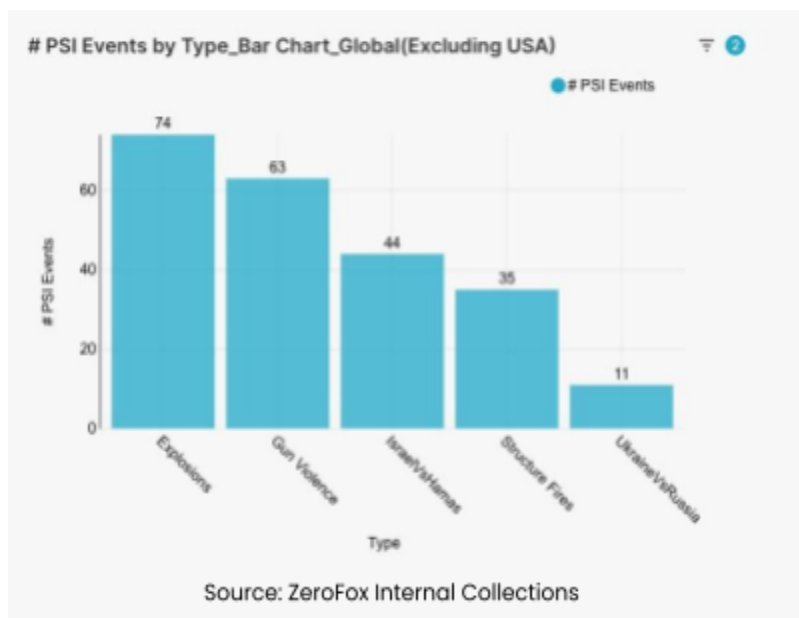
| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

What happened: Excluding the United States, ZeroFox observed a 17 percent decrease in mass casualty incidents perpetrated by elements across the globe, with Mexico, Syria, and Colombia contributing to the highest number of alerts in the category. The aforementioned countries contributed 43 percent of all the explosions recorded this week. General alerts pertaining to Israel-Hamas (including protests, raids, and involvement in the neighboring countries) showed a 46 percent decrease compared to the previous week. This week Israel and Palestine contributed 16 percent of the total

explosions. Additionally, the alerts pertaining to the ongoing Russia-Ukraine war showed a 27 percent decrease compared to the previous week. The three most-alerted subtypes this week were explosions (23 percent decrease), gun violence (3 percent decrease) and structure fires (25 percent increase).

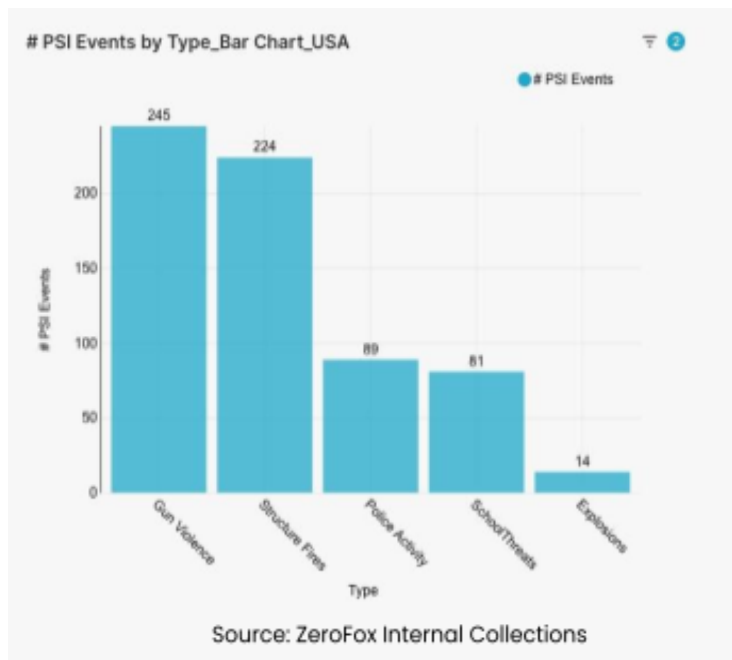


- **What this means:** This week Hamas released six hostages as part of the ceasefire agreement and also handed over the bodies of four others who were captured during the raids on October 7, 2023. Following suit, Israel released [600](#) prisoners of war, including women and children, as part of the deal. However, despite the ceasefire, there were instances of ceasefire violations recorded this week after drones and tanks were used to attack homes in the city of Rafah. In [Bat Yam](#), three buses were detonated with explosives as part of an attack protesting against the ongoing conflict. Two other inert explosive devices were also found on the scene. As of February 27, talks for the second round of ceasefire agreements have started to take place, with the Israeli Prime Minister sending a team to [Cairo](#) to start the negotiations. If the ceasefire talks continue, the Israeli Army is expected to fall back completely from Gaza and the Egyptian border, while Hamas is expected to hand over all living hostages in exchange for the remaining Palestinian prisoners. Despite a decrease in the percentage of alerts compared to the previous week,

the region saw conflicts with targeted bombing of the [Ozernoye Military Airport](#) and attacks using drones in the Tuapse and [Anapa](#) cities of Krasnodar Krai, Russia. On the political front, Ukraine President Vladimir Zelensky is scheduled to meet U.S. President Donald Trump to discuss the possibility of a ceasefire and to potentially sign an [agreement](#) giving the United States the right to mines in the Ukrainian region as a form of payment for all the aid given to Ukraine by the previous U.S. administration. In the city of [Bukavu](#) in the Democratic Republic of Congo (DRC), 11 people were killed and over 60 others were injured after two grenades were hurled at a M23 faction meeting involving a high-ranking leader. DRC has been facing a humanitarian crisis due to the ongoing power struggle involving the Congolese Government, the M23 rebel group, and various other armed factions. In [Bielefeld](#), Germany, on February 26, four people were shot by two suspects outside a courthouse in connection with an ongoing trial. Germany has been seeing a rise in mass casualty attacks, with the last one being a car-ramming in Munich.

Physical Security Intelligence: United States

What happened: Similar to the previous week, gun violence, structure fires, and police activity formed the three most alerted subtypes in the United States. California had the most number alerts in the gun violence category (41 alerts), while New York and Illinois were second with 19 alerts each. All three cities together contributed to 32 percent of all the alerts. In the structure fires category, New York and Texas contributed the highest number of alerts with a total of 59, contributing 26 percent of all total alerts. The third most-alerted subtype this week was police activity, with Florida contributing 11 alerts and New York and Texas contributing 10 each; the three states together contributed 35 percent of the total alerts. Compared to the previous week, the gas leak subtype increased by 29 percent.



- **What this means:** This week, U.S. gun violence incidents rose by 10 percent, with multiple incidents of mass casualty; gun violence remained a significant concern and a top category this week. In York, Pennsylvania, an armed individual entered the [UPMC](#) Hospital, where he shot and injured two doctors and a civilian and then opened fire at LE on the scene, injuring two officers and killing another. In [Lake Station](#), Indiana, two adults and three children were found dead during a welfare check; investigations later revealed that four were shot before the fifth person took his own life in the residence. Structure fires is one of the major incident subtypes that continues to be among the top three subtypes every week. However, this week saw a decrease in the number of alerts compared to the previous week, albeit the number was still large. ZeroFox anticipates this number decreasing as Winter ends and Spring begins in March. School threats are incidents that occur when police activity takes place within a school or in the vicinity of a school. Police presence at schools is becoming more prevalent as incidents of gun brandishing, threats of a mass shooting, or bomb threats are on the rise. An 11-year-old student was arrested this week after making threats to kill people in a school in [Nassau County](#), Florida. Compared to the previous week, incidents with the SchoolThreats tag increased 17 percent this week. Following similar trends seen last week, gas leak alerts increased this week by 28 percent.

| 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%