



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

October 17, 2026

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 (EDT) on October 15, 2026*; 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 – Ransomware Recovery CEO Charged for Secret Payments	2
ZeroFox Intelligence Flash Report – French Supermarket Cyberattack amid Civil Unrest	
Consistent with Pro-Russia Cyber Tactics	2
 Cyber and Dark Web Intelligence Key Findings	4
Threat Actor Group n0n Claims Extortion of 38 Shipping and Port Organizations Globally	4
China-Linked Phishing Ecosystem Disrupted	5
FBI Warns of Evolving North Korean IT Worker Scheme Targeting U.S. Companies	5
 Exploit and Vulnerability Intelligence Key Findings	8
CVE-2026-96951	8
CVE-2026-104935	8
 Ransomware and Breach Intelligence Key Findings	11
Ransomware Group, Industry, Regional Trends	11
Notable Data Breaches this Week	14
 Physical and Geopolitical Intelligence Key Findings	16
Physical Security Intelligence: Global	16
Physical Security Intelligence: United States	17
 Appendix A: Traffic Light Protocol for Information Dissemination	18
 Appendix B: ZeroFox Intelligence Probability Scale	19

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Flash Report – Ransomware Recovery CEO Charged for Secret Payments

On October 7, 2026, the owner and chief executive officer (CEO) of a ransomware recovery company was arrested and charged with one count of conspiracy to commit wire fraud and two counts of wire fraud. The CEO allegedly defrauded ransomware victims by claiming to use proprietary technology to recover encrypted data while reportedly paying the attackers for decryption keys. A ProPublica investigation from 2019 reported that security researchers had created their own ransomware and approached recovery companies posing as victims; the CEO reportedly contacted the fake ransomware group and offered to pay the ransom. This fraud and subterfuge incident is almost certainly an isolated example of unscrupulous actors in the cybersecurity industry. Fraud schemes from cybersecurity companies are very likely rare but represent a unique insider threat; they almost certainly present a secondary threat layer that businesses should keep in mind when developing their defensive operations and mitigation plans.

ZeroFox Intelligence Flash Report – French Supermarket Cyberattack amid Civil Unrest Consistent with Pro-Russia Cyber Tactics

ZeroFox assesses the October 11–12 cyberattack on French supermarket refrigeration systems is consistent with pro-Russia cyber techniques used against European states supporting Ukraine; no actor has claimed responsibility, and attribution remains unconfirmed. The attack is suspected to have exploited previously disclosed vulnerabilities in end-of-life or outdated Danfoss AK-SM 800A refrigeration controllers, including flaws that could allow authentication bypass and remote code execution (RCE). The attack occurred amid civil unrest that Russia-linked influence operations are almost certainly already exploiting. Organizations operating internet-exposed, end-of-life, or outdated Danfoss refrigeration controllers face elevated risk of similar attacks.

| Cyber and Dark Web Intelligence |

| Cyber and Dark Web Intelligence Key Findings



Threat Actor Group n0n Claims Extortion of 38 Shipping and Port Organizations Globally

What we know:

- On October 13, 2026, ZeroFox observed threat actor group "n0n" listing 38 organizations largely related to the shipping, port, and logistics sector (including support firms) on its dark web leak site in a single batch.
- The group threatened to publish stolen data unless ransoms are paid by October 19.

Background:

- The listed organizations include major port and container terminal operators, shipping lines, and port IT providers largely concentrated in the Asia-Pacific region, with South Korean entities topping the list. The target list also includes entities from the Middle East and South American regions.
- The stolen data allegedly includes port disbursement records, banking correspondence, demurrage and despatch financial records, vessel performance data, schedules, and infrastructure configuration files.

Analyst note:

- When n0n first emerged, the group's defining characteristic was targeting victim data backups. Its current maritime campaign shows no evidence of data backup targeting, very likely reflecting either a shift in tradecraft or an additional layer of targeting.
- The legitimacy of the claims cannot be determined, as none of the listed entities have confirmed the attack.
- ZeroFox noted some listed entities are attributed to incorrect regions, suggesting inconsistencies in the group's claims.
- If legitimate, the breach likely stems from the compromise of a shared environment.
- In the context of the Middle East conflict and cyber and physical attacks targeting vessels at strategic chokepoints, a sector-wide data breach is very likely to be leveraged in follow-on activities by financially and ideologically motivated actors, including state-backed groups.



China-Linked Phishing Ecosystem Disrupted

What we know:

- U.S. authorities and partners have seized and redirected domains used by a Chinese-language cybercrime ecosystem, including those of YAM Store, CoGUI, and Iron Man.
- The operation also disabled more than 20,000 associated accounts and blocked roughly 100,000 domains used for impersonation and fraud.

Background:

- The three illicit platforms reportedly provided infrastructure, compromised cloud accounts, and phishing kits for large-scale credential and payment data theft.
- They were also reportedly linked to more than one billion malicious messages targeting over 75,000 organizations across 150 countries, including more than 750 million messages targeting Microsoft customers since the start of 2026.

Analyst note:

- As the disruption affected multiple interconnected services spanning infrastructure provision and phishing operations, relaunching the ecosystem with fresh infrastructure is likely to be more difficult in the near term.
- Operators are likely to seek alternative infrastructure suppliers or migrate to other criminal ecosystems.



FBI Warns of Evolving North Korean IT Worker Scheme Targeting U.S. Companies

What we know:

- The U.S. Department of Justice (DOJ) announced a series of enforcement measures against North Korea's remote IT worker scheme and charged 14 individuals, arrested two U.S. nationals, and seized about 187 laptops and devices.
- The Federal Bureau of Investigation (FBI) has also warned that North Korean IT workers use legitimate network access to steal sensitive company data and conduct extortion to generate revenue for the regime.

Background:

- The FBI noted that North Korean IT workers are increasingly recruiting U.S.-based facilitators and subcontracting work to third country nationals as companies improve their ability to detect fraudulent North Korean employees.
- Recent cases also involve threats of physical violence against victims and targeting of positions requiring security clearances.

Analyst note:

- Operators are likely to refine techniques to evade law enforcement and circumvent identity and access checks. U.S. businesses and financial entities used by the threat actors to launder money for the operations are also likely to face law enforcement scrutiny if counter measures are not implemented.

| **Exploit and Vulnerability Intelligence** |

| Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in technology, software development, and critical infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA) added six new vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on [October 13](#) and [October 14, 2026](#). Additionally, CISA released two Industrial Control Systems (ICS) advisories on October 13, 2026, featuring [CVE-2026-92817](#) and [multiple other vulnerabilities](#). An authentication bypass vulnerability in Ivanti Connect Secure VPN appliances ([CVE-2026-104935](#)) was actively exploited in the wild alongside two additional zero-days. GitLab patched a critical integer overflow vulnerability in its continuous integration and continuous delivery (CI/CD) Regular Expression Compiler ([CVE-2026-97229](#)), and SonicWall patched a pre-authentication server-side request forgery flaw in SMA1000 appliances ([CVE-2026-102255](#)).



HIGH

CVE-2026-96951

What happened: Microsoft patched an actively exploited Windows Shell zero-day vulnerability enabling unauthenticated attackers to bypass Mark of the Web (MOTW) protections and evade security warnings.

- **What this means:** Unauthenticated attackers can potentially bypass MOTW protections to execute malicious files without triggering expected Windows security warnings.
- **Affected products:**
 - Windows Shell, .NET Framework, MessagePack-CSharp



HIGH

CVE-2026-104935

What happened: An authentication bypass vulnerability in Ivanti Connect Secure VPN appliances was actively exploited in the wild by threat actor “UTA0576”.

- **What this means:** UTA0576 reportedly chained the authentication bypass and RCE vulnerabilities covered by CVE-2026-104935 with a separate privilege-escalation zero-day

to achieve unauthenticated root-level code execution on a fully patched appliance. The actor then conducted credential theft and Active Directory reconnaissance..

> **Affected products:**

- Ivanti Connect Secure 25.1.1.1 and prior
- 25.1.2.2 and prior
- 22.8R2.4 and prior

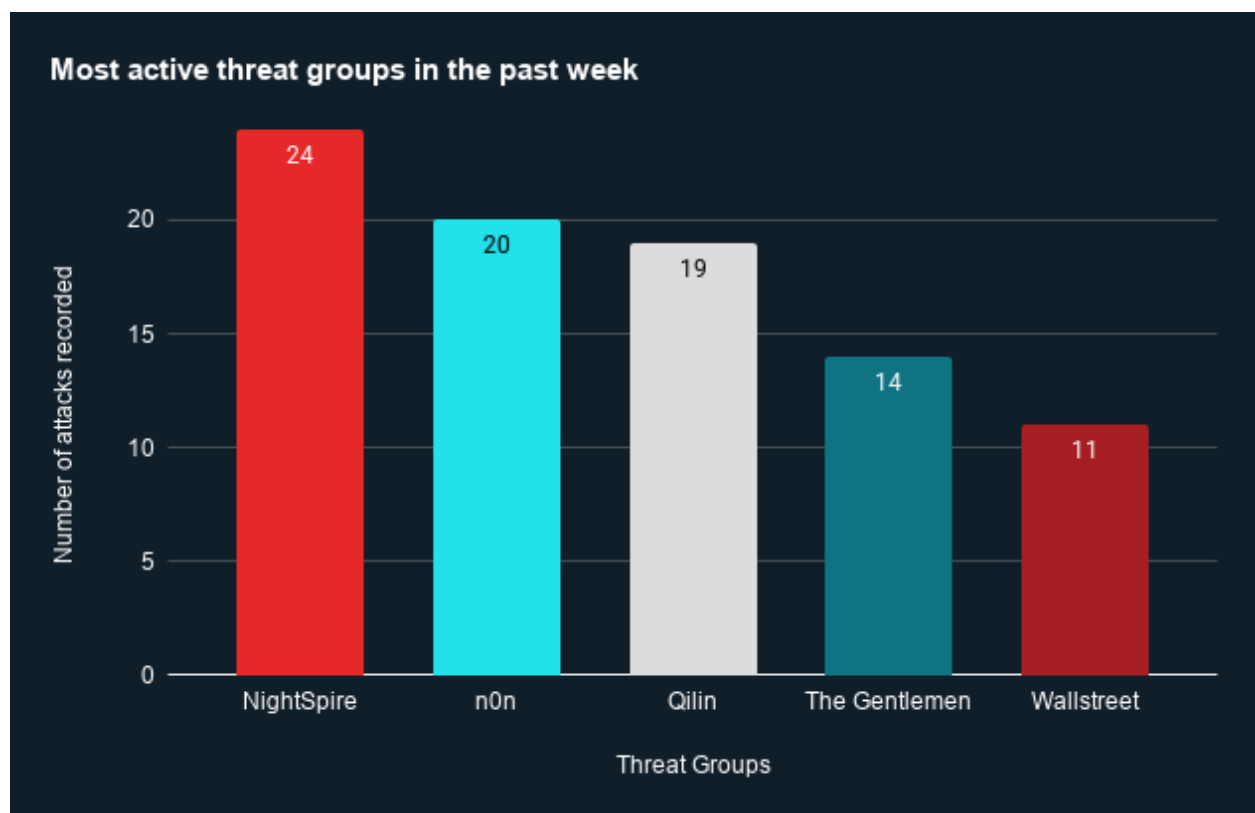
Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings



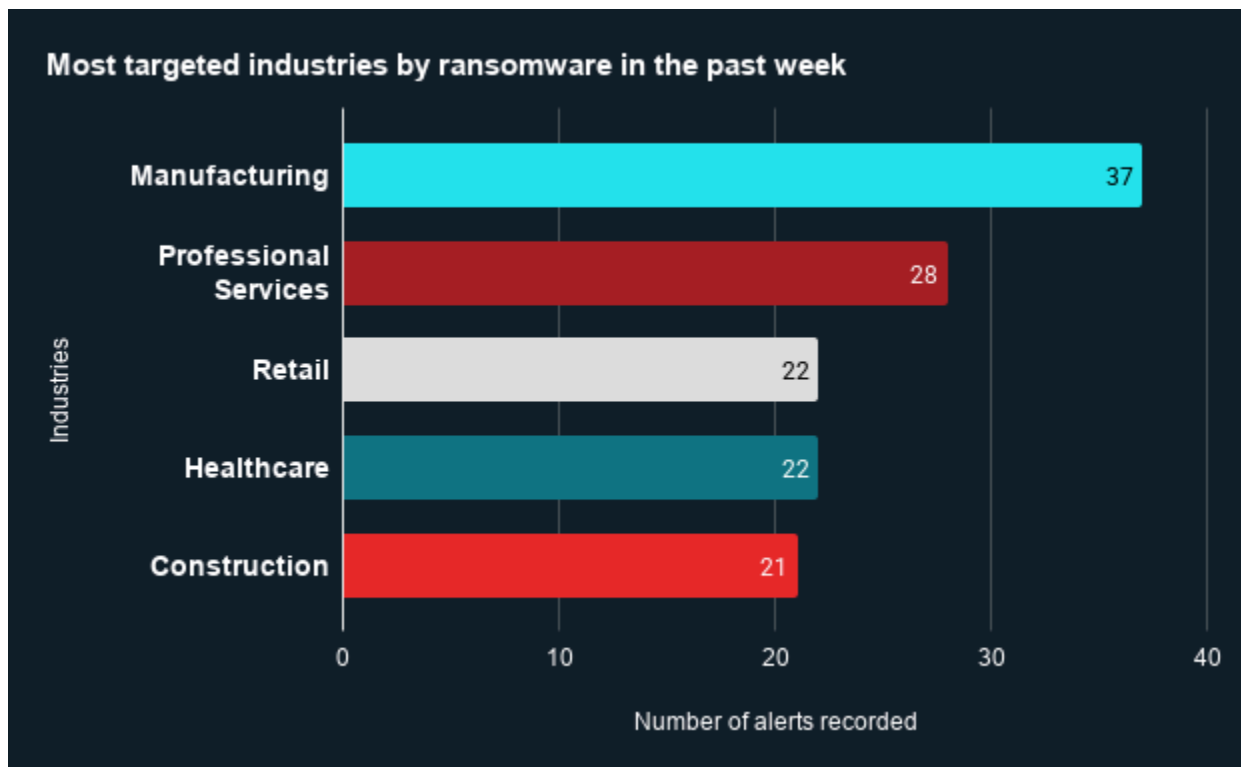
Ransomware Group, Industry, Regional Trends

Last week in ransomware: In the past week, NightSpire, n0n, Qilin, The Gentlemen, and Wallstreet were the most active ransomware groups. ZeroFox observed close to 226 ransomware victims disclosed, most of whom were located in North America. NightSpire accounted for the largest number of attacks, followed by n0n.



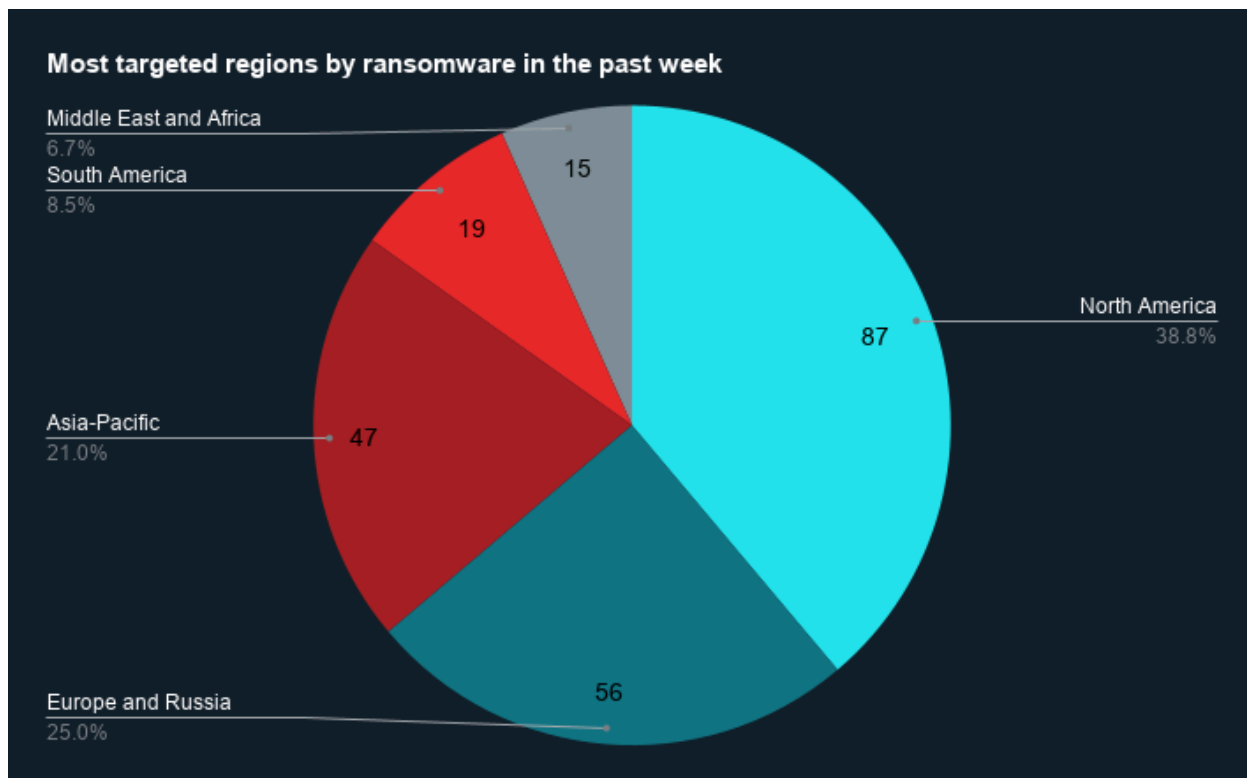
Source: ZeroFox Internal Collections

Industry ransomware trends: In the past week, ZeroFox observed that manufacturing was the industry most targeted by ransomware attacks, followed by professional services, retail, healthcare, and construction.



Source: ZeroFox Internal Collections

Regional ransomware trends: Over the past seven days, ZeroFox observed that North America was the region most targeted by ransomware attacks, followed by Europe and Russia and Asia-Pacific. There were at least 87 ransomware attacks observed in North America, while Europe and Russia accounted for 56, Asia-Pacific for 47, South America for 19, and Middle East and Africa for 15.



Source: ZeroFox Internal Collections



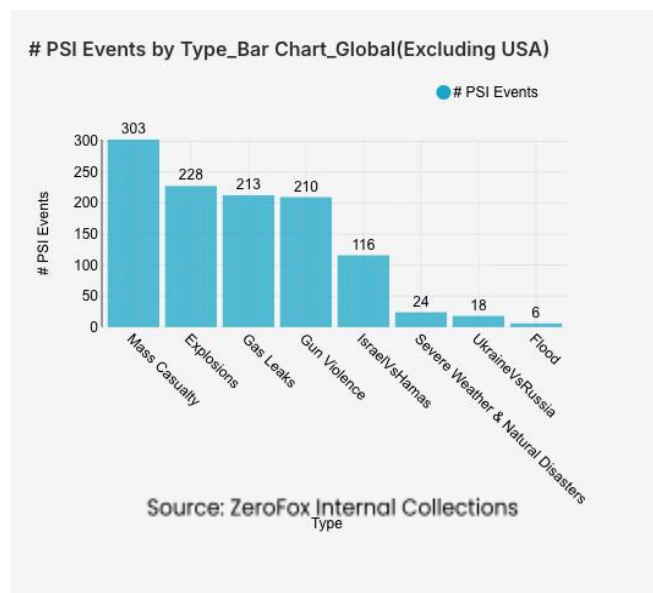
Notable Data Breaches this Week

Targeted Entity	<u>iRhythm Technologies</u>	<u>Ampath Laboratories</u>	<u>Ukrainian organizations and critical infrastructure</u>
Compromised Entities/Victims	At least 360,000 patients	80 million patient records	Ukrainian individuals, e-commerce platforms, and critical energy infrastructure
Compromised Data Fields	Names, addresses, email addresses, dates of birth, phone numbers, account numbers, device serial numbers, insurance numbers, and dates of service	Personally identifiable information of patients	628,000 personal records, e-commerce data, and operational network access data
Suspected Threat Actor	N/A	bytetobreach	CyberXero
Country/Region	United States	Southeast Asia	Ukraine / Eastern Europe
Industry	Healthcare	Healthcare	Critical Infrastructure / E-Commerce / Government
Possible Repercussions	Phishing, social engineering, and identity fraud using exposed personal, insurance, and account information	Phishing, identity fraud, or other social engineering activity, depending on the data compromised.	Resale of exfiltrated personal and payment records, identity theft, and state-backed exploitation of critical energy infrastructure networks.

Three major breaches observed in the past week

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings



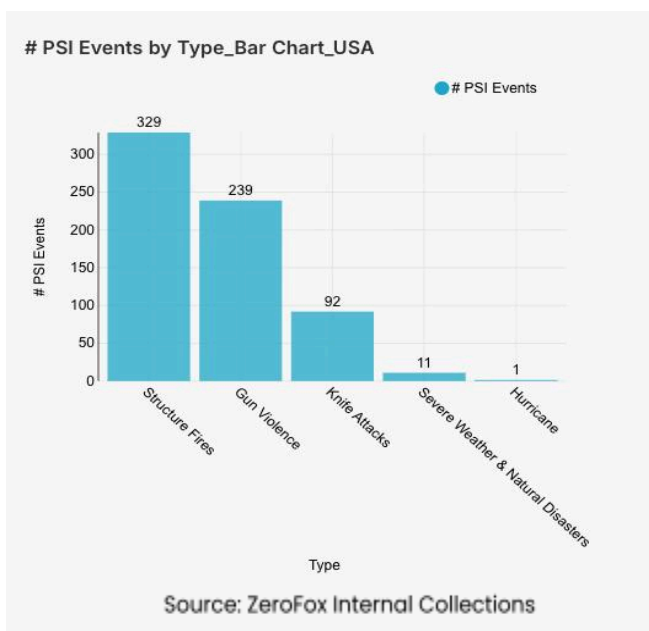
Physical Security Intelligence: Global

What happened: Excluding the United States, there was an 8 percent decrease in mass casualty events this week from the previous week, with the top contributing countries or territories being the Palestinian territories, Yemen, and India, in that order. Approximately 75 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 30 percent of all mass casualty alerts. General alerts related to the

Israel-Hamas conflict increased by 30 percent from the previous week, and alerts related to Russia's war with Ukraine increased by 6 percent. The top three most-alerted subtypes were structure fires, which saw a 5 percent increase from the previous week; explosions, which decreased by 4 percent; and gas leaks, which increased by 33 percent. Notably, alerts labeled "Severe Weather and Natural Disasters" increased by 41 percent.

- What this means:** Global physical security this week was shaped by continued conflict violence and a sharp rise in weather-related hazards. On October 14, [Israeli strikes](#) killed four people in Gaza, days after the first anniversary of the U.S.-mediated ceasefire. A [Russian missile and drone barrage](#) on October 12–13 killed two people in Kyiv and four in Kharkiv. In Yemen, Houthi-affiliated health officials reported three deaths from [shelling and an unexploded ordnance blast](#). In India, a [polyfoam warehouse fire](#) in Sonipat killed two workers on October 15, in line with structure fires and gas leaks topping the alert subtypes. On October 11, a [flash flood in Gorkha, Nepal](#), swept away multiple homes and left five people missing weeks after the August floods, reflecting the sharp rise in severe weather and natural disaster alerts. In Mexico, [Hurricane Simon and the remnants of Tropical Storm Rache](#) have killed at least eight people and left two missing. Overall, global physical security remained volatile, with persistent conflict-driven violence compounded by a surge in weather and disaster threats.

Physical Security Intelligence: United States



What happened: In the past week, the top three most-alerted incident subtypes were structure fires, gun violence, and knife attacks. Gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim, knife attacks include confirmed stabbings or slashings, and structure fires are fires that affect man-made buildings. The top two states with the most gun violence alerts were Illinois and California, which together made up 26 percent of this week's nationwide total. Gun violence across the United States overall increased by 1 percent from the week prior. Knife attack alerts did not increase or

decrease from the previous week, and the top contributing states were Illinois and California. Structure fires increased by 15 percent, and the top two states for this subtype were California and New York. Notably, alerts labeled "Severe Weather and Natural Disasters" increased by 22 percent.

- **What this means:** Domestic physical security this week was driven by steady violent crime and a sharp rise in weather-driven disruption. [Hurricane Isaias](#), the first hurricane of the Atlantic season, made landfall near Destin, Florida, as a Category 2 storm on October 9 and killed at least six people in Florida, with outages peaking above one million customers across the Southeast. On October 10–11, [the remnants of Tropical Storm Rachel](#) caused severe flooding in Las Vegas, Nevada, after forcing coastal evacuations in Long Beach, California. Meanwhile, in line with the increase in gun violence alerts, Chicago, Illinois, recorded at least four killed and 11 wounded in [weekend shootings](#); in Pico-Union, Los Angeles, California, a father allegedly [shot and killed two children before shooting himself](#) on October 11. Structure fires also rose; a [vacant historic church in Los Angeles](#), California, burned for the third time on October 12 and required about 180 firefighters. Overall, domestic physical security remained elevated this week, with persistent firearm and knife violence in major states combined with rising structure fire activity and a sharp surge in storm-driven disruption across the Southeast and Southwest.

| Appendix A: Traffic Light Protocol for Information Dissemination

WHEN SHOULD IT BE USED?

Red

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.

Amber

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

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.

Clear

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%