ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

April 18, 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 April 16, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Weekly Intelligence Brief

© 2026 ZeroFox, Inc. All rights reserved.

This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Flash Report - SITREP #34 - SoH Blockade - April 14, 2026

A U.S. naval blockade of the Strait of Hormuz (SoH) began on April 13, following the collapse of talks between U.S. and Iranian negotiators in Pakistan. The talks ended without a deal, almost certainly due to differences over reopening of the SoH and curbs on Iran's nuclear program. The United States has moved additional military assets into the region, increasing the likelihood of renewed hostilities. Despite the blockade, the 14-day ceasefire between the United States and Iran is holding—notably without Iran retaliating to the blockade. Further talks are therefore likely. However, the conflict remains fragile elsewhere, with Israel targeting Hezbollah. Israel's Lebanon campaign risks prolonging the conflict with Iran, which has signaled its readiness to reopen the SoH only if attacks on Hezbollah cease. Ships are unlikely to transit the SoH, as doing so will either be in defiance of the United States, making them subject to confiscation, or Iran, making them military targets. However, as it has become clear that Iran is unlikely to retaliate to the blockade, leading economic indicators have thus far remained positive To know more about how the conflict has progressed, read previous SITREPs.

© 2026 ZeroFox, Inc. All rights reserved.

ZEROFOX
Weekly Intelligence Brief

Cyber and Dark Web Intelligence

© 2026 ZeroFox, Inc. All rights reserved.

Cyber and Dark Web Intelligence Key Findings

Fake Ledger App Stole over USD 9 Million from 50 Victims

What we know:

- A malicious fake Ledger Live app on Apple's App Store targeted macOS users, draining nearly USD 9.5 million in cryptocurrencies from 50 victims across Bitcoin, Ethereum, Tron, Solana, and Ripple wallets.
- Users were tricked into exposing their seed phrases, enabling threat actors to gain full wallet control and make immediate unauthorized transfers to attacker-controlled addresses.

Background:

- The fake app was reportedly listed on the Apple App Store under "Leva Heal Limited" (now taken down); it is not affiliated with Ledger, which only offers its macOS app via its official website and not the App Store.
- Meanwhile, another major cryptocurrency company, Kraken, has reported that it is being extorted after insider-driven unauthorized access exposed limited client support data, though no funds were confirmed to be at risk.

Analyst note:

- Although the campaign was short-lived, the attackers siphoned a sizable amount of funds from a relatively small pool of victims (50 wallet owners), likely suggesting they targeted and exploited seed phrases belonging to high-value users before the fake app was discovered.

Trojanized Hardware Monitoring Tools Spread via Compromised CPUID Infrastructure

What we know:

- Threat actors compromised a CPUID API and temporarily replaced official download links with trojanized versions of tools such as CPU-Z and HWMonitor.

© 2026 ZeroFox, Inc. All rights reserved.

- During the brief attack, malicious files such as HWiNFO_Monitor_Setup were distributed, using a Russian-language installer and Dynamic Link Library (DLL) sideloading via a rogue CRYPTBASE[.]dll.
- The issue has since been fixed.

Background:

- CPU-Z and HWMonitor are tools used to monitor a device's hardware health—including temperatures, voltages, and performance—and have had millions of downloads.
- For this attack, threat actors distributed trojanized versions of CPU-Z (2.19), HWMonitor Pro (1.57), HWMonitor (1.63), and PerfMonitor (2.04).
- Over 150 users, including in organizations across sectors in Brazil, Russia, and China, have reportedly downloaded the malicious software.

Analyst note:

- The threat actors likely targeted IT professionals, system admins, hardware owners, and developers to access user and corporate endpoint devices.
- Compromised systems and endpoint devices are likely to be repurposed into proxy nodes or relay infrastructure, enabling attackers to route malicious traffic through trusted networks.

W3LLSTORE PhaaS, Linked to Over USD 20 Million in Fraud, Dismantled

What we know:

- W3LLSTORE phishing market has been dismantled by the Federal Bureau of Investigation (FBI) and the Indonesian National Police.
- The global phishing-as-a-service (PhaaS) operation is linked to over USD 20 million in attempted fraud and was used in over 17,000 attacks worldwide between 2023 and 2024.

Background:

- Authorities seized criminal infrastructure and detained a suspect. The W3LL phishing kit enabled cybercriminals to create fake login pages for legitimate platforms and steal credentials.
- While the marketplace shut down in 2023, the phishing kit continued to be sold privately through encrypted messaging platforms.

Analyst note:

- The law enforcement action is likely to help authorities identify other collaborators who developed and operated the PhaaS, potentially leading to their detention.

© 2026 ZeroFox, Inc. All rights reserved.

- However, the W3LL phishing kit's code is likely to be leaked to the wider cybercrime world, enabling other cybercriminals to create different versions of the kit.

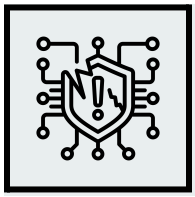
© 2026 ZeroFox, Inc. All rights reserved.

Exploit and Vulnerability Intelligence

© 2026 ZeroFox, Inc. All rights reserved.

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 nine new vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on April 13 and April 14, 2026. Microsoft has released patches for 167 vulnerabilities, including two zero-day bugs tracked as CVE-2026-32201 (SharePoint server spoofing vulnerability) and CVE-2026-33825 (Defender elevation of privilege vulnerability). A pre-authenticated remote code execution (RCE) vulnerability, tracked as CVE-2026-39987, impacts open-source Python notebook Marimo used for data science and analysis. The flaw is reportedly under active exploitation and a credential theft operation is also reportedly underway. SonicWall has patched four vulnerabilities in SMA1000 firewalls, including an SQL injection flaw (CVE-2026-4112) that could enable privilege escalation to admin access.

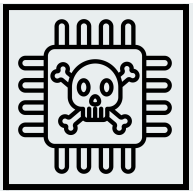


CRITICAL

CVE-2026-5194

What happened: This cryptographic validation flaw in the wolfSSL library weakens certificate validation by improperly checking hash algorithms and sizes in digital signatures. WolfSSL is a lightweight SSL/TLS library designed for embedded systems, Internet of Things (IoT) devices, and critical infrastructure environments.

- **What this means:** Threat actors are likely to carry out man-in-the-middle attacks, wherein they can forge certificates to intercept and manipulate encrypted communications.
  - **Affected products**: WolfSSL versions prior to 5.9.1



CRITICAL

CVE-2026-33032

What happened: This flaw in Nginx UI is being actively exploited, enabling unauthenticated attackers to gain full server control via an exposed MCP endpoint. The bug enables remote config manipulation and service takeover, with thousands of internet-exposed instances at risk despite patches being available.

© 2026 ZeroFox, Inc. All rights reserved.

- **What this means:** Further widespread opportunistic exploitation is likely, with attackers targeting exposed instances for web server hijacking, persistence, and initial access into broader networks.
    - **Affected products:** Nginx versions prior to and including 2.3.5

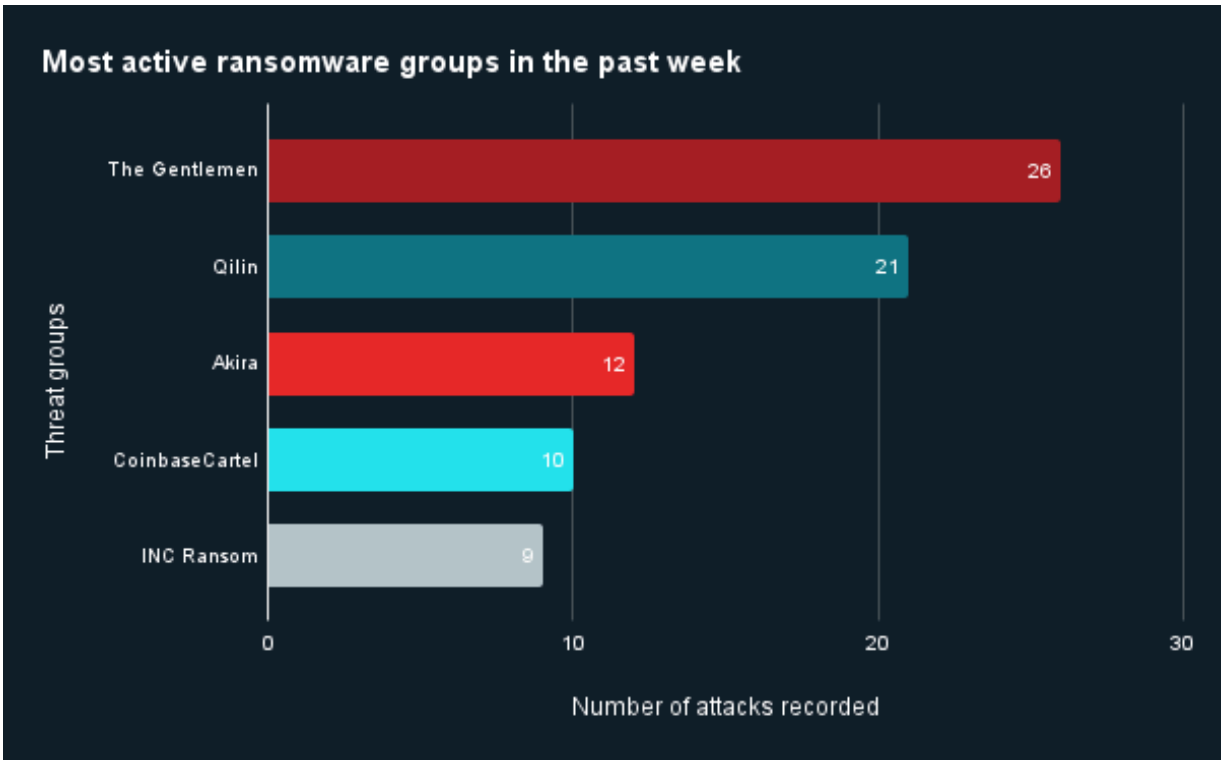
© 2026 ZeroFox, Inc. All rights reserved.

Ransomware and Breach Intelligence

© 2026 ZeroFox, Inc. All rights reserved.

Ransomware and Breach Intelligence Key Findings

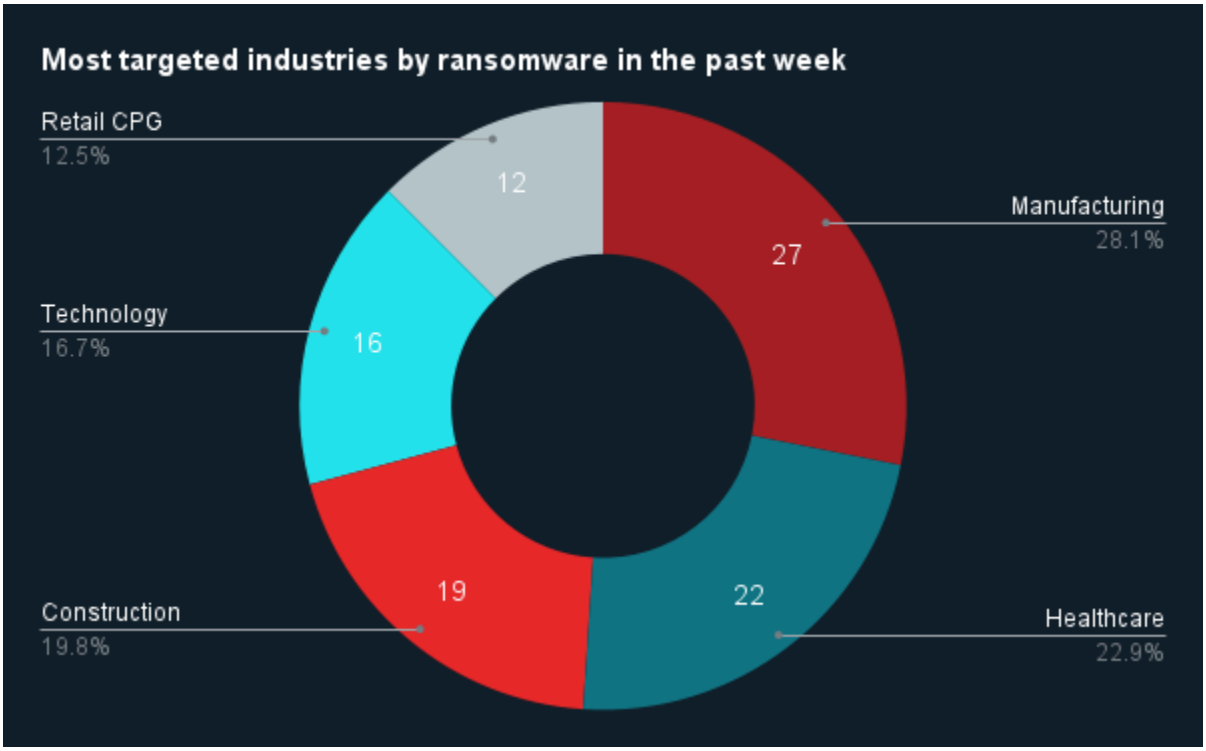
Ransomware Group, Industry, and Region Trends



Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, The Gentlemen, Qilin, Akira, CoinbaseCartel, and INC Ransom were the most active ransomware groups. ZeroFox observed close to 144 ransomware victims disclosed, most of whom were located in North America. The Gentlemen ransomware group accounted for the largest number of attacks, followed by Qilin.

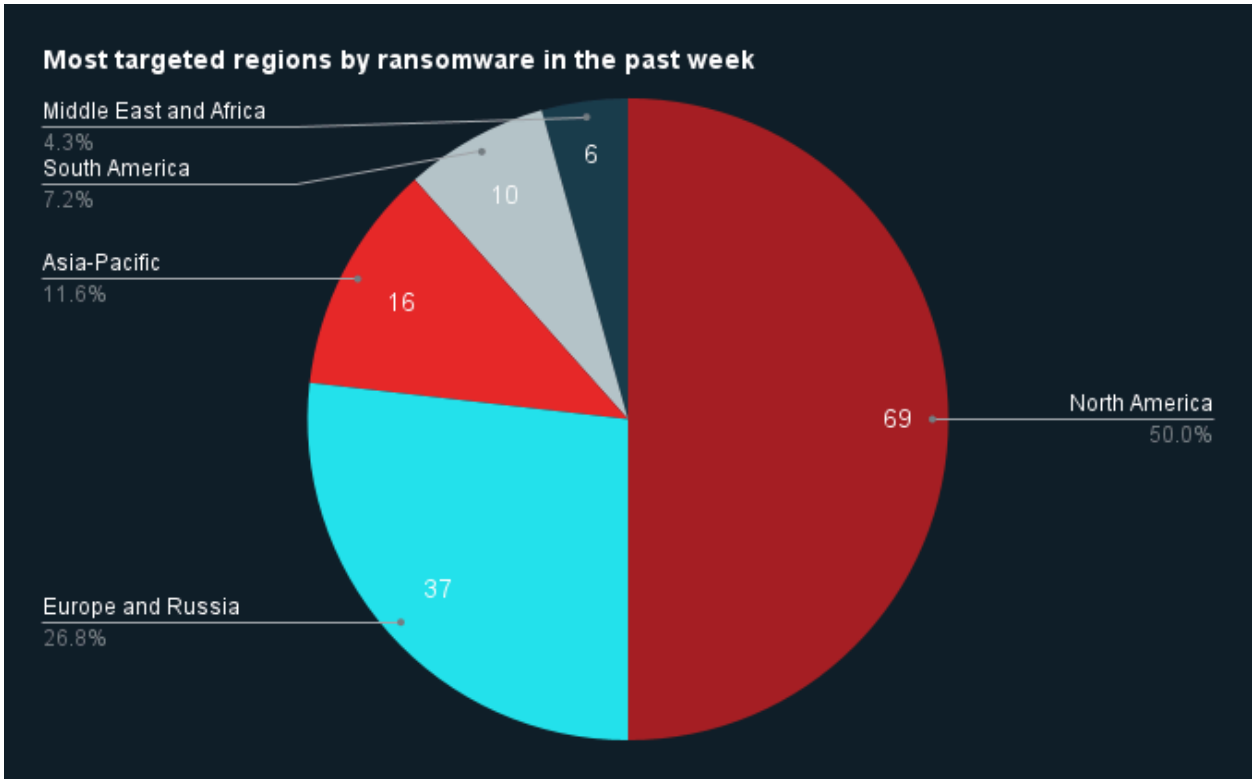
© 2026 ZeroFox, Inc. All rights reserved.



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 healthcare.

© 2026 ZeroFox, Inc. All rights reserved.



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. There were at least 69 ransomware attacks observed in North America, while Europe and Russia accounted for 37, Asia-Pacific (APAC) for 16, South America for 10, and Middle East and Africa for six.

© 2026 ZeroFox, Inc. All rights reserved.

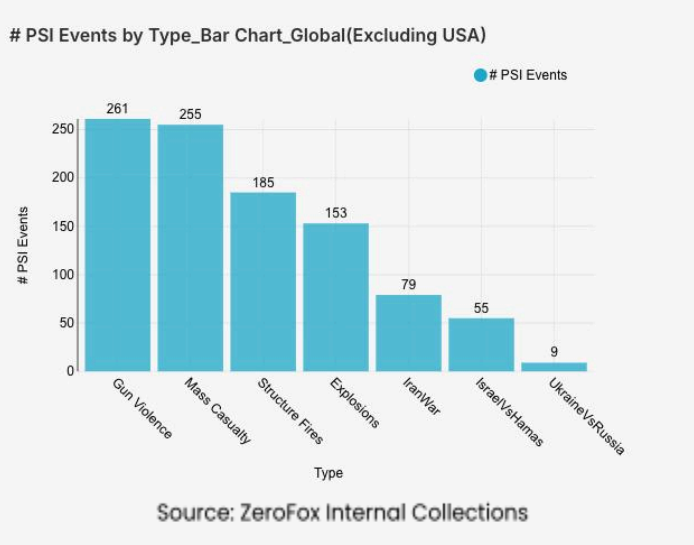
Data Breach Across Major Industries

Targeted Entity	Rockstar Games	Mihnati	Ukrainian Prosecutors
Compromised Entities/Victims	78.6 million records of users	Mihnati platform visitors	170 email accounts of Ukrainian prosecutors and investigators
Compromised Data Fields	Purchase metrics, player behavior tracking, and game economy data for Grand Theft Auto	Unspecified 627,000 records containing personally identifiable information on the job and recruitment platform	Investigative and intelligence services-related information
Suspected Threat Actor	ShinyHunters	M********	Fancy Bear
Country/Region	United States	Middle East	Europe
Industry	Media/entertainment	Professional services	Government
Possible Repercussions	High-value spenders are likely to be targeted	Targeted phishing campaigns and fraudulent job offers	Social engineering attacks, such as business email compromise and phishing campaigns

Three major breaches observed in the past week

© 2026 ZeroFox, Inc. All rights reserved.

Physical and Geopolitical Intelligence Key Findings



Source: ZeroFox Internal Collections

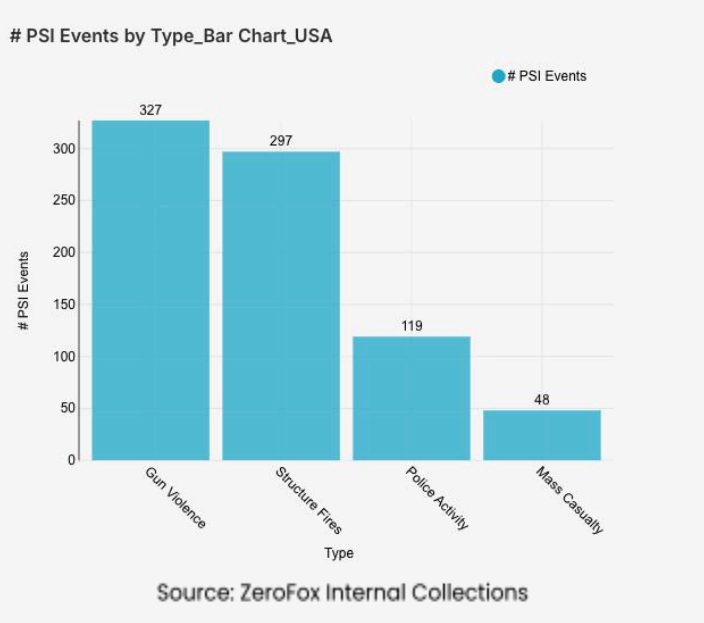
Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 34 percent decrease in mass casualty events this week from the previous week, with the top contributing countries or territories being Mexico, India, and Lebanon, in that order. Approximately 60 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 33 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict increased by 20 percent from the previous week, while alerts related to the war in Iran decreased by 47 percent. Events related to Russia's war in Ukraine increased by 29 percent. The top three most-alerted subtypes were gun violence, which saw a 32 percent increase from the previous week; structure fires, which increased by 71 percent; and explosions, which decreased by 47 percent.

- **What this means:** This week marked a pivotal shift in global security as the implementation of a two-week U.S.-Iran ceasefire, signed on April 8, led to a significant decrease in alerts related to the war in Iran, as well as an overall decrease in the explosions subtype. However, this diplomatic pause inadvertently fueled volatility elsewhere; while mass casualty events outside the United States dropped overall, Lebanon saw a spike in casualties, as Israel maintained the ceasefire did not apply to Hezbollah. The deadliest day occurred on April 8, when Israeli airstrikes killed over 300 people in a single day, now dubbed "Black Wednesday." Additionally, despite the Israel-Hamas ceasefire being in place since October 2025, routine violations—such as the April 9 shooting of a schoolgirl during a raid by Israeli forces—continue to persist, contributing to the increase in alerts this week. Meanwhile, the conflict in Ukraine also saw an increase in alerts as Ukrainian Unmanned Systems Forces ramped up to over 11,000 drone missions per day, as of April 9. In summary, while formal ceasefires are successfully reducing large-scale explosions in some areas, they often redistribute violence into other regions.

© 2026 ZeroFox, Inc. All rights reserved.

Physical Security Intelligence: United States



What happened: In the past week, the top three most-alerted incident subtypes were gun violence, structure fires, and police activity. Gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim, police activity involves law enforcement presence for generalized threats or for unknown reasons, and structure fires are fires that affect man-made buildings. The top two states with the most gun violence alerts were Illinois and Ohio, which together made up 18 percent of this week's nationwide total. Gun violence across the United States overall increased by 30 percent from the week prior. Police activity alerts increased by 40 percent, and the top contributing states were California and Florida. Structure fires increased by 7 percent, and the top two states for this subtype were New York and California.

- **What this means:** The data indicates a significant shift in safety trends across the United States over the past week, marked by a rise in gun violence and intensified law enforcement engagement. This trend is underscored by high-profile incidents, such as a mass casualty shooting in Virginia Beach, Virginia, on April 11, where eight people were injured during an altercation. On the same day, another mass shooting at a restaurant in Union Township, New Jersey, resulted in seven victims. The increase in police activity was most prevalent in California and Florida, often driven by law enforcement responses to large-scale civic disturbances and "street takeovers" that devolved into violence. Furthermore, structure fires increased this week, with a series of incidents occurring in Ontario, California. Just three days after a warehouse fire caused over USD 650 million in damages, Ontario Mills mall was intentionally torched, adding to the state's high volume of fire alerts. The suspect of the first fire reportedly cited anti-capitalist and anti-corporate sentiments, and the second suspect is believed to have been inspired by similar motives. These deliberate acts of arson, combined with a surge in generalized police activity, underscore a period where ideological friction is increasingly manifesting as physical destruction of property and infrastructure.

© 2026 ZeroFox, Inc. All rights reserved.

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.

© 2026 ZeroFox, Inc. All rights reserved.

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%

© 2026 ZeroFox, Inc. All rights reserved.