



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

October 28, 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 9:00 AM (EDT) on October 25, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Weekly Intelligence Brief |

 Cyber and Dark Web Intelligence Key Findings	3
Disinformation and Cyber Threats Ahead of the 2024 Elections	3
Exposed United Nations Database Left Sensitive Information Accessible Online	4
Pro-India Hacktivists Plan to Target Canada amid Escalating Diplomatic Tensions	4
 Exploit and Vulnerability Intelligence Key Findings	7
CVE-2024-47575	7
CVE-2024-38812	8
 Ransomware and Breach Intelligence Key Findings	10
Ransomware Attacks and New Strains Targeting Multiple Sectors	10
Breaches Impact Entities Around the World	11
 Physical and Geopolitical Intelligence Key Findings	14
Physical Security Intelligence: Global	14
Physical Security Intelligence: United States	15
 Appendix A: Traffic Light Protocol for Information Dissemination	16
 Appendix B: ZeroFox Intelligence Probability Scale	16

| Cyber and Dark Web Intelligence |

| Cyber and Dark Web Intelligence Key Findings



Disinformation and Cyber Threats Ahead of the 2024 Elections

What happened: In the wake of escalating disinformation efforts ahead of the elections, the Department of Justice (DOJ) has taken proactive [measures](#) by issuing a Notice of Proposed Rulemaking (NPRM) to implement President Biden's Executive Order 14117, which is aimed at safeguarding Americans' sensitive personal data from foreign adversaries. This initiative comes in response to the growing threat posed by state-sponsored disinformation campaigns. Among these threats, China's Spamouflage disinformation crew (also known as Dragonbridge) has specifically [targeted](#) a prominent U.S. lawmaker. Utilizing fake news campaigns, Spamouflage has trolled his official X account and spread negative narratives on platforms like Reddit and Medium. In a concerning escalation, the group has begun using deepfake technology to craft misleading videos designed to influence the upcoming presidential election. Meanwhile, Russian state-backed actors have [launched](#) a sweeping disinformation campaign that is inundating the American news landscape with fake news masquerading as credible reporting. This strategy aims to overwhelm journalists, diverting their attention from legitimate investigations and making it more challenging to debunk false claims. Amid this chaotic backdrop, Iran's Cotton Sandstorm—a hacking group linked to the Islamic Revolutionary Guard Corps (IRGC)—is [reportedly](#) conducting its own influence operations as the elections draw near. Another Iranian group, Storm-2035, is actively spreading divisive and conspiratorial articles by impersonating various local U.S. news outlets, posting around eight articles weekly and targeting both Democrats and Republicans. Reports suggest that Iran's election activities seem to favor the Harris campaign, while Russia has intensified its attacks against the Harris-Walz campaign. Adding to the tumult, Russian-language accounts on X and Telegram have been observed circulating an artificial intelligence (AI)-enhanced deepfake video of Vice President Kamala Harris. The video depicts her making inappropriate jokes about assassination attempts against Trump and has already garnered tens of thousands of views.

- **What this means:** With the elections less than two weeks ahead, foreign threat actors are likely to intensify their cyberattacks. The DOJ is responding by implementing measures to protect sensitive U.S. data from foreign adversaries. Various state-sponsored groups, including China's Dragonbridge and Iran's Cotton Sandstorm, are employing tactics such as fake news, deepfakes, and impersonation of local news outlets to manipulate public perception and influence political outcomes. This misleading content is often disguised with branding that resembles trusted U.S. news organizations, making it challenging for

citizens to discern credible information from disinformation. The saturation of the information landscape with such content can potentially influence election outcomes. Meanwhile, successful defenses against cyberattacks—such as those by the Georgia Secretary of State’s office, which [defended](#) against a cyberattack targeting the website where voters request absentee ballots—demonstrate ongoing efforts to protect the electoral process in this fraught environment.



Exposed United Nations Database Left Sensitive Information Accessible Online

What happened: A database belonging to the United Nations (UN) Trust Fund to End Violence Against Women was found exposed online, revealing over 115,000 sensitive files related to organizations working with vulnerable communities globally—including under oppressive regimes. The data included staffing information, contracts, and detailed financial audits. A researcher discovered the misconfigured database and notified the UN, which promptly secured it.

- **What this means:** The exposed data poses a significant risk to both organizations and individuals, particularly in vulnerable communities. At an organizational level, the leak provides detailed financial audits, staffing information, and operational breakdowns, which could be misused in scams or to undermine these entities’ operations. The exposure of personal information linked to sensitive projects could endanger the safety of people receiving assistance, especially those living under oppressive regimes or in dangerous conditions. Individuals facing persecution, LGBTQ+ people, and victims of violence or abuse could be specifically targeted for extortion, retaliation, or law enforcement action based on the leaked information. Financial audits, including bank account details, could be misused in scams—especially since the UN is a highly trusted organization. The data reportedly includes detailed insights into the funding, operations, and staff of civil society organizations, which could be leveraged by malicious actors or authoritarian governments to target these groups and the vulnerable people they serve. Such information could potentially jeopardize the safety and activities of organizations working in hostile regions.



Pro-India Hacktivists Plan to Target Canada amid Escalating Diplomatic Tensions

What happened: On October 22, 2024, pro-India hacktivist groups Indian Cyber Force and Indian Cyber Army announced preparations for a cyberattack on Canada, intending to disrupt its cyber infrastructure. This escalation occurs amid heightened geopolitical tensions between India and Canada. The hacktivists framed their planned actions as retaliation against Canadian Prime Minister Justin Trudeau, accusing him of aligning with Khalistani extremists and having an anti-India stance. This is not the first time Indian hacktivists have targeted Canadian cyber assets. In September 2023, Indian Cyber Force launched cyberattacks on websites connected to the Canadian military following the controversial killing of Canadian Sikh leader Hardeep Singh Nijjar, which strained relations between the two nations.

- **What this means:** The current cyber landscape is dotted with politically aligned threat actors, especially hacktivists, and cyberwarfare often reflects the ongoing political and diplomatic conflicts around the world. Indian Cyber Force and Indian Cyber Army view Trudeau's alleged stance on Khalistan as not just a political disagreement but a destabilizing threat to India's national security. Canada's cyber infrastructure—possibly including public services, government websites, and critical sectors—is likely to face a medium threat from potential distributed denial-of-service attacks orchestrated by the Indian hacktivist groups. Should such attacks occur, they are likely to deepen diplomatic rifts, prompt retaliatory actions (very likely from Canada-allied or even West-allied hackers), and further destabilize bilateral relationships. Canada's response to these imminent attacks, whether by cyber countermeasures or diplomatic pressure, will further impact the stability of this tense relationship.

| **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, within the Known Exploited Vulnerabilities (KEV) catalog, and by software development services. VMware has released new patches for [CVE-2024-38812](#), a critical vCenter Server remote code execution (RCE) vulnerability initially mis-patched in September 2024. [CVE-2024-44068](#) is a use-after-free, high-severity, zero-day bug in the mobile processor of affected Samsung mobiles that leads to privilege escalation. [Two](#) critical vulnerabilities—identified as CVE-2024-45274 and CVE-2024-45275—can be exploited by unauthenticated, remote attackers to execute arbitrary operating system commands (due to insufficient authentication) and take complete control of an affected device (through hardcoded credentials). The Cybersecurity and Infrastructure Security Agency (CISA) has added [three](#) vulnerabilities to its KEV catalog. The vulnerability [CVE-2024-8260](#) arises from inadequate input validation, enabling attackers to deceive an Open Policy Agent (OPA) into accessing a malicious Server Message Block (SMB) share. [CVE-2024-37383](#) is a vulnerability in the Roundcube Webmail email client and is a stored cross-site scripting (XSS) vulnerability that can allow attackers to execute JavaScript code on the user's page. [CVE-2024-47575](#) is a flaw in the FortiManager fgfmnd daemon, which has been identified as missing authentication for critical functions [CWE-306], that allows a remote unauthenticated attacker to execute arbitrary code or commands through specially crafted requests. A security vulnerability, [CVE-2024-9050](#), has been found in Red Hat's NetworkManager-libreswan plugin, which could enable local attackers to escalate their privileges and obtain root access on Linux systems. [CVE-2024-45309](#) is a critical vulnerability identified in the OneDev DevOps platform, impacting versions prior to 11.0.9.



CRITICAL

CVE-2024-47575

What happened: Fortinet has disclosed a critical zero-day vulnerability (CVE-2024-47575) affecting FortiManager API that is used to steal sensitive data like device configurations and credentials. Fortinet initially warned customers privately on October 13 about the issue. A valid certificate from Fortinet devices is needed to exploit the bug, which enables unauthorized access to networks. Some customers reported being attacked weeks before the advisory.

- **What this means:** Exploiting this vulnerability can allow attackers to hijack FortiManager systems, gaining control over firewalls and potentially spreading across corporate networks, as well as those overseen by managed service providers (MSPs). Attackers could

disable security controls, steal sensitive information, or disrupt operations by altering configurations. Moreover, unauthorized access to one firewall could expose multiple networks. With over 59,000 FortiManager servers accessible online, organizations face heightened risks if mitigations or patches are delayed.

➤ **Affected products:**

- FortiManager 7.6 version 7.6.0
- FortiManager 7.4 versions 7.4.0 through 7.4.4
- FortiManager 7.2 versions 7.2.0 through 7.2.7
- FortiManager 7.0 versions 7.0.0 through 7.0.12
- FortiManager 6.4 versions 6.4.0 through 6.4.14
- FortiManager 6.2 versions 6.2.0 through 6.2.12
- FortiManager Cloud 7.4 versions 7.4.1 through 7.4.4
- FortiManager Cloud 7.2 versions 7.2.1 through 7.2.7
- FortiManager Cloud 7.0 versions 7.0.1 through 7.0.12
- FortiManager Cloud 6.4 versions 6.4 all versions



CRITICAL
CVE-2024-38812

What happened: VMware has released new patches for CVE-2024-38812, a critical vCenter Server RCE vulnerability initially mis-patched in September 2024. The flaw, exploited during China's Matrix Cup, affects multiple vCenter versions and has no workaround.

- **What this means:** The vCenter Server [contains](#) a heap-overflow vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger this vulnerability by sending a specially crafted network packet potentially leading to RCE.
- **Affected products:**
- vCenter version 7.0.3
 - vCenter version 8.0.2
 - vCenter version 8.0.3

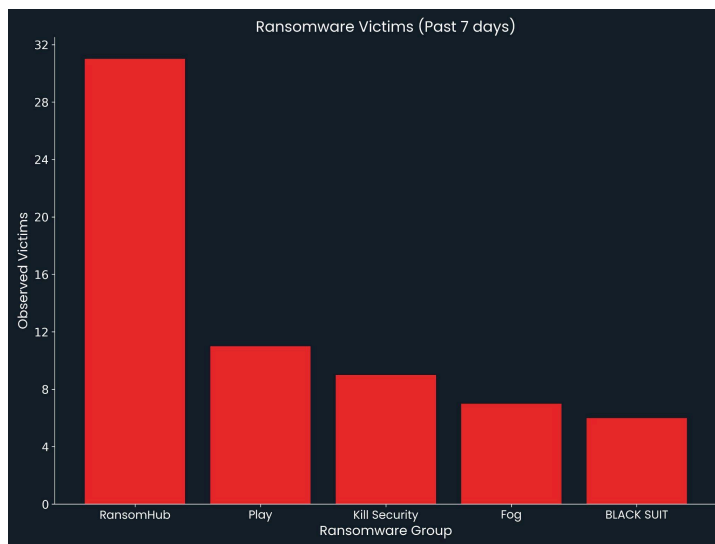
| Ransomware and Breach Intelligence |

Ransomware and Breach Intelligence Key Findings



Ransomware Attacks and New Strains Targeting Multiple Sectors

What happened: NotLockBit, a new macOS malware family written in Go has been [observed](#) mimicking LockBit ransomware. The malware targets both Windows and macOS systems, encrypting files, stealing data for double extortion, and deleting shadow copies to prevent recovery. It also collects system information and uses a public key to secure its encryption process. Threat actors have been [exploiting](#) Amazon S3's Transfer Acceleration feature in ransomware attacks to exfiltrate victim data and upload it to S3 buckets they control. These attackers are leveraging LockBit's reputation to increase pressure on victims, using the service's speed to streamline data theft during the ransomware operation. [Nidec](#) Corporation confirmed that hackers behind a ransomware attack earlier this year stole and leaked confidential data on the dark web after the company reportedly did not meet their demands. The attackers gained access by using valid VPN credentials from a Nidec employee. Although Nidec has not named the perpetrators responsible for this attack, ZeroFox observed threat actors [8Base](#) and [Everest](#) claiming to leak the company's data on their leak sites. Researchers have [identified](#) an advanced version of Qilin ransomware with enhanced evasion tactics, including a custom infostealer targeting Google Chrome credentials. This allows Qilin to infiltrate entire networks and reestablish itself on systems even after attempted cleanups, posing a significant risk to infected environments.



Source: ZeroFox Internal Collections

- **What this means:** NotLockBit is the first functional ransomware observed targeting macOS, posing a new threat to macOS users. With capabilities like double extortion, data encryption, and shadow copy deletion, it introduces risks previously limited to Windows environments, potentially leading to significant data loss and disruption for both individual users and businesses relying on macOS systems. By using a legitimate cloud service feature, threat actors can evade traditional detection mechanisms in the Amazon S3

attack, making it harder for organizations to detect and stop the data theft. Additionally, leveraging the notorious LockBit name adds psychological pressure on victims, increasing the likelihood of ransom payments. This tactic also demonstrates how attackers are evolving by exploiting trusted cloud platforms for malicious purposes, which presents new challenges for cybersecurity defenses. The threat actors reportedly leaked over 50,000 files from Nidec, including business contracts, procurement policies, and internal documents. While the attack did not encrypt files, the stolen data could be exploited in targeted phishing campaigns or other malicious activities. Employees, contractors, and business partners are likely to face targeted phishing attacks, financial fraud, or reputational damage due to the stolen information. The advanced Qilin ransomware is significant because it adds a highly sophisticated tool to the arsenal of notorious threat groups, enabling them to carry out more effective and persistent attacks. Its ability to steal credentials, evade detection, and reestablish itself after cleanups gives attackers a prolonged presence on devices, allowing them to carry out extended data theft, extortion, or further lateral movement within networks.



Breaches Impact Entities Around the World

What happened: A threat actor [claimed](#) to leak personal data allegedly tied to over 180,000 Esport North Africa (ESNA) users just a day before a tournament in Morocco. The 3 GB package posted on BreachForums contains usernames, email addresses, IP addresses, and session details, though no passwords or financial data were exposed. Meanwhile, a hacker known as Satanic [claims](#) to have stolen data on 350 million Hot Topic customers, including names, emails, addresses, and partial payment info. The breach reportedly happened due to a malware infection at a third-party vendor. The stolen data is priced at USD 20,000, with the hacker offering to take down the listing for USD 100,000. Landmark Admin, a third-party insurance administrator, [disclosed](#) a data breach impacting over 800,000 individuals due to a May 13 cyberattack. The attackers accessed sensitive personal information, including Social Security numbers, medical data, and financial account details. The U.S. Securities and Exchange Commission (SEC) has [charged](#) several U.S.-based companies with misleading disclosures about cybersecurity incidents. They have collectively agreed to pay over USD 7 million in fines without admitting wrongdoing. The Internet Archive [faced](#) a third cyberattack on October 20 due to unrotated Zendesk API tokens, exposing sensitive support data. This follows two earlier cyberattacks, compounding security failures.

- **What this means:** Recent cyberattacks, including a breach [targeting](#) a developer behind the Pokémon series and an attack on ESNA, likely indicate that gaming platforms are

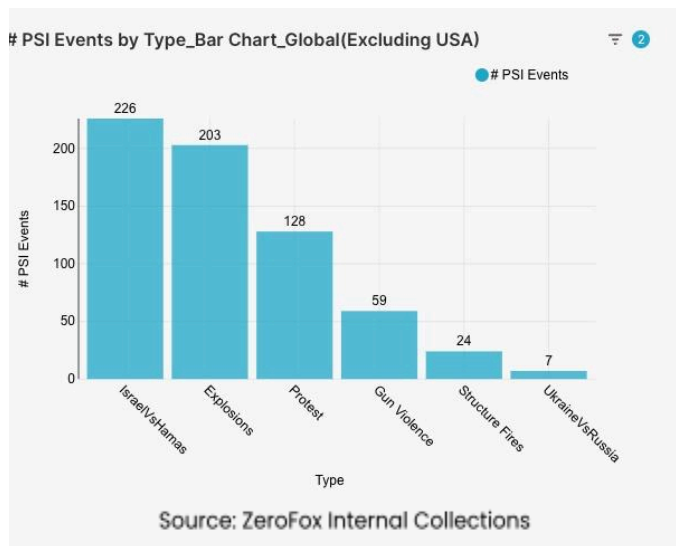
becoming popular targets for hackers. The alleged ESNA breach will likely disrupt upcoming tournaments and expose users to phishing attempts, with attackers potentially posing as ESNA staff to steal money or identities. In the Hot Topic breach, customers had personal data exposed, increasing the risk of phishing. Although the breach did not include full financial details, names, emails, and partial payment information is enough for scammers to launch convincing attacks. The incident highlights how security failures at third-party vendors can harm retailers like Hot Topic, potentially damaging their reputations. The charges the SEC filed against several companies for allegedly not following protocol in disclosing any cybersecurity incident come after the firms minimized or framed breaches in hypothetical or vague terms—despite knowing the attacks had already occurred. In some instances, companies ignored major breaches or underreported how much data was compromised. Misleading disclosures can disrupt response efforts as well as negatively impact customers and dependent businesses. The Landmark Admin breach forced the company to shut down IT systems and hire external cybersecurity experts to investigate. It poses significant risks for more than 800,000 victims, exposing them to risks of identity theft, financial fraud, and medical identity misuse. The involvement of high-profile insurance carriers compounds the damage, as the compromised data spans life insurance policies, health plans, and financial accounts.

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

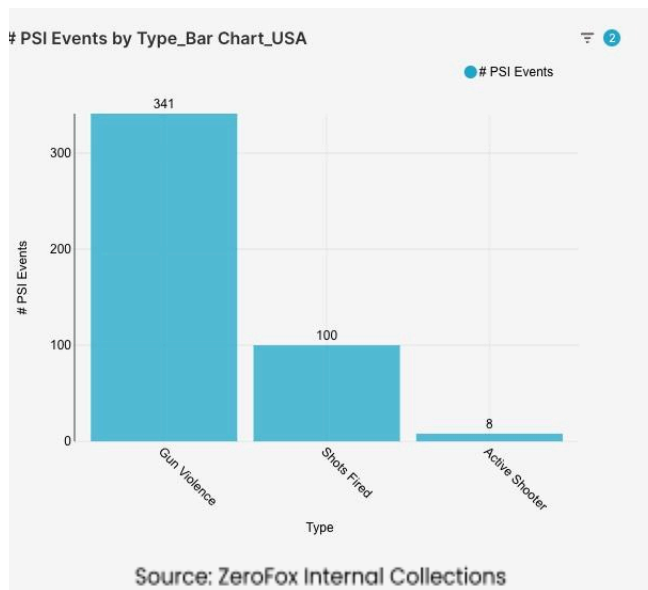
What happened: Excluding the United States, there was a 9 percent increase in the Mass Casualty incidents perpetrated by elements across the globe. The top three countries that contributed to the Mass Casualty incidents were Lebanon, Israel, and Palestine, and approximately 57 percent of the total were explosions. General alerts pertaining to the ongoing Israel-Hamas war (including Protests, Raid, and involvement in the neighboring countries) increased by 15 percent this week compared to last week. Palestine and Israel contributed to nearly 70 percent of all the International alerts. Additionally, the events related to the ongoing Russia and Ukraine war decreased by 30 percent. The top three most-alerted subtypes this week were Explosions, Gun Violence, and Structure Fire. Compared to the previous weeks, Explosions increased by 11 percent, while Gun Violence and Structure Fire both decreased by 1 percent and 14 percent, respectively. Global Protest activities increased by 30 percent this week.



- **What this means:** The ongoing conflict between Israel and Palestine continued, with [78 people](#) injured in an attack on Beit Lahiya and 33 people killed in an attack on Jabalia Refugee Camp. Attacks on Lebanon continued this week, with [40 people](#) injured in the incident as well. [Yahya Sinwar](#), the chairman of Hamas, was killed this week by the Israeli Defence Forces in a coordinated and targeted attack on Beirut. Additionally, the ongoing Russia-Ukraine war gained momentum, as multiple cross-border shellings were reported this week. Ukraine claimed through Telegram that it was successful in attacking a Russian military base in [Lipetsk](#) on Sunday. Ukraine later also claimed another successful attack on a major weapons factory in Nizhny Novgorod Region. A third explosion was reported this week from Russia's Tambov region, when a drone struck a bio-chem plant. With no peace treaty in sight, violence is going to continue in both of these conflicts for the foreseeable future. Despite a fall in the number of alerts compared to the previous week, the armed attack in Ankara stands out in this subtype this week. Armed assailants stormed the [Turkish Aerospace Industry \(TUSAS\)](#), killing five and injuring 22. While most of the news outlets attribute this attack to the Kurdistan Workers Party (PKK), the PKK has not yet claimed responsibility. This week saw multiple Natural Disasters, with Storms affecting the

Philippines and India. Tropical [Cyclone Trami](#) in the Philippines claimed 23 lives over the week in the Southeast region of Manila and has caused widespread landslides and flooding in the Northeastern part of the Philippines. In India, [Cyclone Dana](#) made landfall in the district of Odisha on Thursday evening/night. The cyclone is expected to move inland into the district, causing heavy rains and winds for the next 24 hours.

Physical Security Intelligence: United States



What happened: In the past week, the most alerted subtypes were Gun Violence, Structure Fire, and Shots Fired. Illinois and Ohio recorded the highest number of Gun Violence incidents, with 69 and 26 alerts, respectively, contributing to 29 percent of the total alerts. New York and California recorded the highest number of alerts pertaining to Structure Fire with both the cities contributing 28 percent to the total. Alerts relating to]Shots Fired increased by 17 percent this week compared to the previous one, while Active Shooter-related incidents showed a 700 percent rise in comparison to last week. School Threats this week showed a decrease

of 18 percent as the number of incidents alerted fell from 110 to 90.

- **What this means:** This week the United States saw a general fall in the number of alerts pertaining to most subtypes, with the exceptions of Gun Violence and Shots Fired. On Saturday, October 19, three people were killed and eight others were injured after a [man opened fire](#) on a school crowd celebrating a football game win on North Highway 17 near Lexington, Mississippi. This is the second incident proximal to a school reported within the span of one week; the first occurred near Tennessee State University in Nashville, claiming [one life and leaving nine others injured](#). Two of the eight incidents comprising the 700 percent increase in Active Shooter incidents over the week were reported near schools but fortunately none of the incidents resulted in Mass Casualty. New York and Pennsylvania contributed the highest number to the Shots Fired subtype. A positive trend this week has been the decrease in incidents tagged SchoolThreats and Wildfires.

| 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%