



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

November 18, 2024

Scope Note

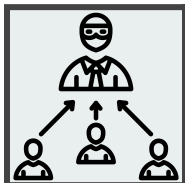
ZeroFox's Weekly Intelligence Briefing highlights the major developments and trends across the threat landscape, including digital, cyber, and physical threats. ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary 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 (EST) on November 15, 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
Encrypted Networks Lure Minors into Organized Crime, Europol Warns	3
German Interior Minister Warns of Cyber Threat Ahead of Election	3
Telegram's Recent Policy Shift Leads Threat Actors to Platform Exodus and Backup Channels	4
 Exploit and Vulnerability Intelligence Key Findings	7
CVE-2023-4699	7
CVE-2024-9463	8
 Ransomware and Breach Intelligence Key Findings	10
Ransomware Attacks on Critical Infrastructure Industries	10
Data Breaches Hit Retail, Gaming, and More in the Past Week	11
 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	17
 Appendix B: ZeroFox Intelligence Probability Scale	18

| **Cyber and Dark Web Intelligence** |

| Cyber and Dark Web Intelligence Key Findings



Encrypted Networks Lure Minors into Organized Crime, Europol Warns

What happened: Europol has issued a report revealing that criminal networks across Europe are intensifying the recruitment of minors for serious organized crime. Recruitment tactics include targeting young individuals on social media platforms and encrypted messaging apps. Disguising criminal activities as “challenges” or games, these networks lure minors and engage in encrypted messaging and further gamified tasks. The assignments range from extortion to violent crimes. This method also shields interactions, leaving almost no traceable digital evidence for the authorities to track.

- **What this means:** Several ongoing geopolitical conflicts, polarizing views, economic inflation, pandemic risks, and accelerated climate change have made minors more susceptible to new threats. Involving minors in their operation is not a new phenomenon for organized crime networks. As noted in a UNICEF [report](#), “a diversified group of armed actions, including non-state armed groups, organized criminal groups and violent networks,” are adapting tactics, often recruiting, coercing or inciting children to engage in violent acts. The cyber-themed recruitment drive is yet another example of this evolving threat. It creates a potent challenge for law enforcement, as criminals leverage encrypted channels and social media to mask their activities and evade surveillance. Encryption and coded language minimize digital traces, disrupting efforts to monitor or intercept recruitment campaigns. By focusing on encrypted channels, social media platforms, and “gamifying” tasks, these criminal networks lower the barrier to entry for minors and target them where they are most active, making criminal activity seem accessible and even appealing. This particular evolution in the criminal recruitment strategy is likely to accelerate the entry of minors into violent crime and complicate digital evidence-gathering.

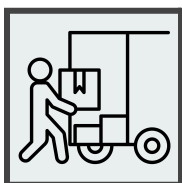


German Interior Minister Warns of Cyber Threat Ahead of Election

What happened: Germany’s interior minister, Nancy Faeser, warned that the country must enhance its cyber defenses against disinformation and [cyberattacks](#), reportedly from Russia, as it

prepares for early elections set to take place in February 2025. The Federal Office for Information Security's report stated no major incidents occurred during the recent European Union (EU) and state elections, but monitoring will intensify for national elections. Russian disinformation campaigns highly likely aim to destabilize and manipulate citizens. Germany is especially likely to be vulnerable to such falsified and heightened claims since Social Democrat Olaf Scholz's three-way coalition's recent [collapse](#).

- **What this means:** In Germany, officials have [uncovered](#) a massive disinformation campaign involving reportedly 50,000 fake user accounts and up to 200,000 automated X posts, which are then "amplified" by tens of thousands of other accounts attempting to influence real users and their feeds. Between August and March 2024, a large-scale, pro-Russian propaganda campaign reportedly exposed 38 million German and French users to political advertisements on a major social media platform. Additionally, Russian disinformation is highly likely to ramp up since the collapse and the resultant upheaval of Olaf Scholz's three-way coalition, which is likely to bring added political volatility to Germany's snap elections—creating opportunities for foreign threat actors and their disinformation campaigns. Disinformation could be used to incite divides among the people, exaggerate/misconstrue opposition narratives, or undermine public trust in democratic institutions. Since at least 2022, Russian disinformation and misinformation has reportedly attempted to sow discord by shaping public opinion. Russia has attempted to disparage and spread false narratives about Ukraine and, allegedly, Germany's support to Ukraine at the cost of its people. In addition to Germany, Russia has also interfered with other high-profile elections in 2024. In the months and days leading up to the U.S. elections, ZeroFox [observed](#) Russian cyber activity that likely posed the greatest threat to the election. Threats reportedly stemmed from Russian state media outlets such as Russia Today (RT) and Tass, as well as fabricated news sites that attempt to spoof the domains of legitimate U.S. media outlets in order to lure unsuspecting visitors before presenting them with disinformation.



Telegram's Recent Policy Shift Leads Threat Actors to Platform Exodus and Backup Channels

What happened: ZeroFox has observed significant shifts in the behavior of threat actor groups following recent changes to Telegram's policies. The platform now allows users to report illegal activities for automated takedown or manual moderation, and its updated privacy policy permits the disclosure of users' phone numbers and IP addresses if a valid court order is issued. In response to these changes, threat actors—including groups like Anonymous Collective, Dark Storm

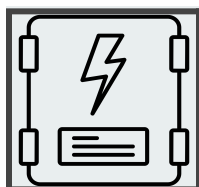
Team, and Mysterious Team Bangladesh—have begun deleting their Telegram channels. They are also removing links to these channels and reorganizing their operations to create new backup channels to ensure continued communication and evade detection.

- > **What this means:** The new policy changes on Telegram have prompted threat actors to adopt a more cautious and decentralized approach to avoid exposure and maintain their illicit activities. By deleting channels and moving communications to alternative platforms such as X (formerly Twitter) and Discord, these groups are attempting to reduce the risk of being traced or banned from Telegram. The shift towards backup Telegram channels suggests that threat actors are seeking redundancy and resilience in their operations, while also attempting to keep their activities under the radar of both users and law enforcement. Essentially, these groups are adjusting their tactics to stay one step ahead of security efforts aimed at disrupting their operations. This shift in behavior illustrates the ongoing challenge of combating cybercrime in an increasingly decentralized digital landscape. The fact that threat actors are evolving their tactics to bypass platform-specific controls indicates that efforts to curb illegal activities through centralized platforms like Telegram may not be sufficient. The increasing reliance on multiple communication channels complicates detection and enforcement, making it harder for authorities and platforms to effectively track and prevent illicit actions. Meanwhile, pro-Palestine hacktivist group RipperSec (allegedly operating from Malaysia) made [statements](#) about many teams being banned on Telegram, including NoName Eng, AlixSec, and Moroccan Dragons. According to RipperSec, its "Spy Team" has concluded that the leaders of ransomware groups AzzaSec and DoubleFace are responsible for attacking multiple groups, and they employ unknown tools to ban numerous hacktivist channels.

| **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, industrial control systems (ICS), and government services. Threat actors have recently begun to target end-of-life D-Link network attached storage (NAS) devices that have a critical severity vulnerability ([CVE-2024-10914](#)) after D-Link said it would no longer support end-of-life D-Link devices. Microsoft's November 2024 Patch Tuesday [addressed](#) 91 vulnerabilities, including four zero-days (two actively exploited). Key fixes include critical remote code execution and privilege escalation flaws across Windows 10 and 11 updates. Microsoft also [fixed](#) bugs in Windows Server 2025, causing installation, upgrade, and Blue Screen of Death (BSOD) issues on high-core-count systems. Citrix has [addressed](#) vulnerabilities in its Virtual Apps and Desktops' Session Recording feature, clarifying that exploitation requires authentication. A vulnerability in PostgreSQL's PL/Perl extension ([CVE-2024-10979](#)) allows arbitrary code execution and data access, affecting versions before 17.1. [Fortinet](#), [Adobe](#), and [Ivanti](#) have released security updates to address vulnerabilities in multiple products. CISA [released](#) two [advisories](#) about seven exploited vulnerabilities. It also [released](#) 24 ICS [advisories](#). CISA, collaborating with international cybersecurity agencies, released an [advisory](#) to provide details collected and compiled by the authoring agencies about the Common Vulnerabilities and Exposures (CVEs) routinely and frequently exploited by malicious cyber actors in 2023.



CRITICAL

CVE-2023-4699

What happened: A vulnerability has been identified in various Mitsubishi Electric industrial products, including several series of their CPU modules and CNC systems. This flaw, categorized as a "Missing Authentication for Critical Function," allows an attacker to send specially crafted network packets to the affected devices. These packets bypass the authentication process, enabling the attacker to execute arbitrary commands remotely without needing to authenticate. As a result, the attacker can interact with the device's control systems, potentially compromising the system's integrity and operations.

- **What this means:** The impact of this vulnerability is significant, as it could lead to several types of malicious activities. Attackers could manipulate control programs, potentially causing operational disruptions or even catastrophic system failures. They could also gain unauthorized access to sensitive data or tamper with critical information. Moreover, the

attacker could induce a denial-of-service (DoS) condition by resetting the device's memory to factory settings, effectively rendering the affected equipment inoperable or severely degraded.

➤ **Affected products:**

- CISA has [listed](#) the affected products in the ICS advisory addressing this bug.



CRITICAL

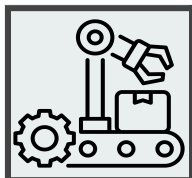
CVE-2024-9463

What happened: CVE-2024-9463 is an operating system (OS) command injection vulnerability in Palo Alto Networks Expedition that allows an unauthenticated attacker to run arbitrary OS commands as root in Expedition, resulting in the disclosure of usernames, cleartext passwords, device configurations, and device API keys of PAN-OS firewalls.

- **What this means:** These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise. CISA has [added](#) this vulnerability, as well as CVE-2024-9465, to its Known Exploited Vulnerabilities (KEV) Catalog based on evidence of active exploitation.
- **Affected products:**
 - Palo Alto Networks Expedition versions affected from 1.2.0 before 1.2.96

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

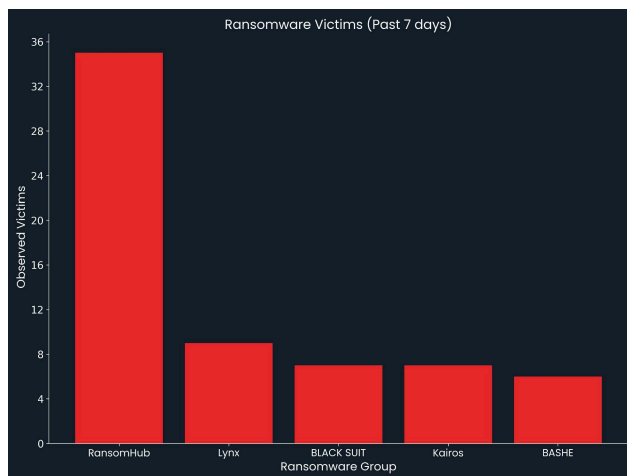


Ransomware Attacks on Critical Infrastructure Industries

What happened: A new ransomware family, [Ymir](#), has been identified as encrypting systems compromised earlier by the RustyStealer malware. RustyStealer, a credential-harvesting tool, helped attackers gain high-privilege access, allowing lateral movement across networks before deploying Ymir. Ymir executes from memory, evading detection, and uses the ChaCha20 cipher to encrypt files, generating ransom notes in PDF format in directories containing encrypted files. In other news, Halliburton has revealed that the company suffered a loss of almost USD 35 million because of a ransomware attack in August. It

[experienced](#) a USD 0.02 per share impact on its adjusted earnings from lost or delayed revenue due to the ransomware attack and storms in the Gulf of Mexico. [Newpark Resources](#), a Texas-based oil drilling services provider, was hit by a ransomware attack, causing disruptions to some of its information and business systems. The company reported limitations in access to key operational and corporate functions, including financial reporting. Following the breach, Newpark activated its security response plan and restricted access to affected systems. ZeroFox has [observed](#) an update on the Embargo Ransomware leak site targeting American Associated Pharmacies (AAP), United States. AAP reportedly fell victim to the Embargo ransomware gang, which claims to have stolen and encrypted 1.469 TB of AAP's data. Embargo alleges that AAP paid USD 1.3 million for decryption and is demanding an additional USD 1.3 million to prevent data leaks. AAP has not confirmed the attack, but all user passwords were recently force-reset on its websites, possibly indicating security concerns. Foreign hackers [breached](#) Hungary's Defence Procurement Agency, but no sensitive military data was reportedly accessed. The compromised information included military procurement plans, but officials confirmed there are no national security risks.

- > **What this means:** Cybercriminals working together is likely an upward trend. This year saw another collaboration similar to that of North Korea-linked [Andariel](#) and the Play ransomware group, wherein information stealers act as access brokers for ransomware



Source: ZeroFox Internal Collections

deployment. Ymir's in-memory execution and advanced encryption make it hard to detect, posing a heightened risk to organizations. Such tactics could accelerate the spread and impact of ransomware threats. This hybrid approach could make ransomware more resilient to standard detection methods and heighten recovery costs due to encrypted data and possibly stolen credentials. Halliburton has yet to confirm the technical scope of the breach and the impacted data amid ongoing investigations into the ransomware attack. It is likely that the company will incur more losses in legal fees, given that the threat actors were able to exfiltrate some data in the attack. Additionally, the threat actors are likely to leak or sell the exfiltrated data to other threat actors or competitors of Halliburton, despite ransom negotiations. A ransomware attack on critical infrastructure, like that on Newpark Resources, poses significant risks. Such disruptions can halt essential operations, potentially endangering public safety and causing economic fallout due to downtime. Compromised systems may expose sensitive operational data, opening pathways for further attacks or espionage. Additionally, critical infrastructure often serves interconnected industries, where disruptions can impact supply chains and other sectors reliant on continuous operation. Ransomware attacks on healthcare organizations like AAP expose sensitive information, disrupt essential services, and have high financial costs. With AAP overseeing a large network of independent pharmacies, compromised data could affect countless patients, risking exposure of private health information and financial records. While no highly classified information was reportedly accessed, the attack can still likely expose potential gaps in security, which could reveal trends or vulnerabilities for future attacks. In the past seven days, ZeroFox has observed over 150 ransomware attacks (mostly on the healthcare sector) primarily conducted by the RansomHub ransomware group. Over 45 percent of these targeted industries are from North America.



Data Breaches Hit Retail, Gaming, and More in the Past Week

What happened: In the past seven days, a series of significant data breaches affecting millions of individuals across various industries have been reported. Over 54 million customers of Hot Topic, Box Lunch, and Torrid had their personal and financial information [exposed](#), including names, emails, birthdays, phone numbers, addresses, purchase histories, and encrypted credit card numbers. A breach in the Dominican Republic reportedly [compromised](#) vaccination records and personal identifiers, while a leak from a B2B data aggregator [exposed](#) contact information for over 100 million people. The leaked data was initially offered for sale on BreachForums in February 2024.

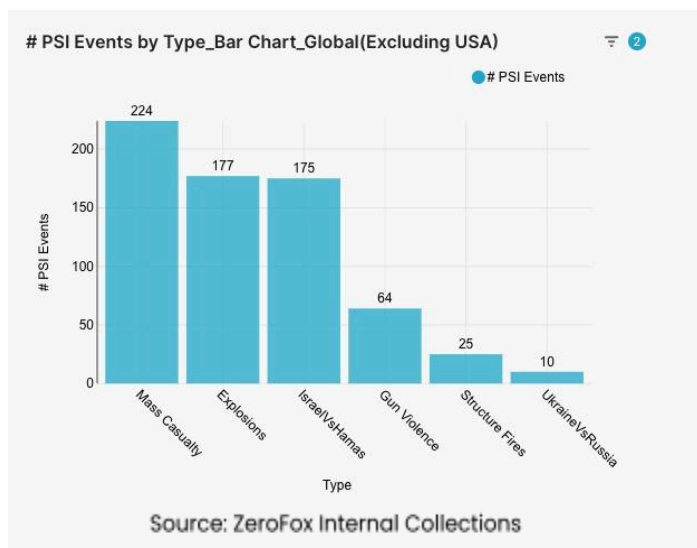
for USD 6,000. ZeroFox [observed](#) that the data was reportedly exposed on BreachForums in August 2024, leaving millions of business contacts vulnerable to potential misuse. The DeFi Capital Investment Fund also reportedly [suffered](#) a breach, exposing sensitive investor data. In another incident, the Qatar Olympic Committee's database was compromised, leaking details about athletes and staff. Threat actor Coloniza [claimed](#) to have leaked the database on dark web forum BreachForums. A major data breach exposed [sensitive](#) information from the German Federation's statistical database on the dark web, including 3.8GB of governmental data, raising concerns over national security. LinkedIn [experienced](#) a breach exposing the personal and professional details of 50,000 users. Threat actor 888 claimed responsibility for leaking databases from U.S.-based motorcycle company [Appleton Harley-Davidson](#) and [Tibber](#), a Norwegian-Swedish energy company. The Appleton Harley-Davidson breach reportedly exposed 19,729 rows of customer data, including names and email addresses, while the Tibber breach affected 243,000 rows, revealing names, usernames, email addresses, postal codes, and activity details. Other high-profile incidents involved [Roblox](#), a popular gaming platform, and a Michelin-starred [restaurant](#) in Singapore. Roblox experienced a breach that affected millions of users, a particular concern given its young audience. Meanwhile, the data leak involving the Michelin-starred restaurant exposed the personal information of 148,000 customers, and the leaked data has since been listed for sale on a dark web forum.

- **What this means:** The recent wave of data breaches across various sectors highlights the growing and widespread risks posed by cyberattacks. The exposure of personal and financial information for over 54 million customers of retailers like Hot Topic, Box Lunch, and Torrid puts millions at risk for identity theft, financial fraud, and targeted phishing attacks. Similarly, the breach in the Dominican Republic, which compromised vaccination records and personal identifiers, threatens not only individual privacy but also the integrity of public health data. The leak from a B2B data aggregator, affecting over 100 million individuals, exposes a massive trove of contact information that can be exploited for spam, scams, and business email compromise. Meanwhile, the breach of DeFi Capital's sensitive investor data raises concerns about financial security and insider threats in the rapidly growing world of decentralized finance. The Qatar Olympic Committee's database leak puts athletes' personal and professional information in the hands of malicious actors, potentially leading to privacy violations and targeted harassment. In Germany, the exposure of 3.8GB of government data on the dark web raises serious national security concerns, while LinkedIn's breach impacting 50,000 users highlights the risks to professional reputations and career prospects. Data leaks from Appleton Harley-Davidson and Tibber put customer information at risk, exposing individuals to potential fraud and identity theft. Roblox's breach, especially concerning given its young user base, highlights the dangers of exposing personal data in gaming environments, while the leak from a Michelin-starred restaurant in Singapore demonstrates how even seemingly low-risk

industries can fall victim to cybercriminals. Each of these incidents not only exposes sensitive data but also undermines trust in the security of organizations and platforms, with long-term implications for individuals and businesses alike.

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings



Physical Security

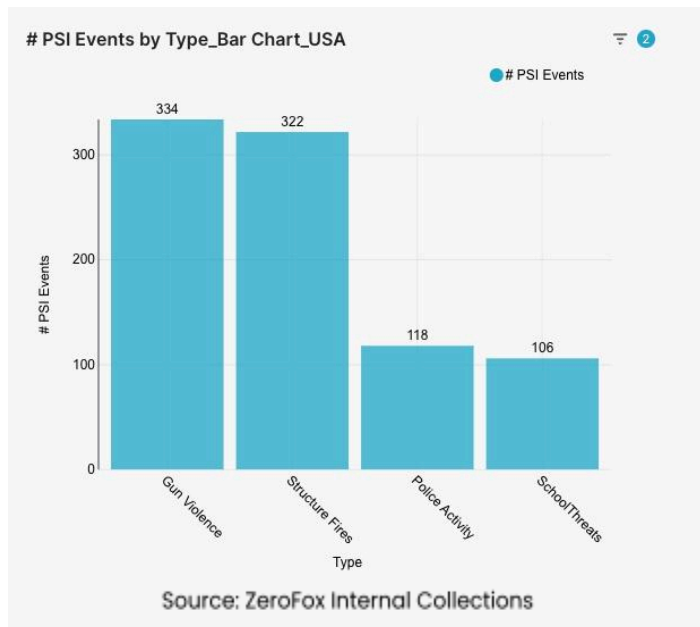
Intelligence: Global

What happened: Excluding the United States, there was a 10 percent increase in mass casualty events this week from the previous week, with the top contributing countries being Lebanon, Israel, and Palestine in that order. Approximately 79 percent of these events were explosions, and the three aforementioned countries accounted for about 50 percent of all mass casualty alerts. General alerts

related to the Israel-Hamas War (including protests, raids, and involvement in neighboring countries) decreased by 13 percent from the previous week. Events related to Russia's war in Ukraine decreased by 17 percent. The top three most-alerted subtypes were explosions, which saw a 4 percent increase from the previous week; gun violence, which increased by 52 percent; and structure fires, which decreased by 44 percent. Global protest activity increased by 20 percent.

- > **What this means:** This week, gun violence increased substantially, with Guatemala and Mexico being the top contributing countries to these alerts. For instance, In Mexico, there was a shooting [attack](#) on Los Cantaritos bar in Queretaro's downtown district, which left 10 people dead and at least seven injured. Spiraling violence, much of it linked to drug trafficking and gangs, has seen more than 450,000 people murdered in Mexico since 2006. Unlike gun violence, structure fires actually saw a significant decrease, with Chile once again being the top contributor. As Chile leaves its winter season and temperatures begin to rise, heating devices are not utilized as often, which explains the decrease in structure fire alerts overall. Lebanon had the highest number of mass casualty alerts and undoubtedly contributed to the overall increase of this subtype. Israel launched [airstrikes](#) on Beirut's Hezbollah-controlled southern suburbs on November 15, keeping up an intensive bombardment of the area for a third consecutive day. However, an Israeli security cabinet member indicated that a ceasefire was closer than at any point since the war began, though he said a sticking point was ensuring Israel retains the freedom to act inside Lebanon should any deal be violated.

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 that had the most gun violence alerts were Illinois and New York, which together made up 24 percent of this week's nationwide total. Gun violence

across the United States overall decreased by 2 percent from the week prior. Police activity alerts increased by 22 percent, and the top contributing states were California and Ohio. Structure fires increased by 14 percent, and the top two states for this subtype were California and New York. Notably, active shooter instances increased by 44 percent.

- > **What this means:** As expected, structure fires increased somewhat significantly, particularly in places with dry climates and densely populated buildings. According to the National Fire Protection Association, home fires occur more in the [winter](#) than in any other season, and heating equipment is involved in one of every six reported home fires. Police activity alerts, which also saw a substantial increase, are often precursors to more serious events that get upgraded to other incident types as more information regarding the law enforcement presence becomes available. Ohio was one of the top contributing states, and it had one of these exact situations unfold earlier this week: the Purina Pet Care plant in Williamsburg Township was evacuated Monday morning, which was alerted with the police activity tag. It was then discovered to be a bomb threat and was re-alerted as such. So, an increase of police activity could be related to increases in other types of events as well. The recent presidential election has also caused some tension and is likely to continue to do so as the transfer of power inches closer.

| 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%