



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

November 4, 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 November 1, 2024**; 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 November 2024 Geopolitical Brief	2
 Cyber and Dark Web Intelligence Key Findings	4
Russian Espionage Campaign Targets Ukrainian Military Recruits with Malware	4
Law Enforcement Action Across the World	5
LottieFiles Supply Chain Attack Exposes Users to Malicious Crypto Wallet Drainer	6
 Exploit and Vulnerability Intelligence Key Findings	8
CVE-2024-50388	9
CVE-2024-47901	9
 Ransomware and Breach Intelligence Key Findings	11
PSAUX Ransomware Attack and the Rise of Collaborative Cybercrime	11
Threat Actors Endanger People's Privacy and Corporate Resources in Global Breaches	12
 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

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence November 2024 Geopolitical Brief

Several Latin American states (led by Peru and Bolivia) are experiencing protest movements reminiscent of the 2019 indefinite protest period, which led to widespread changes in political leadership months later. European authorities are growing increasingly concerned that Russia and Iran are financing criminal groups to carry out acts of sabotage and violence across Europe. The deployment of North Korean troops to Russia carries significant new security considerations for both Europe and the Korean Peninsula. Brazil will host the G20 Summit in mid-November; it is arguably the premier geopolitical forum in the world. However, major takeaways on key issues like war in Ukraine and the Middle East are unlikely with U.S. politics in flux.

| Cyber and Dark Web Intelligence |

| Cyber and Dark Web Intelligence Key Findings



Russian Espionage Campaign Targets Ukrainian Military Recruits with Malware

What happened: UNC5812, a suspected Russian hybrid espionage group, launched an operation targeting the Ukrainian military through a Telegram channel named Civil Defense and a corresponding website. The campaign, active since September 10, 2024, uses operating system (OS) malware to compromise devices. Android OS users are tricked into disabling specific security software, allowing the installation of a remote access trojan (CraxsRAT) hidden within a decoy mapping app called SUNSPINNER. On another popular OS, malware delivery is facilitated through ZIP files containing the Pronsis loader, which distributes SUNSPINNER and PureStealer malware. Beyond malware distribution, UNC5812 also runs influence operations to disrupt Ukrainian military mobilization by spreading anti-recruitment narratives across messaging platforms.

- **What this means:** Russian state actors have been increasingly integrating sophisticated cyber tools in influence campaigns, exploiting common messaging platforms like Telegram for malware delivery and psychological warfare. By using Telegram—a popular social networking and communicating platform—to offer free software that helps conscripts find and share crowdsourced locations of Ukrainian military recruiters, the actors take advantage of the anxiety around conscription. Legitimate Ukrainian-language channels have unknowingly promoted Civil Defense, suggesting that actors can leverage trusted spaces for state-backed operations, complicating efforts to filter misinformation. Furthermore, the ability to bypass security checkpoints highlights gaps in OS security that could become critical for countries at war, where every compromised device poses a strategic threat. Finally, integrating commodity malware, like PureStealer and CraxsRAT, likely indicates that threat actors are blending off-the-shelf tools with custom loaders for scalability. On the other hand, Telegram's permissive stance on privacy has recently drawn backlash following the arrest of its CEO, Pavel Durov, in France. Durov's arrest and the backlash surrounding under-moderation have forced Telegram to reconsider its policies. The company has now committed to sharing more user data with governments and modifying its stance on illegal content—shifts that previously would have seemed unimaginable for a service built around privacy and free speech principles.



Law Enforcement Action Across the World

What happened: This week saw several high-profile law enforcement actions targeting threat actors across the world. Six individuals have been [charged](#) in the United States for their roles in schemes to rig bids, defraud the government, and pay bribes and kickbacks in connection with the sale of IT products and services to federal government purchasers. These are the first charges in the Justice Department's ongoing investigation into IT manufacturers, distributors, and resellers who sell products and services to government purchasers, including to the intelligence community. Dutch National Police, in collaboration with the FBI and other international law enforcement bodies, have disrupted the operations of the Redline and Meta infostealers in an operation called [Operation Magnus](#). They seized the source codes, user data, and identifying information of individuals who used the malware. Four members of the REvil ransomware group have been sentenced to several years in prison in Russia for illegal circulation of payment methods. The Russian Federal Security Service (FSB), in collaboration with the Interior Ministry, [conducted](#) raids across multiple regions and detained 14 suspects linked to the group, though the investigation is still ongoing to determine each individual's involvement in the crimes.

- **What this means:** The six defendants' actions reportedly resulted in overcharges of millions of dollars to the U.S. government, including the Department of Defense (DOD). As alleged in the indictment, the co-conspirators used their positions of trust to learn sensitive, confidential procurement information—including procurement budgets for large U.S. government IT contracts. The co-conspirators used that inside information to craft bids at artificially determined, non-competitive, and non-independent prices, ensuring the accused would win the procurement. Even though it is very likely that new infostealers will emerge to take their place, the revelation of RedLine and Meta user identities will likely expose frequent buyers and disrupt criminal collaborations. Authorities can also use the user data from the seized information to study patterns of threat actor activity or identify imminent threats. As one of the most prominent cybercriminal groups globally, REvil was responsible for major breaches, including attacks on Apple, JBS, and the Texas government. With key members arrested and their financial assets seized, the group's ability to operate has been severely disrupted. This could not only decrease the frequency of large-scale ransomware attacks but also serve as a deterrent to other cybercriminals. The arrest of REvil's members may reveal additional information about the group's dealings and other tactics and techniques, which can likely aid further law enforcement agencies in tracking other active threat groups.



LottieFiles Supply Chain Attack Exposes Users to Malicious Crypto Wallet Drainer

What happened: Software-as-a-service platform LottieFiles' Lottie-Player project recently fell victim to a supply chain attack that resulted in the injection of a crypto-drainer script into various websites. This malicious script is designed to target Lottie-Player users connecting their cryptocurrency wallets, ultimately stealing their assets and NFTs. Reports indicate that at least one individual lost a staggering USD 723,000 in Bitcoin due to this breach. In response, LottieFiles quickly released updated version 2.0.8 and urged users to upgrade immediately. For those unable to do so, it is essential to communicate the potential risks to Lottie-Player end users and caution them against fraudulent wallet connection requests.

- **What this means:** With Bitcoin prices rising again, scams like the recent LottieFiles incident are likely to increase. This incident shows the growing threat of crypto drainers within the cryptocurrency ecosystem, as cybercriminals increasingly exploit vulnerabilities in widely-used software to target unsuspecting users to steal assets. The broader implications are concerning, as this attack reflects a trend of sophisticated tactics employed by threat actors, including hacking prominent social media accounts, compromising websites, and deploying AI-generated videos alongside malicious advertising to direct users to sites embedded with harmful scripts. LottieFiles is actively investigating the breach with the help of external experts. As the situation unfolds, further details may emerge, shedding light on the full scope of the attack and its impact on users.

| **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, network technology, and software development services. Fog and Akira ransomware groups breached corporate networks through VPN accounts by exploiting critical vulnerability [CVE-2024-40766](#). Although the flaw was patched in August 2024, attackers quickly leveraged it, executing at least 30 remote access intrusions, with 75 percent of these attacks tied to Akira. Researchers have discovered a new attack targeting a popular OS that leverages CVE-2024-21302 and CVE-2024-38202 to bypass Driver Signature Enforcement (DSE) via OS downgrades, [enabling](#) rootkits unless VBS with UEFI lock and Mandatory mode are enforced. Both bugs have been previously addressed, with an opt-in mitigation available as an interim solution for [CVE-2024-21302](#) and a workaround available for [CVE-2024-38202](#) to reduce the risk of exploitation. Apple's visionOS 2.1 update [addresses](#) over 25 critical security vulnerabilities, including a kernel memory corruption bug (CVE-2024-44285) and a path handling problem allowing unauthorized data access (CVE-2024-44255). It also fixes WebKit memory corruption vulnerabilities (CVE-2024-44244 and CVE-2024-44296) and enhances user privacy with improved data redaction (CVE-2024-44262). Apple has also released security updates for [iOS 18.1 and iPadOS 18.1](#), [iOS 17.7.1 and iPadOS 17.7.1](#), [macOS Sequoia 15.1](#), [macOS Sonoma 14.7.1](#), [macOS Ventura 13.7.1](#), [watchOS 11.1](#), and [tvOS 18.1](#). In other news, Pwn2Own Ireland 2024 [awarded](#) USD 1,066,625 to participants for exploiting 70+ zero-day vulnerabilities. Notable exploits included TrueNAS X and Lexmark printers. CVE-2024-41992 is a command injection flaw in the Wi-Fi Test Suite, [enabling](#) unauthenticated attackers to execute arbitrary commands with root privileges on Arcadyan routers. A new automated exploit, Muraider, has been [observed](#) abusing SQL injection vulnerability CVE-2024-32640 to infect websites that use affected CMS versions. [CVE-2024-10456](#) affects Delta Electronics InfraSuite Device Master versions prior to 1.0.12, which suffer from a deserialization vulnerability that targets the Device-Gateway and could allow deserialization of arbitrary [.]NET objects prior to authentication. The Cybersecurity and Infrastructure Security Agency (CISA) has added [seven](#) Industrial Control Systems (ICS) advisories.

**CRITICAL****CVE-2024-50388**

What happened: A vulnerability involving OS command injection has been identified in HBS 3 Hybrid Backup Sync. If exploited, this issue could enable remote attackers to execute arbitrary commands on the affected system.

- **What this means:** This vulnerability allows unauthorized users to execute commands with the same privileges as the application, potentially enabling attackers to manipulate the system, access sensitive data, or disrupt operations. Organizations using HBS 3 Hybrid Backup Sync should prioritize applying security updates and implementing measures to mitigate this risk. To address the vulnerability, users should update to the latest version of HBS 3 Hybrid Backup Sync.
- **Affected products:**
 - HBS 3 Hybrid Backup Sync 25.1.x

**CRITICAL****CVE-2024-47901**

What happened: The web server of affected devices does not sanitize the input parameters in specific GET requests that allow for code execution on the OS level. In combination with other vulnerabilities (CVE-2024-47902, CVE-2024-47903, and CVE-2024-47904), this could allow an unauthenticated remote attacker to execute arbitrary code with root privileges.

- **What this means:** Successful exploitation of these vulnerabilities could allow an attacker to perform remote code execution (RCE), write arbitrary files, or execute arbitrary commands.
- **Affected products:**
 - InterMesh 7177 Hybrid 2.0 Subscriber: All versions prior to V8.2.12
 - InterMesh 7707 Fire Subscriber: All versions prior to V7.2.12

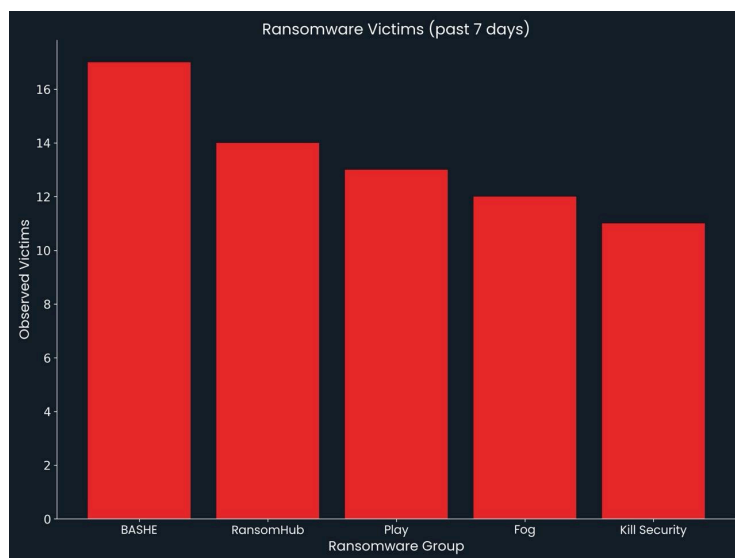
| Ransomware and Breach Intelligence |

Ransomware and Breach Intelligence Key Findings



PSAUX Ransomware Attack and the Rise of Collaborative Cybercrime

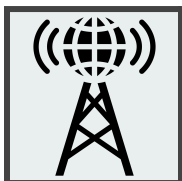
What happened: In the past seven days, ZeroFox has observed over 150 ransomware attacks (mostly on the manufacturing sector) primarily conducted by the BASHE ransomware group. Over 60 percent of these targeted industries are from North America. On October 25, 2024, ZeroFox [observed](#) APT73/ERALEIG ransomware group rebranding as BASHE. Meanwhile, over 22,000 CyberPanel instances were [targeted](#) in a PSAUX ransomware attack via critical RCE vulnerabilities, leading to widespread service disruptions. Attackers exploited these flaws to gain unauthorized access, impacting numerous services. Notably, Security researchers have observed collaborative efforts among foreign threat actors. Recently, a North Korea-linked group known as Andariel [reportedly](#) partnered with the Play ransomware group in a cyber incident. It is still unclear if this collaboration was a one-time event, whether Andariel may be acting as an initial access broker for the Play ransomware group, and if future collaborative efforts are likely.



Source: ZeroFox Internal Collections

- **What this means:** A threat-intelligence search engine has identified nearly 22,000 vulnerable CyberPanel instances visible online, with a substantial number located in the United States. The mass exposure of these vulnerabilities shows the critical need for timely software updates and robust security practices. This situation heightens the risk of cyberattacks—particularly ransomware incidents, as attackers are drawn to easily exploitable targets. The widespread nature of these vulnerabilities can result in significant operational disruptions for businesses that depend on affected instances, potentially leading to costly downtime and revenue loss. Moreover, unauthorized access may facilitate data breaches, raising serious privacy concerns and compliance issues with regulatory standards. Collaborations among threat groups, such as the recent partnership between Andariel and the Play ransomware group, likely enhance their ability to execute streamlined attacks, enabling them to evade detection more effectively. By combining

resources, these groups can target larger or more complex networks, increasing the overall risk to organizations. If such collaborations continue in the future, they can potentially foster an ecosystem in which cybercriminals share tools, infrastructure, and intelligence, leading to more persistent and sophisticated threats. As the threat environment grows more complex, businesses must prioritize cybersecurity strategies to mitigate risks and protect sensitive data.



Threat Actors Endanger People's Privacy and Corporate Resources in Global Breaches

What happened: Hackers [breached](#) the systems of French internet service provider (ISP) Free, stealing some customers' personal information, including international bank account numbers (IBANs) for certain subscribers, though passwords, payment data, and communications content remained secure. ZeroFox observed threat actor kzoldyck [claiming](#) to have leaked a database associated with Interbank in Peru on predominantly English-language dark web forum BreachForums. The actor alleged that Interbank suffered a data breach on October 30, 2024, exposing information on approximately three million customers. [Investigations](#) are still underway to determine the specific victims of the breach that affected 800,000 people in Italy. The attack reportedly breached Italian law enforcement, tax authorities, and other public data. The cause of the attack is reportedly being attributed to a private investigative agency, and investigations are currently attempting to unearth the actor responsible for this breach. Long Island Plastic Surgical Group has confirmed that the data of more than 161,000 individuals was [compromised](#) in a cyber incident early this year. The breach involved a network intrusion in which the threat actors exfiltrated data. It was confirmed that personally identifiable information (PII)—including names, dates of births, Social Security numbers, medical data, biometric data, and clinical photographs—was stolen.

- **What this means:** Free's breach exposed a large ISP's vulnerability, endangering customers' financial and personal data security. Although Free secured sensitive information like passwords and payment details, stolen IBANs could still be misused in phishing attacks or for fraud. Scammers can likely combine these partial data points with social engineering to deceive victims, especially when customers are unaware their data has been compromised. At the time of writing, the breach reportedly has not impacted Free's services, while the company swiftly implemented measures to secure its systems. The Interbank data breach poses significant risks to the victims' exposed sensitive customer information, which could lead to widespread financial fraud, phishing schemes,

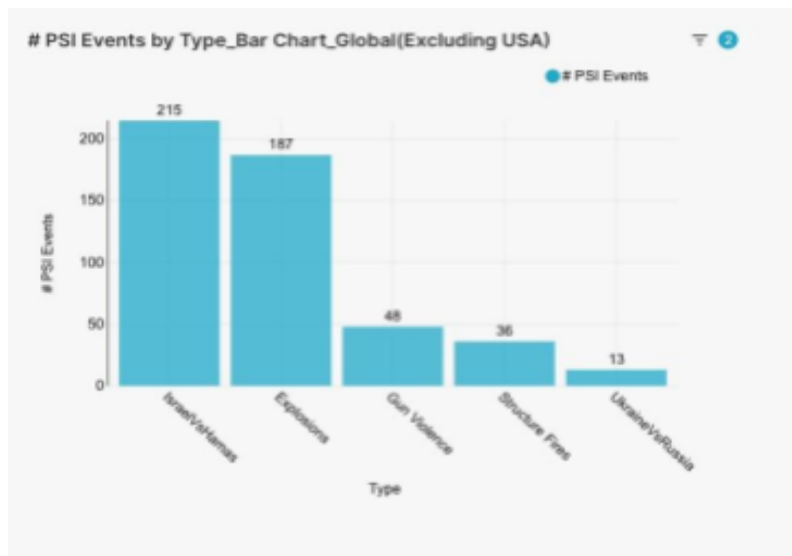
and identity theft. This breach is likely to place a large portion of Peru's population at risk for scams and financial exploitation. Additionally, the posting of this data on BreachForums increases the likelihood that cybercriminals globally may exploit it. The breach of public data in Italy, affecting over 800,000 citizens, has raised serious concerns about digital security and privacy. With high-profile targets including business and political figures, this incident underscores vulnerabilities in critical government databases. Italian officials are now calling for stronger protections, emphasizing that such breaches pose a significant threat to democracy by potentially exposing individuals to manipulation, blackmail, or fraud. Breaches affecting a large healthcare institution like Long Island Plastic Surgical Group endanger sensitive information, especially clinical photos. The threat actors responsible are likely to be more incentivized to press both the institution and patients for exorbitant ransom demands, and patients will likely readily give in to these demands to protect their identity and privacy. Threat actors may even engage in double extortion, whereby threat actors harass the victims to further expose compromised data. Long Island Plastic Surgical Group said that it will continue to monitor the situation and further enhance security measures.

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 3 percent decrease in Mass Casualty incidents perpetrated by actors across the globe this week, with Lebanon, Israel, and Palestine contributing the highest alerts in the category; approximately 65 percent of these events were Explosions. General Alerts pertaining to the Israel-Hamas war (including protests, raids, and involvement in the neighboring countries) decreased by 5 percent. Notably, Palestine and Israel accounted for 40 percent of the total Explosions alerts. Additionally, events related to the ongoing Ukraine-Russia war increased by 85 percent. The top three most alerted sub-types were Explosions, Gun Violence, and Structure Fires. Explosions and Gun Violence decreased by 7 percent and 16 percent, respectively, while Structure Fires increased by 50 percent compared to last week.



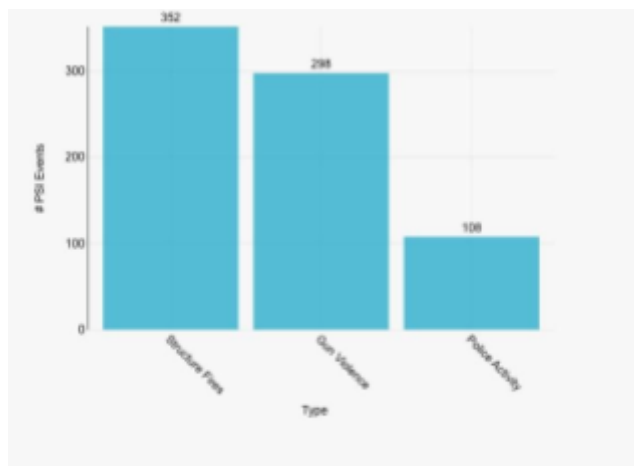
Source: ZeroFox Internal Collections

- **What this means:** The war between Israel and Hamas continued this week, showing no signs of de-escalation. [Thirty-five people were killed](#) in a bombing by Israeli Defense Forces on a residential area in Beit Lahiya, and 53 others were killed during an attack on [Asmaa School](#) in Gaza. On Tuesday, October 29, [109 people were killed](#) in a targeted attack in Northern Gaza, with 93 additional deaths in Beit Lahiya. Bombings in Lebanon continued, with attacks on Sidon that claimed the lives of 33 people and on Southern Lebanon's [Ain Baal](#), where 24 people were killed. This week Israel conducted large-scale attacks on several Iranian cities in a matter of a few hours that severely compromised Iran's surface-to-air capabilities, as well as several missile-producing industries. The war between Ukraine and Russia has gained momentum since last week; 35 people being killed in a targeted attack on a residential building in [Kharkiv](#) on Tuesday. In Horlivka Donetsk, a [public transport facility](#) was targeted by bombing, killing one and injuring two people. In Russia, Ukraine targeted a [chemical distillery](#) of a Russian rocket fuel supply chain using a drone in the Novokhoper district of the Voronezh region. Gun Violence-related incidents decreased this week; however, there were reports of Gun

Violence in the Middle East and Asia. The major incident in this subtype was the attempted killing of the former President of Bolivia, [Evo Morales](#), which resulted in the injury of one person. Structure Fires showed a 50 percent increase, with alerts from the Americas region. Global Protest activity this week saw a decline of 9 percent compared to the previous week.

Physical Security Intelligence: United States

What happened: In the past week, the most alerted subtypes were Gun Violence, Structure Fires, and Police Activity. Illinois and California recorded the highest number of incidents in the Gun Violence category with 49 and 24 alerts, respectively; together both states contributed 24 percent of the total alerts this week. Police Activity, with 108 alerts, increased by 18 percent compared to last week. California and Ohio alerted the highest number of incidents in the subtype, contributing 27 percent to the total. Alerts pertaining to Shots Fired incidents decreased by 8 percent this week, and Structure Fires remained the same. Compared to last week, School Threats increased by 26 percent.



Source: ZeroFox Internal Collections

- What this means:** Police Activity are instances where a large number of police officers respond to address incidents, including Standoffs, Hostages, and School Threats. Incidents of this nature increased this week, along with School Threats. Despite showing a dip in the number of alerts compared to the previous week, Mass Casualty Gun Violence incidents were reported across the United States. Structure Fires remained the same compared to last week; New York and California were the largest contributors of alerts in the subtype. Over the weekend, [21 people were shot](#) in different parts of Chicago, resulting in four deaths. This week also saw a large standoff with an armed individual at the Four Seasons hotel in Midtown Atlanta, Georgia. With the U.S. election season in full swing and the final voting one day away, there were disturbances to the electoral procedure this week. On Monday, [voting ballots sitting in drop boxes](#) were set on fire using incendiary devices in Washington and Portland, Oregon. This incident near the Washington-Oregon border might be related to the ballot burning that occurred months ago in Vancouver, Washington. Additionally, a mob of disorderly people were also seen near the [Kent Island Volunteer Fire Station in Maryland](#). ZeroFox assesses it is likely that such violence will increase in the upcoming final stretch of the U.S. elections.

| 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%