



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

February 3, 2025

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 January 31, 2025**; 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 Assessment Russia-Ukraine Forecast 2025	2
Super Bowl LIX Event Assessment	2
ZeroFox Intelligence Brief – Underground Economist: Volume 5, Issue 2	2
ZeroFox Intelligence February 2025 Geopolitical Brief	3
 Cyber and Dark Web Intelligence Key Findings	5
DeepSeek: Cyberattack and Data Exposure	5
New Smishing Campaign Targets USPS Customers with Phishing PDFs	6
Fraud Ring Members Charged in Multi-Million Dollar BEC and Money Laundering Scheme	6
 Exploit and Vulnerability Intelligence Key Findings	9
CVE-2025-22604	9
CVE-2024-12248	10
 Ransomware and Breach Intelligence Key Findings	12
CI0p Reveals Second Victim List; Ransomware Hits Healthcare and ESXi This Week	12
Data Breaches and Their Impacts on Several Entities	13
 Physical and Geopolitical Intelligence Key Findings	16
Physical Security Intelligence: Global	16
Physical Security Intelligence: United States	17
 Appendix A: Traffic Light Protocol for Information Dissemination	18
 Appendix B: ZeroFox Intelligence Probability Scale	19

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Assessment Russia-Ukraine Forecast 2025

The incoming Trump administration is likely to be one of the most consequential, yet unpredictable, influences on the Russia-Ukraine conflict in 2025. Neither Ukraine nor Russia likely have the military resources or capacity to win the war outright on the battlefield in 2025. As a result, the conflict is highly unlikely to see any strategic-level offensives that alter the course of the war. The Trump administration is likely to pursue diplomatic talks shortly after taking office to achieve a quick end to the conflict. Both Russia and Ukraine have indicated they would be open to such discussions, though numerous roadblocks may hinder the process. The state of its economy is highly likely to be Russia's largest vulnerability in 2025, though President Vladimir Putin is unlikely to let the economy influence his strategy in Ukraine. Hacktivist groups will very likely seek to complement Russia's battlefield gains and Ukraine's manpower shortages with cyber campaigns, including distributed denial-of-service (DDoS) attacks and coordinated hacks on military and private-sector targets

Super Bowl LIX Event Assessment

Super Bowl LIX is scheduled to take place on February 9, 2025, at the Caesars Superdome in New Orleans, Louisiana. The Super Bowl will kick off at 6:30 PM (EST), with Fox broadcasting the game and streaming available via Fubo TV. International viewers can also access the game through Dazn and other streaming services. The halftime show, lasting between 12 to 15 minutes, will feature Grammy-winning hip hop artist Kendrick Lamar. New Orleans suffered a violent terrorist attack on New Year's Day, and the city is expected to have heightened security for attendees and visitors from February 5-9, 2025. Given the Super Bowl's global prominence, it is very likely that threat actors will exploit the event's popularity to conduct financial scams or attempt to steal personal information. Fans attending the game in person or watching remotely will face a range of fraudulent schemes, such as ticketing scams, phishing websites, payment-related fraud, betting-related schemes, counterfeit merchandise, accommodations fraud, and transportation or parking scams.

ZeroFox Intelligence Brief – Underground Economist: Volume 5, Issue 2

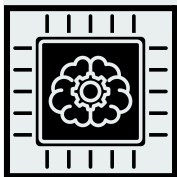
The Underground Economist is an intelligence-focused series illuminating Dark Web findings in digestible tidbits from our ZeroFox Dark Ops intelligence team.

ZeroFox Intelligence February 2025 Geopolitical Brief

With the exception of short-lived tariffs on Colombia, the Trump administration has refrained from administering new tariffs; however that is likely to change starting on February 1, 2025. Recent developments in artificial intelligence by Chinese company DeepSeek likely increase the possibility of harsher-than-anticipated tariffs on China, while at the same time limiting the possibility of tariffs on other regions. The European Union (EU)'s push to increase the economic competitiveness of its businesses will likely coincide with a sharp reduction in regulations, increased defense spending, and efforts to develop advanced technology that could leave EU businesses vulnerable to cyberattacks. A ceasefire in Lebanon between Israel and Hezbollah looks likely to hold for the foreseeable future, but the ceasefire between Israel and Hamas in Gaza has a roughly equal chance of collapsing. Ukraine is likely to have trouble obtaining economic and military support in the coming months as the United States pushes for an end to Russia's war in Ukraine and a number of key European allies hold elections. The Democratic Republic of Congo has become increasingly important to global supply chains for clean and advanced technology, but a war in the mineral-producing region is very likely to continue.

| **Cyber and Dark Web Intelligence** |

| Cyber and Dark Web Intelligence Key Findings



DeepSeek: Cyberattack and Data Exposure

What happened: On January 28, Chinese artificial intelligence (AI) platform DeepSeek announced that it was “[temporarily limiting registrations](#)” to ensure continued service amid allegedly large-scale malicious cyberattacks. On January 29, DeepSeek updated its statement, saying it had identified the issue and was in the process of implementing a fix. Researchers also found a massive amount of [sensitive data exposed on the internet](#). The leaked information included over a million lines of data, such as digital software keys and chat logs from users interacting with the company's AI assistant. DeepSeek took down the data within an hour of being notified of the exposure.

- **What this means:** Though DeepSeek has yet to share details, the recent attacks it faced were likely distributed denial-of-service (DDoS) attacks that targeted the platform's API and web chat services. Researchers have reported that DeepSeek's technology is more vulnerable than other popular AI platforms, making it an easy target for exploitation, especially since its download numbers have surged. DeepSeek has quickly gained popularity, with downloads now surpassing those of ChatGPT on the Apple App Store. In addition, DeepSeek reportedly requires [less computing power and fewer chips](#) to train its model than its competitors. Incidents like these emphasize security risks involving AI platforms, including data exposure, malicious software creation, and exploitation for phishing or social engineering. Moreover, researchers have already found ways to [manipulate DeepSeek's model](#) for harmful outputs, such as creating ransomware—potentially enabling aspiring threat actors to leverage the platform's versatility for malicious uses. The DeepSeek crisis also comes closely at the heels of TikTok's brief ban, further contributing to ongoing fears over foreign apps. DeepSeek has created workarounds to avoid U.S. sanctions, but users have already reported several instances of it [censoring content](#) relating to China. The AI tool collects and sends user data, including chat messages, to servers in China. DeepSeek's privacy policy states that data is stored on secure servers in China and outlines the types of data collected.



New Smishing Campaign Targets USPS Customers with Phishing PDFs

What happened: A new phishing campaign has emerged in which attackers impersonate the U.S. Postal Service (USPS) to trick people into revealing sensitive personal and financial information. The attackers use SMS messages that claim a package cannot be delivered due to "incomplete address information." These messages then direct recipients to click on a PDF file that contains a malicious phishing link. When opened, the link leads to a fake landing page that asks users to enter personal details such as their name, address, email, and phone number. It further redirects victims to a page asking for payment-card information, claiming it is necessary for completing the delivery.

- **What this means:** This appears to be a large-scale phishing campaign; researchers have discovered over 630 phishing pages and 20 malicious PDFs, which could lead to identity theft, stolen financial data, and privacy violations for anyone who clicks the malicious links. By using PDF files, attackers are exploiting a common misconception that they are safe to open. This tactic also makes it more difficult for automated security systems to flag the malicious activity, allowing the attackers to reach a broader pool of potential victims. Additionally, by using SMS as the delivery method, attackers exploit people's tendency to trust messages from seemingly legitimate sources like USPS, increasing the likelihood that the attack will succeed.



Fraud Ring Members Charged in Multi-Million Dollar BEC and Money Laundering Scheme

What happened: The U.S. Department of Justice charged members of a global fraud ring with creating and using more than 1,000 fake businesses to open bank accounts, steal money through business email scams, and launder the funds. The ring caused over USD 60 million in losses and attempted to steal over USD 150 million. The members accomplished this primarily by wiring stolen money to banks in China, outside the reach of U.S. banks.

- **What this means:** In a business email compromise scheme, a threat actor fraudulently persuades a company or individual to send money to a bank account controlled by the scammer. The members of this fraud ring caused significant financial losses and targeted major organizations, city governments, and businesses. They leveraged the international

banking system to launder the stolen money by wiring it to Chinese banks, bypassing U.S. authorities and preventing victims from recovering their losses. Such fraud campaigns could cause critical disruptions in financial business transactions and essential services, leading to loss of public trust and damage to brand reputation.

| **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, and critical infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA) recently [released](#) eight Industrial Control Systems advisories. [CVE-2024-8884](#) involves the exposure of sensitive information to an unauthorized actor, a vulnerability that could cause exposure of credentials when an attacker has access to an application on a network over HTTP. [Three critical vulnerabilities](#) in the open-source PHP package Voyager allow attackers to achieve remote code execution (RCE), exploit JavaScript injection, and manipulate file paths on affected Laravel applications. One of the vulnerabilities ([CVE-2024-55417](#)) allows attackers to bypass MIME-type verification in Voyager's media upload feature, enabling RCE by uploading polyglot files disguised as images or videos. For some Brave browser versions, [CVE-2025-23086](#) could allow a malicious site to initiate a download whose origin in the file select dialog appears as the trusted site that initiated the redirect. In the SMA1000 Appliance Management Console and Central Management Console, [CVE-2025-23006](#) could likely enable a remote unauthenticated attacker to execute arbitrary OS commands. CISA added this to its [Known Exploited Vulnerabilities \(KEV\)](#) Catalog.



CRITICAL

CVE-2025-22604

What happened: A critical security vulnerability has been discovered in the Cacti open-source network monitoring and fault management framework. This flaw allows an authenticated attacker, with device management permissions, to execute arbitrary code on vulnerable instances of the software. Successful exploitation of this vulnerability could enable the attacker to take control of the server, leading to potential theft, modification, or deletion of sensitive data. The issue has been addressed in Cacti version 1.2.29.

- **What this means:** If exploited, this flaw could give attackers privileged access to sensitive systems, thus compromising the confidentiality and availability of critical data. While the vulnerability requires authentication, meaning attackers would need some level of access to the system, its potential for abuse is high, especially in environments where device management permissions are widely distributed. Users are urged to update to the latest version to mitigate the risk of an RCE attack.
- **Affected products:**
 - Affects all versions up to and including 1.2.28.

**CRITICAL****CVE-2024-12248**

What happened: Contec Medical Systems' Contec CMS8000 monitors are infected with CVE-2024-12248 and two other bugs (CVE-2025-0626 and CVE-2025-0683). CVE-2024-12248 is an out-of-bounds write vulnerability, which could enable an attacker to send specially formatted User Datagram Protocol (UDP) requests in order to write arbitrary data. This could result in RCE.

- **What this means:** Successful exploitation of the three vulnerabilities could allow an attacker to remotely send specially formatted UDP requests or connect to an unknown external network that would allow them to write arbitrary data, resulting in RCE. The device may also leak patient information and sensor data to the same unknown external network. Simultaneous exploitation of all vulnerable devices on a shared network is possible. The Food and Drug Administration (FDA) has released a [safety communication](#) in connection with these vulnerabilities. CISA has released an additional [Fact Sheet](#) for CVE-2025-0626 and CVE-2025-0683.
- **Affected products:**
 - CMS8000 Patient Monitor: Firmware version smart3250-2.6.27-wlan2.1.7.cramfs
 - CMS8000 Patient Monitor: Firmware version CMS7.820.075.08/0.74(0.75)
 - CMS8000 Patient Monitor: Firmware version CMS7.820.120.01/0.93(0.95)
 - CMS8000 Patient Monitor: All versions (CVE-2025-0626, CVE-2025-0683)

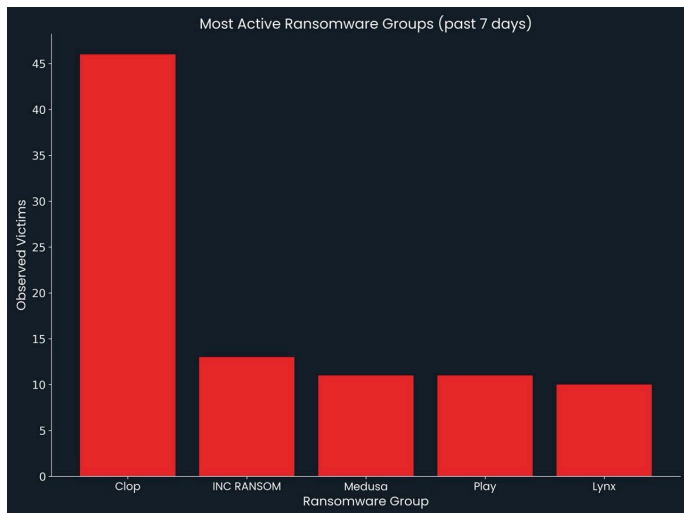
Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings



CI0p Reveals Second Victim List; Ransomware Hits Healthcare and ESXi This Week

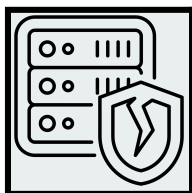
What happened: In the past week, ZeroFox observed over 150 ransomware attacks, most of which were detected in North America. The most affected sector was manufacturing, followed by retail, while the most active ransomware group was CI0p. ZeroFox has observed that Russia-based ransomware collective CI0p has disclosed its [second victim list](#), which likely is a continuation of their exploitation of the Cleo vulnerability. Last week, the group also alluded to possessing data from companies that use Progress MOVEit. In a [statement released on January 29](#), the New York Blood Center (NYBC) disclosed that a [ransomware attack](#) disrupted its operations and forced it to reschedule blood donor appointments. The organization discovered suspicious activity on its IT systems and engaged cybersecurity experts to contain the threat. Meanwhile, cybersecurity researchers have discovered that [ransomware attacks targeting ESXi systems](#) are not only encrypting data but also exploiting compromised appliances to create covert channels for communication. These threat actors are using the ESXi systems to tunnel traffic to their command-and-control (C2) infrastructure, allowing them to maintain control while evading detection. By adopting “living-off-the-land” techniques, they utilize native tools, like Secure Shell (SSH), to establish a SOCKS tunnel, which helps them bypass security measures and stay under the radar.



Source: ZeroFox Internal Collections

- **What this means:** This disclosure by CI0p builds on a [previous announcement](#) made on January 22, 2025, when the group revealed it had compromised 50 more organizations. ZeroFox is unable to independently verify whether these victims were affected through the MOVEit exploit or the Cleo exploit. The release of this updated list of victims could lead to major disruptions for the impacted organizations, many of which may have already been

targeted by other ransomware groups. Given NYBC's critical role in the U.S. healthcare system—collecting nearly 4,000 blood units daily to support over 75 million people—the ransomware attack is likely to disrupt vital services, potentially affecting numerous patients who depend on the center for care. The attack has resulted in canceled appointments and blood drives, which could worsen the already strained blood supply, delaying essential treatments and hindering hospitals' ability to address urgent patient needs. While the full extent of the attack is still being investigated, it is likely that attackers have stolen personal and health data, raising additional concerns—particularly if the information is used for extortion purposes. The incident of ransomware attacks targeting ESXi systems shows how ransomware actors use compromised systems—not only as targets for encryption but also as vehicles for stealthy communication with their C2 infrastructure. The use of native tools and the creation of a tunnel through SSH or equivalent methods minimizes the chances of detection by traditional security systems, making it harder for defenders to track and shut down malicious activity. By utilizing ESXi systems for this purpose, attackers can blend their actions within the normal operational traffic of the environment. Once attackers gain access—either through stolen admin credentials or by exploiting known vulnerabilities—they can establish persistent, undetected communication channels that enable ongoing control over the compromised environment. This increases the risk of long-term disruption, data exfiltration, and further compromise. Additionally, it complicates incident response efforts, as defenders may struggle to identify the malicious tunnel traffic amidst legitimate system communications.



Data Breaches and Their Impacts on Several Entities

What happened: PowerSchool has begun [notifying affected individuals](#) about a late December 2024 that exposed personal data from over 6,500 school districts. While the company is sending notifications and offering identity theft protection, it has yet to disclose the total number of individuals impacted or provide a detailed investigation report. Graphics tablet maker Wacom has notified customers that their [credit card details were likely stolen](#) between November 28, 2024, and January 8, 2025, due to a security vulnerability (CVE-2024-34102) on its website. Meanwhile, Russian cyber efforts to target adversarial states continue to make headlines. The European Union (EU) has sanctioned three hackers from General Staff of the Armed Forces of the Russian Federation (GRU) Unit 29155 for [2020 cyberattacks on Estonian government agencies](#) that resulted

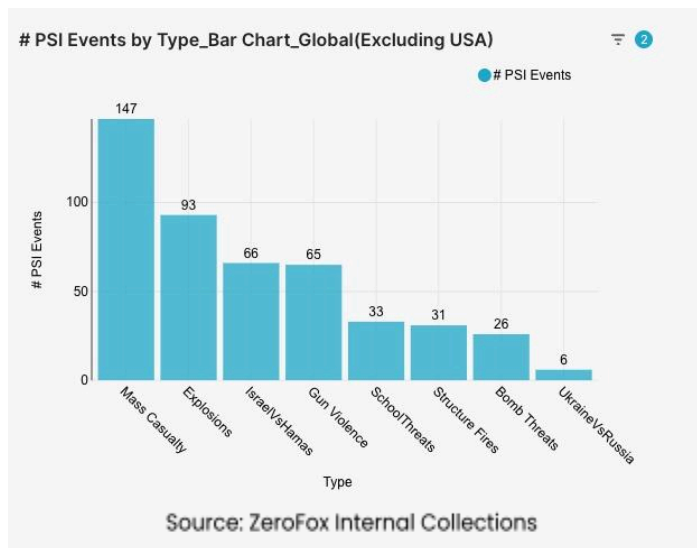
in the [theft of sensitive documents](#) from several ministries. Cybersecurity researchers have discovered a prolonged espionage campaign by the [Russia-linked APT group UAC-0063](#) targeting high-value organizations across Central Asia and Europe. The group employs various malware strains, including HATVIBE and custom-built tools, to penetrate networks and sustain long-term access.

- **What this means:** The PowerSchool breach is another example of how threat actors often leverage third-party customer support portals to exfiltrate sensitive data of institutions with large user bases. Without a clear scope of the impact of the breach, mitigation efforts are likely to be difficult. The Wacom data breach will likely lead to heightened scrutiny of financial transactions and potential exposure to fraud. Unit 29155 conducts cyberattacks on EU nations and Russian adversaries, like Ukraine, aiming to destabilize governments and spread disinformation. By targeting key ministries, threat actors likely seek to disrupt state functions and steal sensitive data. The stolen documents are also likely to be sold on the black market or used in further cyberattacks, such as phishing campaigns or espionage operations. On the other hand, UAC-0063 spreads malware via malicious documents, targeting government, diplomatic, and private sectors. It uses scheduled tasks for persistence and victim exploitation to expand its reach and increase breach success. Both the Unit 29155 and the UAC-0063 attacks are likely part of Russia's efforts to destabilize nations that politically oppose it via cyber warfare instead of military campaigns.

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

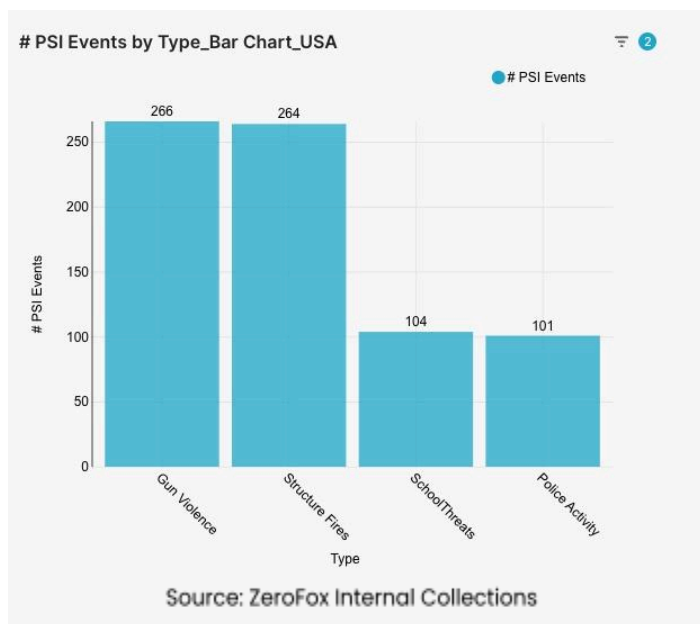


What happened: Excluding the United States, there was a 4 percent increase in mass casualty events this week from the previous week, with the top contributing countries being Lebanon, Israel, and Palestine, in that order. Approximately 63 percent of these events were explosions. General alerts related to the Israel-Hamas conflict (including protests, raids, and involvement in neighboring countries) decreased by 19 percent from the previous week. Events related to the Russia-Ukraine war decreased by 54 percent. The top three

most-alerted subtypes were explosions, which saw an 11 percent decrease from the previous week; gun violence, which decreased by 23 percent; and structure fires, which decreased by 37 percent. Global protest activity decreased by 3 percent. Notably, bomb threats increased by 86 percent, and school-related threats increased by 44 percent.

- **What this means:** Typically, explosions and mass casualty events have a positive correlation, but this week explosions decreased with mass casualty events increasing; this is because bomb threats, which showed a very significant increase, accounted for a larger number of mass casualty events than previous weeks. [India](#) had the highest number of bomb threats this week, with several schools across the country receiving [hoax](#) threats. Explosions as well as events related to the Israel-Hamas conflict both decreased, likely due to the continued [ceasefire](#) which has allowed several hostages on both sides to be released and Palestinians to return to their homes in Gaza. Notably, the United States transferred 90 Patriot air defense interceptors from Israel to Poland this week for delivery to [Ukraine](#). Russia continues to make advances in Eastern Ukraine, as Ukrainian forces continue to hold on to territory in Russia's western [Kursk](#) region.

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 two states that reported the most gun violence alerts were California and Illinois, which together made up 22 percent of this week's nationwide total. Gun violence

across the United States overall increased by 13 percent from the week prior. Police activity alerts increased by 44 percent; the top contributing states were California and Texas. Structure fires increased by 14 percent; the top two states for this subtype were California and New York. Notably, national protest activity increased by 49 percent, and school-related incidents increased by 28 percent.

- **What this means:** The top three subtypes saw increases this week compared to last. In California, the Hughes, Eaton, and Palisades wildfires have been mostly [contained](#), as Los Angeles recently experienced heavy rain and cooler temperatures. Both police activity and school-related threats saw increases this week. Two high schools in the [Athens](#) neighborhood of Los Angeles were placed on lockdown on January 22, as deputies responded to a bomb threat which was later lifted. Across the country, Immigration and Customs Enforcement (ICE) [raids](#) have begun as part of President Donald Trump's executive orders, with three major U.S. cities being targeted per week as per the crackdown plan. As a result, protest activity has emerged in multiple locations.

| 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%