ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

June 27, 2026

Scope Note

ZeroFox's Weekly Intelligence Briefing highlights the major developments and trends across the threat landscape, including digital, cyber, and physical threats. ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 6:00 AM (EDT) on June 25, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Weekly Intelligence Brief

This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Brief - Underground Economist: Volume 6, Issue 13

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

ZeroFox Intelligence Flash Report - DragonForce Conceals C2 in Legitimate Relay Infrastructure

On June 16, 2026, cybersecurity researchers disclosed a December 2025 intrusion at a major U.S. services firm in which operators from the DragonForce ransomware collective deployed a custom backdoor called Backdoor.Turn into the firm's enterprise collaboration infrastructure. Backdoor.Turn is a previously unseen in the wild Go-based remote access trojan (RAT) that can be injected into legitimate trusted collaboration instances to avoid detection. DragonForce almost certainly used this RAT to establish a command-and-control (C2) node within the trusted U.S. services firm's network in order to maintain persistence. ZeroFox assesses that abusing trusted, widely deployed collaboration services for C2, exfiltration, and malware delivery is very likely a tradecraft trend that has evolved since at least mid-2025. This likely represents a further maturation of the ransomware-as-a-service (RaaS) ecosystem, which almost certainly increases detection difficulties for defenders relying primarily on network egress monitoring. This type of intrusion also likely represents a continuing shift from single-event extortion toward dual monetization: initial encryption and data theft followed by durable access that can be exploited later or sold to other criminal operators on deep and dark web (DDW) forums.

ZEROFOX

Weekly Intelligence Brief

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

Dify Issues Fixes for Four Flaws Affecting AI Application Security

What we know:

- Four vulnerabilities in the open-source artificial intelligence (AI) platform Dify have been found to potentially enable threat actors to access sensitive AI application data, including chat histories, uploaded documents, and user files.
- The flaws have been patched in Dify v1.14.2.

Background:

- The four vulnerabilities are tracked as CVE-2026-41947, CVE-2026-41948, CVE-2026-41949, and CVE-2026-41950.
- Dify is reportedly widely deployed, with more than 10 million Docker image downloads and thousands of internet-facing instances.

Analyst note:

- Given the role of AI platforms in managing internal organizational knowledge and business data, successful exploitation of the flaws is likely to enable long-term intelligence collection by providing sustained visibility into organizational processes and data flows.

Brazil's Defense Alert System Reportedly Hacked

What we know:

- Brazil's National Civil Defense has reported a suspected hacking of its official alert system after mass alerts containing the word "misanthropy" were sent to cell phones across multiple Brazilian states.

Background:

- The attacker reportedly deactivated the platform and then maliciously reactivated it to send notifications on behalf of "someone outside the National System of Civil Protection and Defense."

Analyst note:

- The attack was likely designed to demonstrate capability.

- Similar operations are likely to be leveraged to amplify social unrest, disrupt emergency response systems, and erode confidence in government institutions.

Authorities Seize Servers and Credentials Linked to Amadey and StealC Malware Strains

What we know:

- Europol and partners have disrupted Amadey and StealC malware operations' infrastructure as part of Operation Endgame.
- The operation took down over 326 servers and disrupted C2 infrastructure, leading to the recovery of approximately 27 million stolen credentials from over 300,000 systems.

Background:

- StealC is an information-stealing malware strain that extracts credentials and other sensitive data, while Amadey is a loader that delivers additional malware and steals sensitive information from compromised systems.

Analyst note:

- Following the takedown, cybercriminals relying on StealC and Amadey are likely to lose access to stolen assets harvested through these malware strains.
- This is likely to disrupt initial access opportunities required for further attacks. Consequently, an increased demand for alternative infostealers and access services is likely on DDW marketplaces.

Exploit and Vulnerability Intelligence

Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in technology, software development, and critical infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA) added four vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue on June 23, 2026. Additionally, on June 23, 2026, CISA released seven Industrial Control Systems (ICS) advisories, including CVE-2026-1840, CVE-2026-31431, and CVE-2026-46746. Two vulnerabilities (CVE-2026-57283 and CVE-2026-57284) were disclosed in the Pipeline: Groovy Plugin for Jenkins. The flaws affect versions 4331.v9d06ed4658ff and earlier and could enable attackers to abuse the Pipeline Snippet Generator to create unauthorized script approval requests. Microsoft has reportedly patched a vulnerability chain dubbed "AutoJack" affecting AutoGen Studio interface. The flaw reportedly helps manipulate an AI agent into executing arbitrary code on the host system by visiting a malicious webpage. Technology company F5 has released patches for multiple NGINX vulnerabilities, including two flaws (CVE-2026-42530 and CVE-2026-42055) that could enable attackers to cause denial-of-service (DoS) conditions. CVE-2026-47729, dubbed as Squidbleed, is a heap over-read vulnerability in the widely used Squid web proxy that can enable an authorized proxy user to obtain portions of another user's HTTP requests, including credentials, session tokens, and other sensitive data.

HIGH

CVE-2026-8461

What happened: An out-of-bounds write vulnerability (CVE-2026-8461) in FFmpeg's libavcodec library in the MagicYUV decoder enables DoS conditions and, in some cases, can reportedly be exploited for remote code execution (RCE).

- **What this means:** The flaw arises from improper handling of chroma plane heights during video decoding and can allow attackers to trigger a crash or achieve RCE by supplying a specially crafted video file. The exploit can be delivered in common media formats such as AVI, MKV, and MOV and requires only that the target application processes the file.

  Affected products: FFmpeg versions before 8.1.2

CRITICAL

CVE-2025-67038

What happened: Threat actors are actively exploiting CVE-2025-67038, a critical command injection vulnerability affecting Lantronix EDS5000 Series devices. The flaw reportedly enables attackers to inject operating system commands through an unsanitized username parameter, potentially resulting in arbitrary command execution with root privileges.

- **What this means:** Successful exploitation of the Lantronix flaw could enable attackers to fully compromise affected devices and establish a foothold within targeted networks.

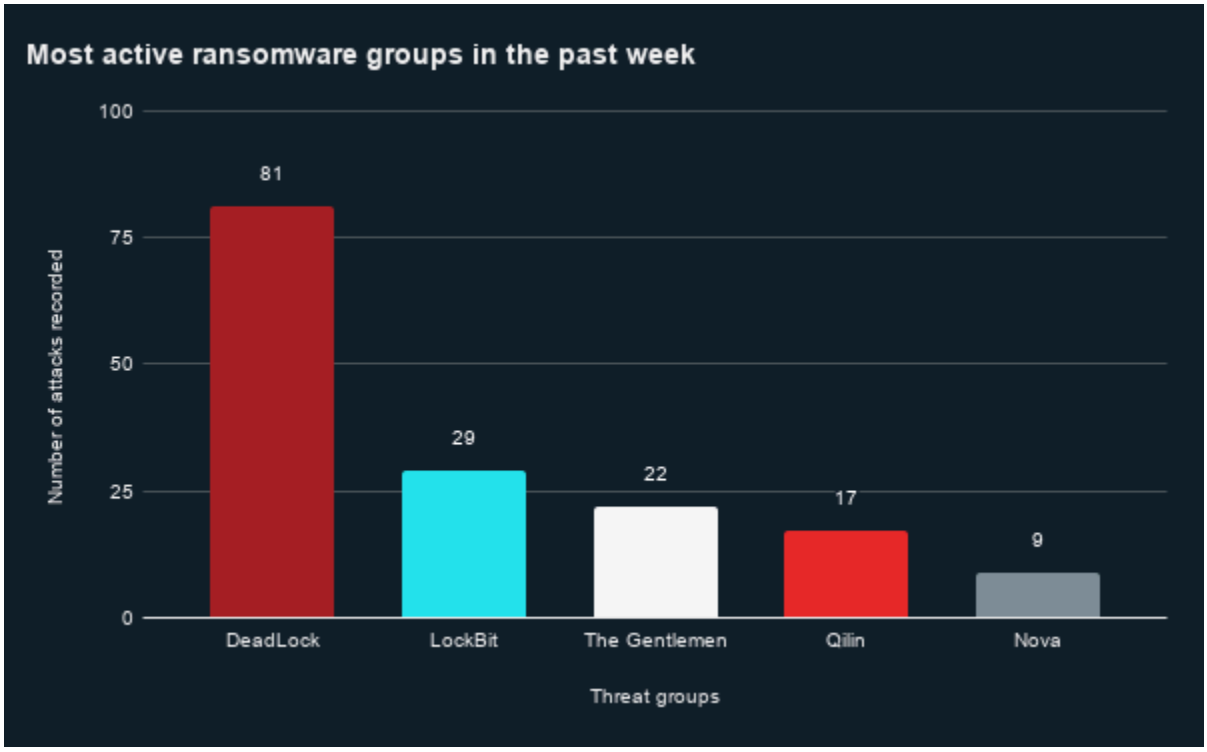
Affected products: Lantronix EDS5000 2.1.0.0R3

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

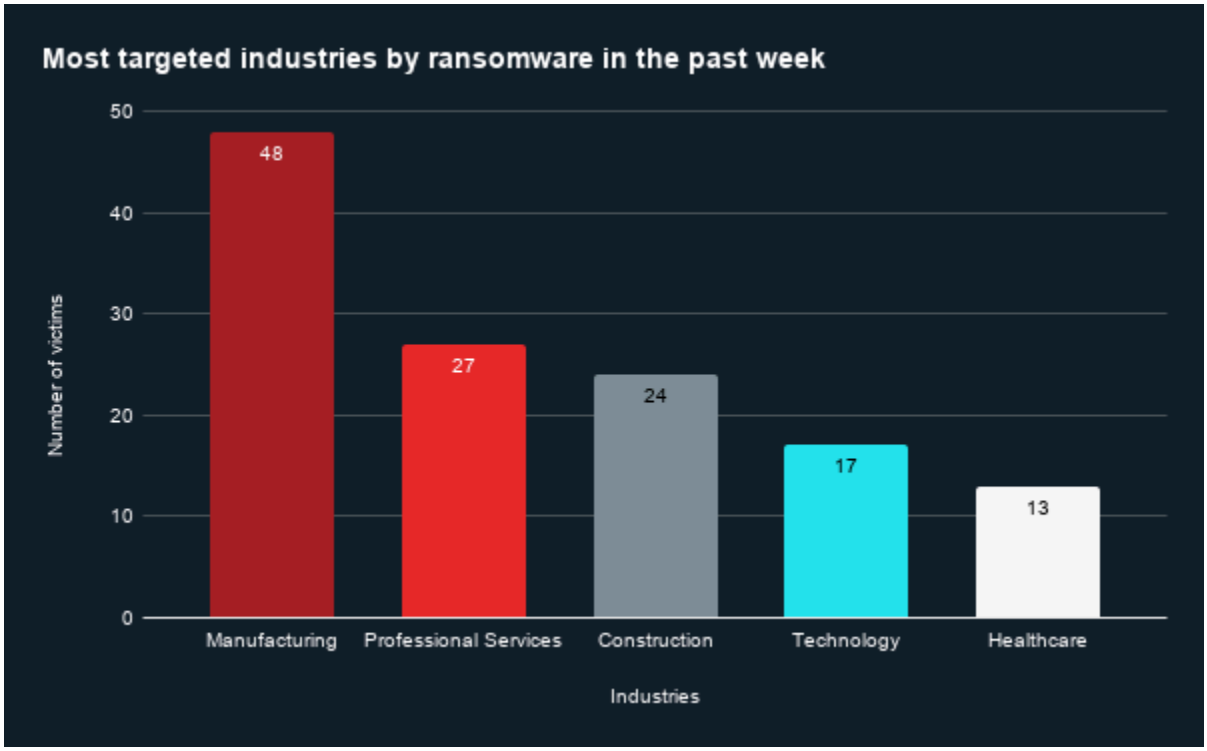
Ransomware Group, Industry, and Regional Trends

Last week in ransomware: In the past week, DeadLock, LockBit, The Gentlemen, Qilin, and Nova were the most active ransomware groups. ZeroFox observed close to 214 ransomware victims disclosed, most of whom were located in Europe and Russia. The DeadLock ransomware group accounted for the largest number of attacks, followed by LockBit.



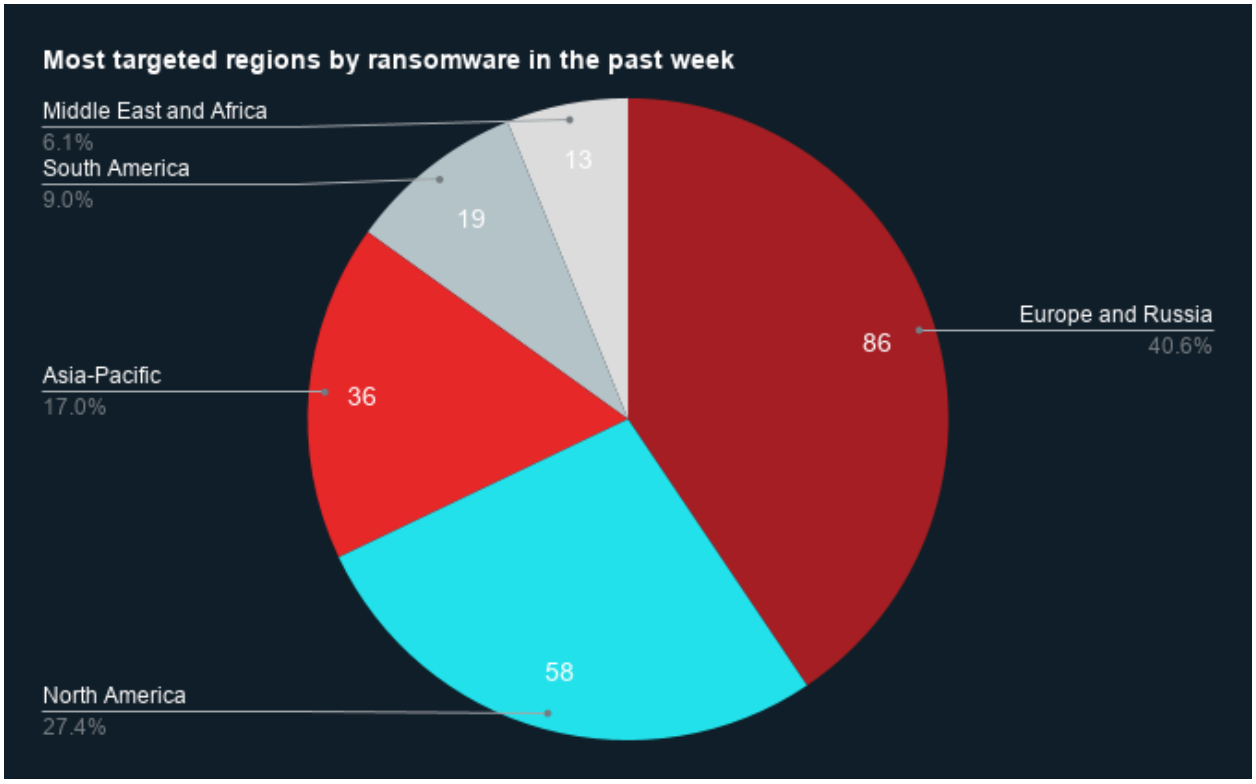
Source: ZeroFox Internal Collections

Industry ransomware trends: In the past week, ZeroFox observed that manufacturing was the industry most targeted by ransomware attacks, followed by professional services.



Source: ZeroFox Internal Collections

Regional ransomware trends: Over the past seven days, ZeroFox observed that Europe and Russia was the region most targeted by ransomware attacks, followed by North America and Asia-Pacific. There were at least 86 ransomware attacks observed in Europe and Russia, while North America accounted for 58, Asia-Pacific for 36, South America for 19, and Middle East and Africa for 13.



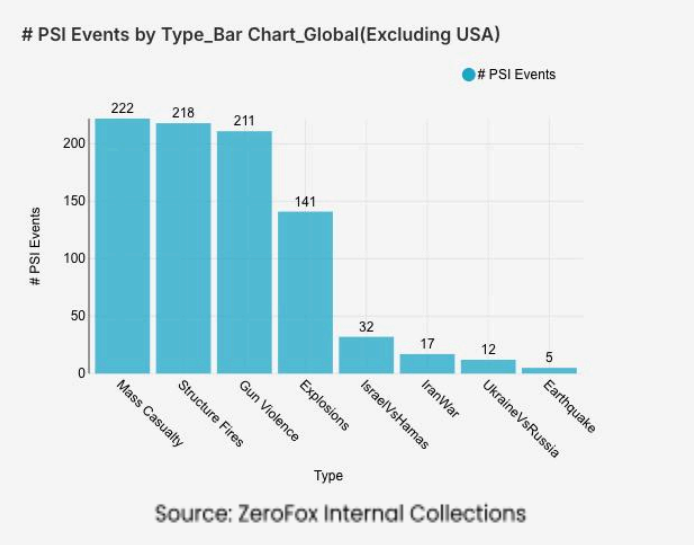
Source: ZeroFox Internal Collections

Significant Data Breaches Reported Over the Week

Targeted Entity	Klue	London Hydro	Tata Electronics
Compromised Entities/Victims	Klue customers using Salesforce integration	London Hydro's customers	Tata Electronics and customers (including Apple and Tesla)
Compromised Data Fields	Customer Relationship Management (CRM)-related data, including business contacts, sales communications, price quotes, competitive intelligence reports, and account data	Names, addresses, email addresses, phone numbers, account and billing numbers, service addresses, pricing plans, contract dates, and meter numbers and types	630 GB of data, comprising over 200,000 files of Outlook email conversations, SAP-related data, Apple supplier specifications, and Tesla manufacturing documents
Suspected Threat Actor	Icarus	N/A	N/A
Country/Region	North America	City of London, Ontario, Canada	India
Industry	Technology	Energy	Manufacturing
Possible Repercussions	Extortion attempts and further intrusion attempts via third-party software-as-a-service (SaaS) integrations using access tokens	Phishing and smishing campaigns impersonating London Hydro, as well as utility frauds	Significant supply chain risk to technology ecosystems; competitive corporate entities or nation-state actors will likely be interested in the stolen data

Three major breaches observed in the past week

Physical and Geopolitical Intelligence Key Findings

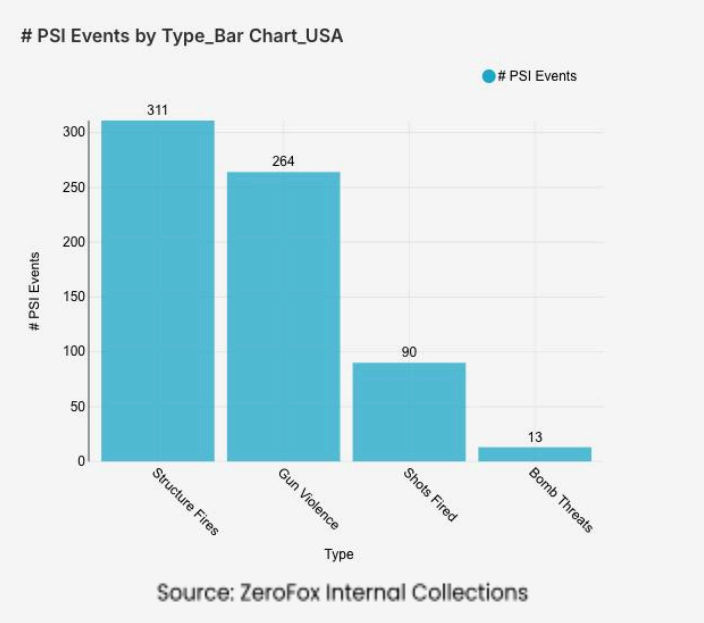


Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 1 percent decrease in mass casualty events this week from the previous week, with the top contributing countries or territories being India, Lebanon, and Mexico, in that order. Approximately 64 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 27 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict decreased by 11 percent from the previous week, and alerts related to the war in Iran increased by 21 percent. Events related to Russia's war in Ukraine increased by 50 percent. The top three most-alerted subtypes were structure fires, which saw a 16 percent decrease from the previous week; gun violence, which increased by 1 percent; and explosions, which increased by 10 percent. Notably, earthquakes increased by 150 percent from the week prior.

- **What this means:** Global mass casualty trends this week reflect an interconnected web of ongoing conflicts and natural disasters that continue to generate alerts worldwide. In India, a fire tore through a building in the city of Lucknow on June 22, killing at least 14 people, adding to a pattern of structure fire and explosion casualties that has made India the leading source of alerts this week. In Lebanon, despite a ceasefire implemented on June 19, there were at least 12 Israeli air raids conducted in the last week, including one on June 20 that killed 16 people and wounded 12 in the Nabatieh district. Russia and Ukraine exchanged fatal strikes on June 22; a Russian drone strike in Sumy killed six people, while a Ukrainian strike on a Russian industrial plant killed five people. The sharp spike in earthquake alerts this week is embodied by events from the past 24 hours: a pair of powerful earthquakes in Venezuela on June 24 killed at least 164 people and injured 971 more, making these the largest earthquakes to hit Venezuela in more than a century. Taken together, this week's data reflects a global physical security environment under significant and multidirectional strain.

Physical Security Intelligence: United States



Source: ZeroFox Internal Collections

What happened: In the past week, the top three most-alerted incident subtypes were structure fires, gun violence, and shots fired. Gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim, shots fired are confirmed shootings with no victims, and structure fires are fires that affect man-made buildings. The top two states with the most gun violence alerts were Illinois and Ohio, which together made up 20 percent of this week's nationwide total. Gun violence across the United States overall increased by 12 percent from the week prior. Shots fired alerts increased by 45 percent, and the top contributing states were Illinois and New York. Structure fires decreased by 4 percent, and the top two states for this subtype were California and New York. Notably, bomb threats increased by 117 percent from the week prior.

- **What this means:** Over the past week, the threat landscape across the United States remained active and varied. A significant illustration of the structure fire trend came from Los Angeles, California, where a blaze ignited on June 17 at a warehouse in the Boyle Heights neighborhood, burning for over a week, triggering shelter-in-place orders, and costing the city approximately USD 3 million in fire department expenses. Gun violence and shots fired continued at an elevated pace across the country; in Chicago, Illinois, the extended Juneteenth holiday weekend saw at least 39 people shot across 24 separate shooting incidents. Bomb threats were among the most notable developments this week, with Arizona being a focal point of this trend; Sierra Vista experienced at least four separate bomb threats within a single week, with the latest occurring on June 24. Authorities noted the calls bore strong similarities to swatting incidents that occurred concurrently in Tucson, suggesting a coordinated or copycat pattern across southern Arizona. Taken together, this week's data reflects a domestic security environment defined by persistent and evolving threats, underscoring the importance of vigilance across both public and private spaces.

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%