ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

September 6, 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 6:00 AM (EDT) on September 4, 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

ZeroFox Intelligence Flash Report: Russian Interference Blamed for Jamming EC President's Plane

The European Commission (EC) publicly blamed Russia for an incident of GPS jamming targeting the plane of EC President Ursula von der Leyen. The incident is likely linked to Russia's aggressive hybrid warfare strategy, which is designed to limit the effectiveness of military aid to Ukraine. While normally reserved for states along Russia's western periphery, Western Europe is likely to see an escalation in attacks as it steps up support for Ukraine. The European Union (EU) remains deeply divided on how to address a variety of issues, and it is in Russia's interest to worsen these divisions.

ZeroFox Intelligence Flash Report - Exploitation of Salesforce Systems Likely to Continue

Beginning around August 8, 2025, and continuing until approximately August 18, 2025, a sophisticated supply chain breach targeting the Drift-Salesforce integration AI chatbot was reportedly carried out by a threat actor leveraging OAuth credentials to exfiltrate Salesforce instance data from multiple companies. Notably, customers who integrate online services with Salesloft's Drift platform (such as Slack, Google Workspace, Amazon S3, Microsoft Azure, and OpenAI) can potentially be impacted by threat actors using the stolen OAuth tokens. ZeroFox assesses that more companies that have utilized the compromised Salesforce integration with Salesloft Drift are likely to be publicly disclosed as victims in the coming weeks.

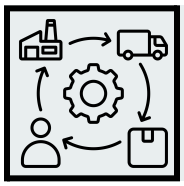
ZeroFox Intelligence Brief - Hacktivism: Tactics, Techniques, and Procedures

Hacktivist collectives are motivated by an array of incentives ranging from perceived persecution to the pursuit of transparency, justice, or systemic reform. Hacktivists are typically politically, socially, or ideologically motivated. Although hacktivists are most often driven by political, social, or ideological motivations—matters that do not usually draw state entities into offensive cyber activity—state-affiliated collectives are aligned with national interests to some extent through a shared ideology, informal coordination, or direct sponsorship. Hacktivists use a variety of methods to achieve their desired end state, which are collectively referred to as their tactics, techniques, and procedures (TTPs). They employ a wide range of TTPs, which can be attributed to disparity in expertise, available resources, risk appetite, and technical knowledge, all of which vary significantly across collectives.

ZEROFOX
Weekly Intelligence Brief

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings



Salesforce Supply Chain Breach Expands: Workiva, Cloudflare, and Zscaler Disclose Impact

What we know:

- Attackers have been exploiting the Salesloft Drift supply chain compromise to access Salesforce-connected systems.
- Workiva, Cloudflare, Palo Alto Networks, PagerDuty, and Zscaler have recently confirmed breaches tied to the incident.
- Stolen data includes OAuth and API tokens; customers' personally identifiable information (PII), such as names, emails, phone numbers, and job titles; and support ticket information ranging from basic contact details to sensitive case text that could expose system or security insights.

Background:

- The incident began with the compromise of Salesloft Drift integrations, which has affected several organizations.
- Attackers leveraged stolen OAuth tokens to infiltrate Salesforce instances of downstream companies.
- Salesforce environments are widely used for customer support, Customer Relationship Management (CRM), and integrations, creating a large attack surface.
- The Salesforce breach has been attributed to the ShinyHunters group, which has previously targeted software-as-a-service (SaaS) and CRM platforms.

What is next:

- In the coming weeks, more Salesforce and Salesloft customers are likely to be affected.
- Attackers are likely to resell stolen CRM datasets on underground forums, which could leave the affected organizations even more vulnerable to further attacks.
- Follow-on attacks mainly targeting customers through phishing and business email compromise (BEC) are very likely, with additional risks of impersonation and stolen OAuth or API token reuse to regain access or pivot into connected SaaS environments.

Threat Actor Claims Live Access to AT&T Database

What we know:

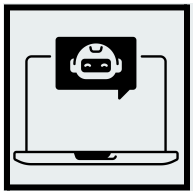
- Threat actor "gorgina" is claiming to sell "live access" to American telecom company AT&T's core infrastructure on LeakBase for USD 100,000 in BTC. The database allegedly contains information of approximately 24 million active subscribers.

Background:

- The threat actor claims to have persistent access, supposedly having evaded detection for over three weeks. A screenshot provided by the threat actor shows several data fields, including phone number, device type, registration date, account status, and last activity date.
- ZeroFox observed that the threat actor joined LeakBase on August 31, 2025, the same day as the post was made.

Analyst note:

- The actor has made sensational claims of leveraging the database to carry out SIM swapping and OTP interception.
- The claim is likely to be false, given the unverified reputation of the threat actor and interactions on the post claiming the data is old.
- Moreover, SIM swapping requires compromising or manipulating an employee of the mobile carrier company, and only access to network infrastructure is unlikely to be adequate.



Cybercriminals Exploit Grok to Spread Malicious Links on X

What we know:

- Cybercriminals are exploiting Grok, X (formerly, Twitter)'s AI assistant to bypass link restrictions by hiding malicious URLs in advertisement metadata.
- To avoid detection, they push out low-quality video advertisements with adult clickbait but deliberately omit direct links in the main body.

Background:

- X's advertisement restrictions were designed to block malicious links. However, attackers hide URLs in the "From:" metadata of video advertisements to bypass the restrictions.

Analyst note:

- Hiding the URLs enabled attackers to effectively turn malicious advertisements into credible promotions.
- Users are very likely to click links echoed by a system account, which could expose them to scams, fake CAPTCHA traps, and information-stealing malware.

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 eight vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on August 29, September 2, September 3, and September 4. CISA also released nine Industrial Control System (ICS) advisories on September 2 and September 4. Google has patched 120 flaws, including two zero-days. Additionally, the company has released an advisory addressing six security fixes for Windows, macOS, and Linux. Threat actors are weaponizing AI-powered red-teaming tool HexStrike-AI to rapidly exploit newly disclosed Citrix flaws such as CVE-2025-7775, enabling faster automation of attacks and reducing defenders' patching window. Click Studios has warned users of an authentication bypass flaw in its Passwordstate enterprise password manager that could enable attackers to access the administration section via a crafted URL. An emergency patch has been released for CVE-2025-57819, which was exploited to breach FreePBX servers exposed to the public internet. The vulnerability enables attackers to access the FreePBX administrator panel. Threat actors are deploying a zero-day exploit for a bug present in CrushFTP. It has been patched in CrushFTP versions v10.8.5 or v11.3.4. Threat actors are exploiting a zero-day vulnerability (CVE-2025-53690) in legacy Sitecore deployments.

MEDIUM

CVE-2025-55177

What happened: WhatsApp has patched a vulnerability in its iOS and Mac apps that enabled zero-click spyware attacks. The flaw was exploited to secretly compromise about 200 targeted users' devices.

- **What this means:** The bug stemmed from incomplete authorization in linked device sync, which, when chained with an Apple image-handling flaw (CVE-2025-43300), enabled silent malware installation. Apple had already patched its part of the chain.
- **Affected products:**
  - WhatsApp Desktop for Mac versions 2.22.25.2 before 2.25.21.78

CRITICAL

CVE-2025-54857

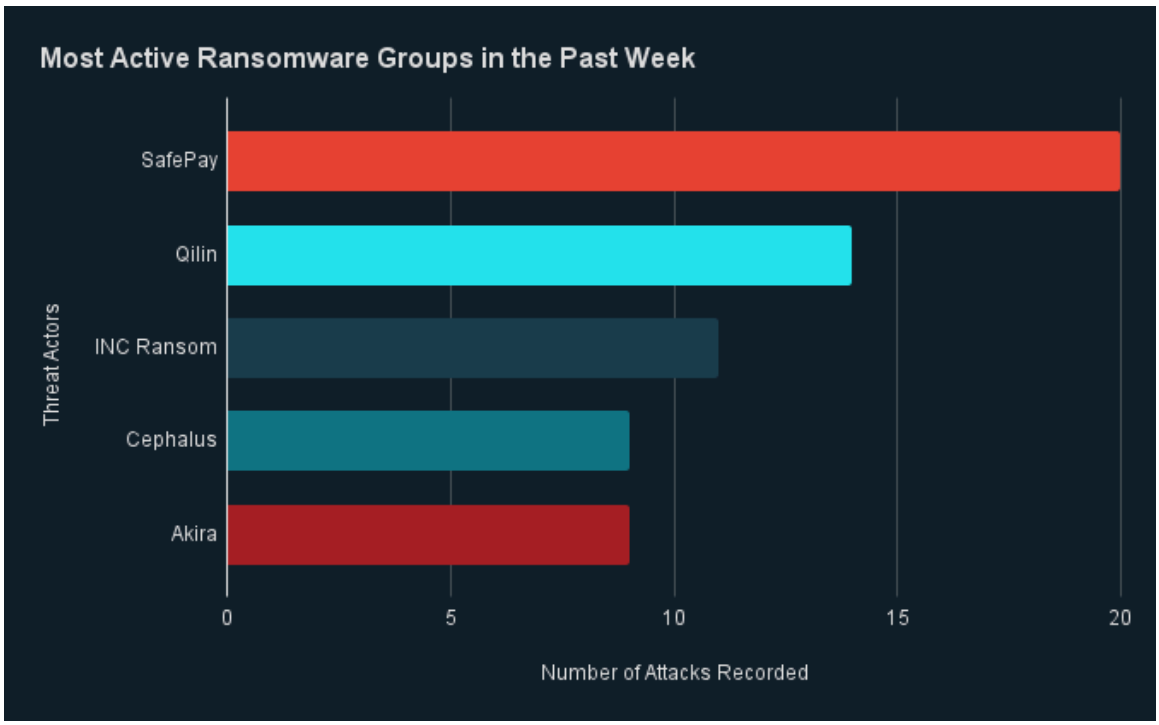
What happened: This vulnerability arises from improper handling of special elements in operating system (OS) commands. It could enable a remote, unauthenticated attacker to execute arbitrary OS commands with root-level privileges.

- **What this means:** Since no authentication is required, successful exploitation could give the attacker complete control of the affected device, leading to data theft, operational disruption, malware installation, or use of the system as a launch point for further attacks.
- **Affected products:**
  - SkyBridge BASIC MB-A130 Ver.1.5.8 and earlier

Ransomware and Breach Intelligence

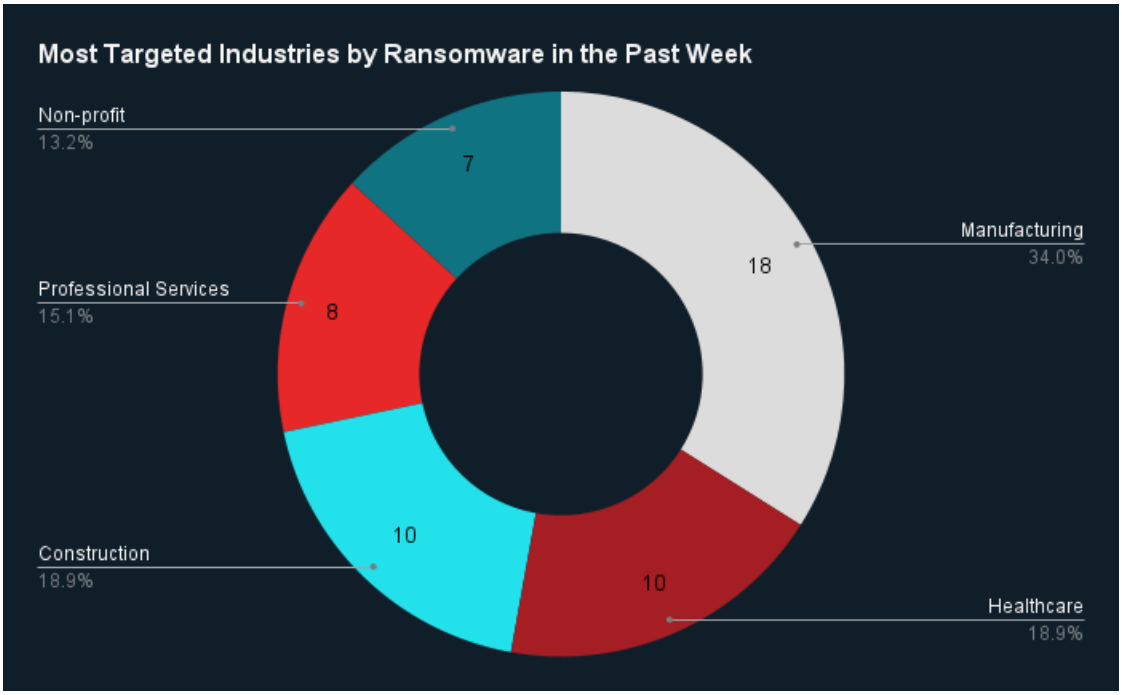
Ransomware and Breach Intelligence Key Findings

Ransomware Roundup: Top Threat Groups, Industries Impacted, and More



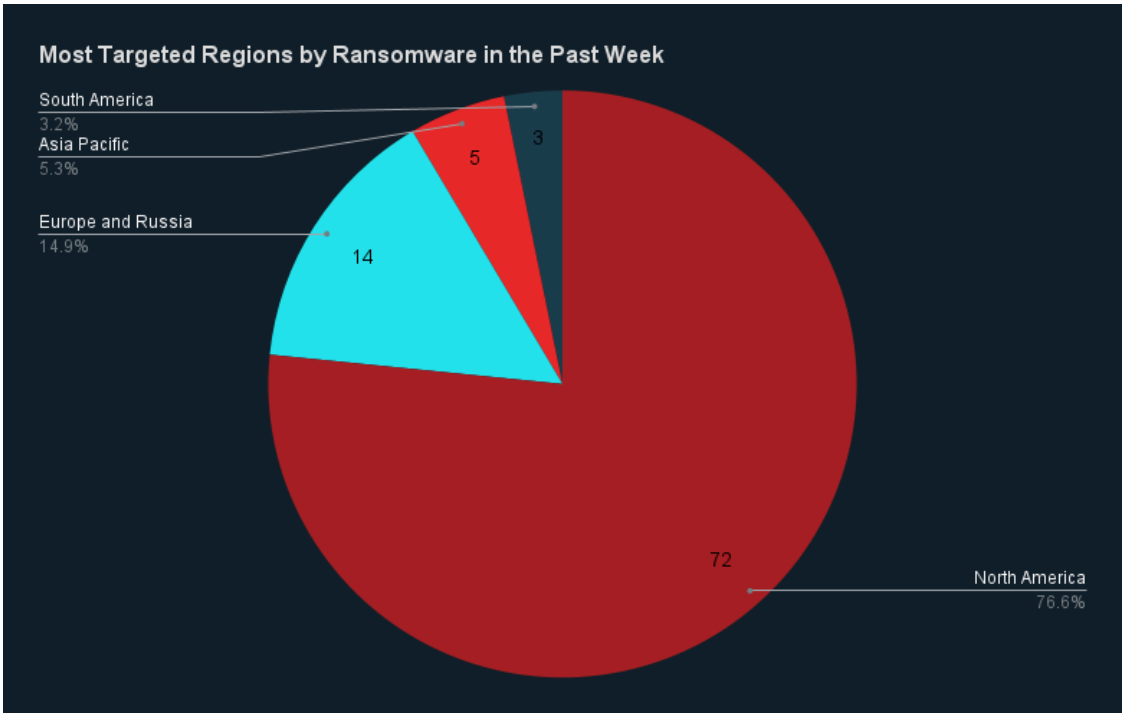
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, SafePay, Qilin, INC Ransom, Cephalus, and Akira were the most active ransomware groups. ZeroFox observed at least 90 ransomware victims disclosed, most of whom were located in North America. The SafePay ransomware group accounted for the largest number of attacks, followed by Qilin.



Source: ZeroFox Internal Collections

Industry ransomware trend: In the past week, ZeroFox observed that manufacturing was the industry most targeted by ransomware attacks, followed by healthcare, construction, professional services, and non-profit.



Source: ZeroFox Internal Collections

Regional ransomware trends: Over the past seven days, ZeroFox observed that North America was the region most targeted by ransomware attacks, followed by Europe-Russia. There were at least 72 ransomware attacks observed in North America, while Europe-Russia accounted for 14, Asia-Pacific (APAC) for five, and South America for three.

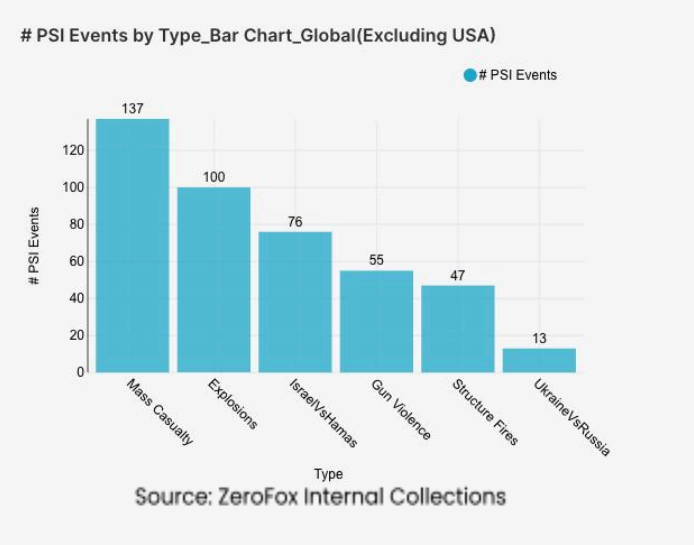
Major Data Breaches Disclosed in the Past Week

Targeted Entity	Nx	Absolute Dental	Lotte Card
Impacted Entities	Over 1,000 JavaScript developers	1.2 million individuals	Estimated 9.65 million customers
Compromised Data Fields	GitHub OAuth keys, personal access tokens (PATs), API keys, AI credentials	PII such as Social Security number (SSN), health information such as insurance information, and financial information such as payment card details	1.7 GB of customer data reportedly involving card information and online payment request details
Suspected Threat Actor	N/A	N/A	N/A
Country/Region	Global	Nevada, United States	South Korea
Industry	Technology	Healthcare	Financial Services
Possible Repercussions	The breach is very likely to create a wider supply chain compromise. Multiple organizations worldwide are likely to be affected.	Exposed individuals are likely to be targeted in phishing, social engineering, and data theft attacks, presenting the risk of financial losses.	Threat actors are likely to use the data to carry out fraudulent transactions.

Three major breaches observed in the past week

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

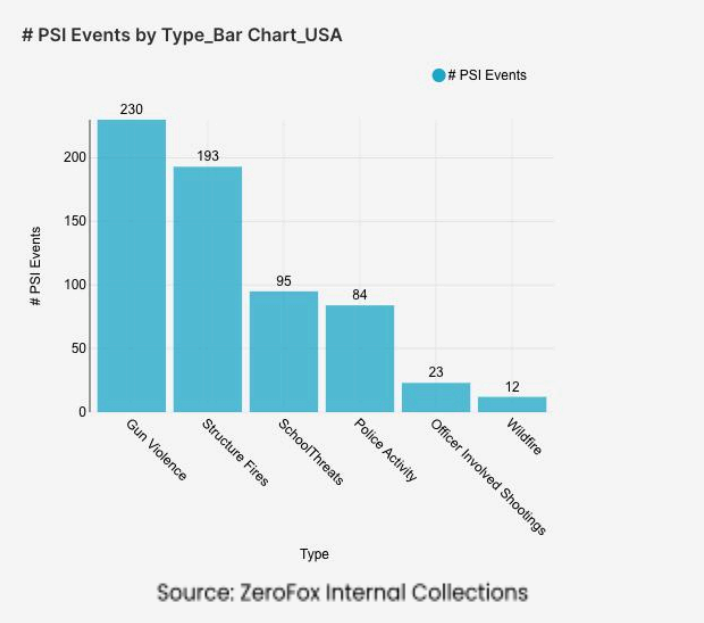


Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 1 percent increase in mass casualty events this week from the previous week, with the top contributing countries or territories being the Palestinian Territories, Pakistan, and India, in that order. Approximately 69 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 35 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict (including protests, raids, and attacks) increased by 20 percent from the previous week. Events related to Russia's war in Ukraine increased by 180 percent. The top three most-alerted subtypes were explosions, which saw a 15 percent increase from the previous week; gun violence, which decreased by 3 percent; and structure fires, which increased by 96 percent. Global protest activity did not show any increase or decrease from the week prior.

- **What this means:** This week has seen several notable escalations across various world conflicts, with the Palestinian Territories having the highest number of mass casualty incidents. The increase in alerts related to the Israel-Hamas conflict can be attributed to several instances; for example, on September 4, Israeli forces were reported to have killed at least 54 people in Gaza with attacks on residential areas and aid distribution points. Pakistan, which also had a notable amount of mass casualty instances this week, saw at least 11 people killed in what is suspected to be a suicide bombing targeting a political rally in Quetta on September 2. The Ukraine-Russia conflict escalated significantly this week as well, as Russia launched a sweeping air attack on Ukraine on September 3 that injured at least four people and damaged critical infrastructure; this occurred as Russian President Vladimir Putin attended a military parade marking the end of WWII in Beijing, where Chinese President Xi Jinping warned that the world faced a choice between peace and war. All of these aforementioned events have contributed to the overall rise in explosions and mass casualty alerts and highlight the volatility of global physical security.

Physical Security Intelligence: United States



Source: ZeroFox Internal Collections

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, structure fires are fires that affect man-made buildings, and police activity involves law enforcement presence for generalized threats or for unknown reasons. The top two states with the most gun violence alerts were Illinois and Pennsylvania, which together made up 30 percent of this week's nationwide total. Gun violence across the United States overall increased by 3 percent from the week prior. Structure fires increased by 9 percent, and the top two states for this subtype were California and New York. Police activity alerts increased by 13 percent, and the top contributing states were California and Pennsylvania. Notably, officer-involved shootings increased by 21 percent.

- **What this means:** This week, crime and other incidents in the nation have been on the rise in several key areas, partly due to Labor Day weekend; for instance, between August 29 and September 1, Chicago, Illinois alone saw 58 people shot in 37 separate shootings. As a response, U.S. President Donald Trump has threatened to deploy national guard troops to the city, similarly to what has been done in Washington, D.C. to combat crime, illegal immigration, and homelessness. This, along with other local law enforcement efforts to combat violence over the holiday weekend, may explain the rise in police activity overall. Officer-involved shootings also saw a significant increase, with one such instance in Phoenix, Arizona that resulted in two officers shot and three suspects injured on September 2. Finally, structure fires rose as well, with California and New York being the most affected states. In California, wildfires that are part of the TCU September Lightning Complex have burned homes and other structures in the historic Gold Rush town of Chinese Camp. The data on the aforementioned subtypes—along with the recent examples in various states—illustrates the persistent public safety challenges facing the United States.

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%