



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

June 10, 2024

Scope Note

ZeroFox's Weekly Intelligence Briefing highlights the major developments and trends across the cyber threat landscape. 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 (EDT) on June 7, 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 Flash Report – Advertised Malicious Tool Targets Gmail Accounts	2
ZeroFox Intelligence Brief – EU Parliamentary Elections Present Cyber and Physical Threats	2
 Cyber Intelligence Key Findings	4
Russia Amps up Efforts to Disrupt Paris Olympics with Disinformation	4
Hackers Exploit TikTok Zero-Day to Break into CNN Account	4
Chinese State-Backed Cyber Espionage Targets Southeast Asian Government	5
 Deep and Dark Web Intelligence Key Findings	7
Threat Actor Advertises New Multi-Threaded Brute Force Tool	7
Threat Actor Advertised Several Exploits	7
Threat Actor Group Conducts Cyberattack Against UAE Government	8
 Exploit and Vulnerability Intelligence Key Findings	10
CVE-2018-20062 and CVE-2019-9082	10
CVE-2017-3506	11
 Ransomware and Breach Intelligence Key Findings	13
Ransomware Intelligence: London Hospitals Cancel Operations Following Critical Ransomware Incident at Synnovis	13
Breach Intelligence: Data Breach at Australian Rare-Earth Mining and Exploration Company	14
 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	19
 Appendix B: ZeroFox Intelligence Probability Scale	20

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Flash Report – Advertised Malicious Tool Targets Gmail Accounts

On May 20, 2024, untested actor “Plifal” announced a new malicious tool named Plifal Software on the Russian-speaking dark web forum Exploit. The tool allegedly bypasses Google application programming interfaces (APIs) and policies, enabling threat actors to exploit session cookies and illicitly access Gmail user accounts. The advertisement garnered positive feedback from the Exploit community. On June 1, 2024, actor “vasiliev84” claimed that the software had operated as expected, stating that the product is a “game changer” and recommending it to fellow threat actors. While the advertisement offers no further detail surrounding the capabilities of Plifal Software, illicit access to an individual or business Gmail account can enable a threat actor to conduct a myriad of malicious activities. Software tools targeting widespread and diverse software solutions that are becoming increasingly prominent in the workplace are almost certainly a coveted target for threat actors seeking to gain illicit access and conduct subsequent malicious activity.

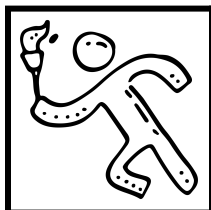
ZeroFox Intelligence Brief – EU Parliamentary Elections Present Cyber and Physical Threats

The European Union (EU) will hold a transnational parliamentary election from June 6–9, with results expected by the end of the last day of voting. The EU parliament writes legislation and oversees the bloc’s annual budget, which totaled EUR 185.6 billion in 2023. It also approves candidates for some of the top positions within the wider EU bureaucracy, such as President of the European Commission. Due to sluggish post-pandemic economic growth and concerns over security, Eurosceptic parties (those opposed to increasing the powers of the EU) are expected to make significant electoral gains. At the same time, the main center-right alliance is very likely to win the largest number of seats and maintain its historical dominance of parliament. In the cyber realm, the EU election represents a key target for state-backed threat actors, particularly Russian-linked groups. The campaign season has already been impacted by several online influence campaigns, and there could be digital disruptions on the days of voting. In terms of physical security, there is a low risk that the election will be the target of an organized terrorist operation. Instead, attacks by lone actors constitute the main threat.

| Cyber Intelligence |

Cyber Intelligence Key Findings

Russia Amps up Efforts to Disrupt Paris Olympics with Disinformation

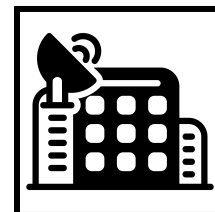


What happened: Researchers have observed Russian threat actors, including “Storm-1679” and “Storm-1099”, ramp up disinformation campaigns to target France, French President Emmanuel Macron, the International Olympic Committee (IOC), and the upcoming 2024 Paris Olympic Games. The campaign aims to besmirch the IOC while creating an impression of potential violence disrupting the international event. Storm-1679 released a feature-length film, *Olympics Has Fallen*, using artificial intelligence (AI) to impersonate Tom Cruise and discredit the IOC. Additionally, Storm-1679 has been disseminating false videos to incite fear of violence at the Games, while Storm-1099 has amplified anti-Olympics messaging through multiple fake news sites.

- **What this means:** Storm-1679 and Storm-1099 have reportedly been devising Olympic-specific disinformation campaigns since June 2023. These efforts are likely to invite more state-linked activity targeting the IOC and the Olympics, undermining the legitimacy of the committee and French security forces. The use of AI in these operations indicates a higher level of sophistication, making detection and mitigation more challenging. The Russian disinformation campaigns, if not checked, can also be used for fear-mongering among the audience and the participants, leading to lower spectator turnout, heightened security concerns, and damaged public trust in the IOC and French authorities. As the Games approach, the proliferation of these disinformation efforts is likely to increase, with potential real-world provocations exacerbating tensions and fear that could severely impact the Olympics' success and global perception.

Hackers Exploit TikTok Zero-Day to Break into CNN Account

What happened: Threat actors exploited a TikTok zero-day bug to hijack high-profile accounts, including those of celebrities and companies, and plant malicious code on CNN's official page. The now-patched flaw in the social media platform's direct message feature allowed hackers to compromise accounts merely by having the target open a malicious message.



- **What this means:** This TikTok zero-day exploit underscores the vulnerability of even well-established platforms to sophisticated cyber threats. The hijacking of high-profile accounts and the planting of malicious code on CNN's official page highlight the potential

for spreading misinformation, compromising user data, and undermining trust in both the affected individuals or organizations and the platform itself. The White House has had TikTok on its radar recently, calling for its ban in the United States on national security grounds. In the run-up to the upcoming U.S. presidential elections, hackers are likely to conduct more such nuisance and disruption in legitimate news sources to spread misinformation. Cybersecurity researchers have observed content farms impersonating reputable media outlets, aiming to exploit their trustworthiness for financial gain and to potentially manipulate public discourse. Additionally, threat actors are likely to use information extorted from the hijacked high-profile accounts to target account holders in malicious attacks like phishing, extortion, and blackmail.

Chinese State-Backed Cyber Espionage Targets Southeast Asian Government



What happened: A Chinese state-sponsored cyberespionage operation called Crimson Palace has been observed targeting a high-profile government organization. The threat group reportedly accessed critical IT systems, collected military and technical information, and conducted command-and-control (C2) communications in the interest of furthering state agendas.

➤ **What this means:** China has been at odds with various Southeast Asian countries over territory disputes in the South China Sea. Additionally, the Philippines opened a new Coast Guard station in its northern islands near Taiwan, which China claims as its own territory. The threat group's active reconnaissance of users of critical IT infrastructure could potentially point toward China gathering intelligence on surrounding territories to further its claims to the South China Sea.



ZEROFOX®

Weekly Intelligence Brief

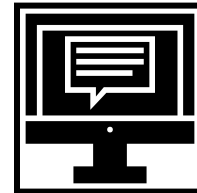
TLP:GREEN

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

Threat Actor Advertises New Multi-Threaded Brute Force Tool

What happened: On June 5, 2024, untested threat actor "S O V A" advertised a new, multi-threaded brute force tool on the predominantly Russian-language dark web forum xss. In the post, the actor claims that the unnamed tool—which it is charging USD 3,000 for access to—automatically generates strings for testing and uploads data to an unlimited number of servers.



S O V A further touts the tool's easy set-up process and friendly graphical user interface. The tool also reportedly supports popular virtual private network (VPN) vendors—such as Fortinet, Global Protect, Citrix, and Cisco—and runs on a variety of different operating systems, including Windows and Linux distributions Ubuntu and Kali.

- **What this means:** Despite the advanced sophistication of many of the tactics, techniques, and procedures (TTPs) used by threat actors today to gain initial access to a victim environment, simple brute force attacks remain a highly reliable technique by which to do so. Brute-forcing is a trial-and-error hacking method predominantly used to crack account passwords and decrypt files. Although the method is relatively simple in nature, it has evolved alongside the cybersecurity technology it attempts to bypass, namely through automated and streamlined processes achieved via custom tools and malware bots with password crackers. This has allowed threat actors to test billions of string combinations very quickly, resulting in a higher level of successful compromises—even from passwords deemed strong and complex. Because of this, new tools promoting the ability to automate the brute force process should be of concern, particularly as the use of AI technology increases the efficiency of cybercriminal activity.

Threat Actor Advertised Several Exploits



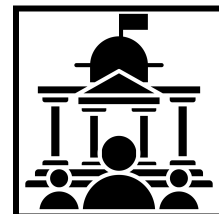
What happened: On June 4, 2024, well-regarded threat actor "johndoe7" advertised Remote Code Execution (RCE) and Local Privileges Elevation (LPE) exploits for various services on the predominantly Russian-language dark web forum xss. The actor did not specify the charge for the exploits, opting to have threat actors communicate with them via the forum's private message system. The actor also claimed that the exploits are private implementations that come with an easy-to-navigate GUI and an ability to pass sessions to and from C2. Johndoe7 stated that the source code for each exploit would be included as well. According to the actor, the exploits include:

- Exim RCE (CVE-2023-42115)

- Windows LPE (CVE-2024-26169)
- Microsoft Outlook RCE (CVE-2024-21413) with added support for unauthenticated SMTP servers
- GlobalProtect RCE (CVE-2024-3400)
- Fortinet FortiOS RCE (CVE-2024-21762)
- CrushFTP RCE (CVE-2024-4040)
- ScreenConnect RCE (CVE-2024-1709)
- Jenkins Exploit (CVE-2024-23897)
- JetBrains RCE (CVE-2024-27198)
- **What this means:** As johndoe7 is a well-regarded actor, their claims are likely credible. It is likely that there will be interested buyers for these exploits to conduct attacks if there are not patches for these vulnerabilities. The exploits will likely be sold privately, as the actor asked to be contacted via private message, so it will be unknown if any are purchased. It is important to ensure all systems are patched and operating on the most up-to-date software to minimize security risk.

Threat Actor Group Conducts Cyberattack Against UAE Government

What happened: On June 6, 2024, threat actor group Dark Storm Team (aka Dark Strom Team) announced a “massive cyberattack” against the United Arab Emirates (UAE) government. The attack, which targeted the Emirati Ministry of Education, was claimed on the group’s Telegram channel. The attack was carried out via distributed denial-of-service (DDoS) and was reportedly conducted in response to the UAE’s support of Israeli actions.



- **What this means:** Dark Storm is a hacktivist group whose primary cause is anti-Israeli/pro-Palestinian action. The group has carried out a number of attacks (all done via DDoS) against Western and Middle Eastern nations, including multiple attacks against U.S. targets in May 2024, and has previously targeted infrastructure in the UAE. DDoS attacks offer an easy, low-risk threat vector that allows the attacker to gain notoriety for themselves and their purported cause. It is likely hacktivist groups will maintain their current operational tempo over the near term.

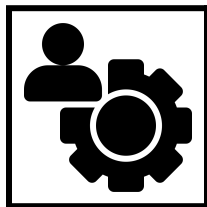
| Exploit and Vulnerability Intelligence |

| Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox has observed vulnerabilities, exploits, and updates disclosed by prominent companies in software solutions, asset management, and network security domains. A now-patched flaw in TikTok's direct message feature [allowed](#) hackers to compromise accounts merely by having the target open a malicious message. Zyxel has [released](#) patches addressing command injection and RCE vulnerabilities in two NAS products that have reached end-of-vulnerability support. Researchers have [released](#) a proof-of-concept exploit for CVE-2024-4358, a critical RCE vulnerability in Progress Telerik Report Servers that allows the unauthorized creation of admin accounts. Cox Communications has [resolved](#) a security flaw that allowed hackers to exploit backend APIs, potentially resetting millions of modems and stealing sensitive customer data. In the past week, CISA [added](#) CVE-2017-3506, an OS command injection vulnerability in the Oracle WebLogic Server, to its Known Exploited Vulnerabilities (KEV) catalog. Chinese threat actors are [exploiting](#) vulnerable ThinkPHP applications infected with CVE-2018-20062 and CVE-2019-9082 to install a persistent web shell named Dama.

Notable vulnerabilities:

[CVE-2018-20062 and CVE-2019-9082](#)

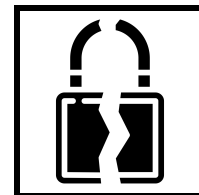


What happened: Chinese threat actors are exploiting ThinkPHP applications with vulnerabilities CVE-2018-20062 and CVE-2019-9082 to install the Dama web shell. Initially observed in October 2023, the malicious activity has recently intensified. Attackers use these vulnerabilities to perform RCE, impacting underlying content management systems by downloading the obfuscated Dama web shell. CVE-2018-20062 is a **CRITICAL** vulnerability with a CVSS score of 9.8, while CVE-2019-9082 is a **HIGH**-severity vulnerability with a CVSS score of 8.8.

- **What this means:** By exploiting vulnerable systems where users have not deployed patches for old bugs, attackers gain remote control over compromised servers, turning them into nodes for further attacks. Moreover, the Dama web shell facilitates further exploitation, allowing attackers to integrate compromised endpoints into their infrastructure. The campaign's broad targeting scope suggests opportunistic motives, increasing the threat landscape. The latest ThinkPHP versions contain patches to these bugs.
- **Affected products:**
 - CVE-2018-20062: NoneCMS 1.3
 - CVE-2019-9082: ThinkPHP versions 3.2.4 and older

[CVE-2017-3506](#)

What happened: There is a vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Services). Supported versions that are affected are 10.3.6.0, 12.1.3.0, 12.2.1.0, 12.2.1.1, and 12.2.1.2. This difficult-to-exploit vulnerability allows unauthenticated attackers with network access via HTTP to compromise the Oracle WebLogic Server.

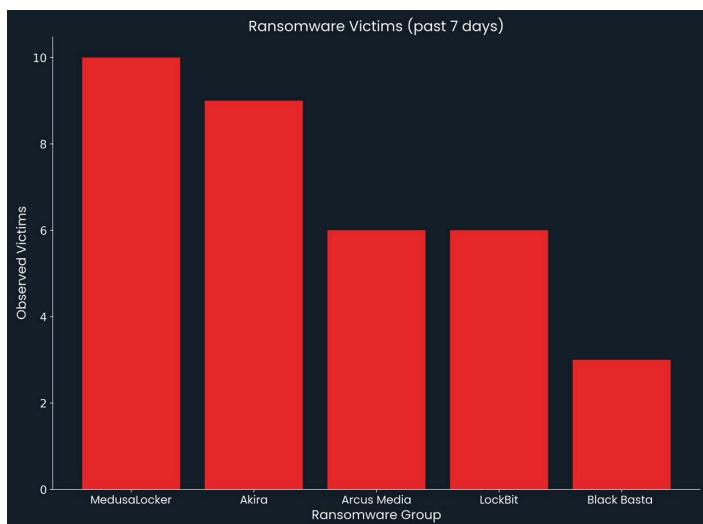


- **What this means:** Successful attacks of this vulnerability can result in unauthorized creation, deletion, or modification access to critical data or all Oracle WebLogic Server accessible data. This **HIGH**-severity bug has a CVSS 3.0 Base Score of 7.4.
- **Affected products:**
 - Oracle WebLogic Server versions 10.3.6.0
 - 12.1.3.0
 - 12.2.1.0
 - 12.2.1.1
 - 12.2.1.2.

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

Ransomware Intelligence: London Hospitals Cancel Operations Following Critical Ransomware Incident at Synnovis



What happened: A Russian-speaking ransomware gang called “Qilin” is suspected of being behind the cyberattack on National Health Service (NHS) medical services provider Synnovis, which has severely disrupted hospital operations and affected general practitioners across London. The attack forced leading London hospitals to cancel operations and divert emergency patients, significantly impacting services such as blood transfusions and test results. The Federal Bureau of

Investigation (FBI) recently obtained over 7,000 decryption keys for LockBit ransomware and is urging past victims to come forward to recover their encrypted data for free. The development is part of the FBI’s LockBit decryption efforts following an international operation, Operation Cronos, which dismantled the LockBit infrastructure in February 2024.

- **What this means:** The London hospital incident is part of a series of ransomware attacks on healthcare organizations this year, which have compromised patient services and exposed sensitive data. Qilin has been increasingly active, claiming responsibility for over 50 hacks in the past four months. The high disruption caused by targeting healthcare services makes these organizations lucrative targets for extortion, potentially endangering patient lives. The United States and Europe witnessed close to 70 percent of these ransomware incidents. LockBit has extorted up to USD 1 billion in ransoms from over 7,000 attacks worldwide. Despite law enforcement efforts, LockBit remains active, still targeting victims and leaking stolen data. The FBI’s call to action and provision of decryption keys represent crucial steps in combating ransomware and assisting affected organizations in recovering their data without making a ransom payment.

Breach Intelligence: Data Breach at Australian Rare-Earth Mining and Exploration Company

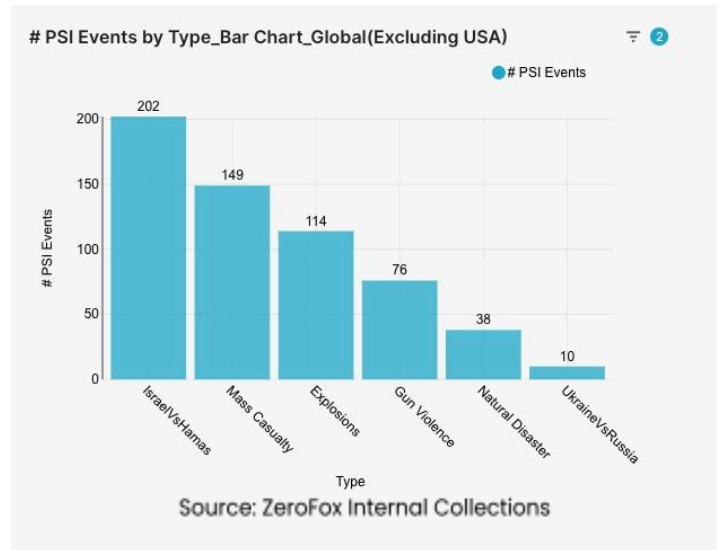
On June 4, ZeroFox observed an update on the BianLian ransomware leak site targeting Northern Minerals, an Australia-based mining company focused on the development of heavy rare-earth projects. The breach included operational, shareholder, financial, and employee data. Also, on June 3, ZeroFox [observed](#) threat actor Sanggiero claiming to sell Pandabuy's data for USD 40,000 on the English-language dark web forum BreachForums. Sanggiero claims to possess over 17 million records following a partial data leak on March 31. The debt collection agency Financial Business and Consumer Solutions (FBCS) has [updated](#) the number of individuals affected by a February data breach to over three million people.



Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

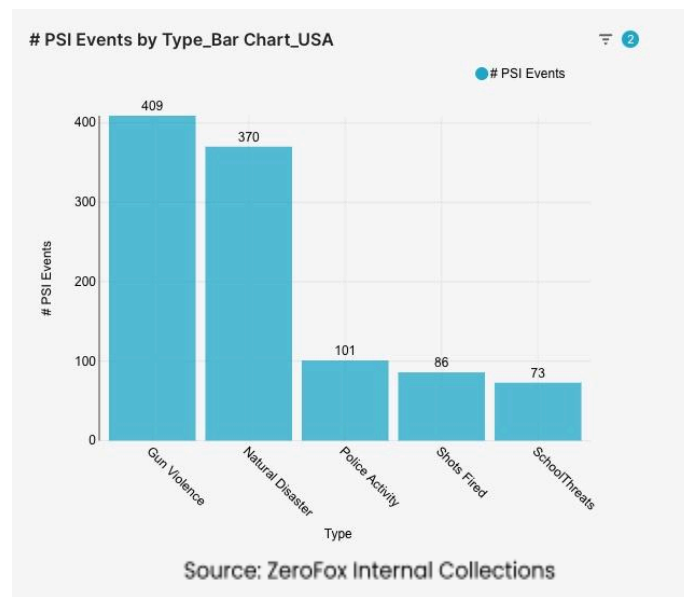


What happened: Excluding the United States, there was a one percent decrease in mass casualty events this week from the previous week, with the top contributing countries being Palestine, Israel, and Mexico (in that order); approximately 77 percent of these events were explosions. General alerts related to the Israel-Hamas War (including protests, raids, and involvement in neighboring countries) increased by one percent from the previous week. Additionally, events related to Russia's war in Ukraine

decreased by nine percent. The top three most-alerted subtypes were explosions, which saw a three percent increase from the previous week; gun violence, which increased by 65 percent (Mexico contributed to 16 percent of all gun violence alerts this week); and natural disasters, which increased by 15 percent.

- **What this means:** This week, Mexico had the third-highest mass casualty rate internationally and was the top contributor to gun violence, which saw a significant increase from the previous week. This is undoubtedly due to Mexico hosting its presidential election on June 2, which resulted in Claudia Sheinbaum becoming the country's first female president after one of the deadliest campaigns in Mexico's history. Thirty-seven candidates have been [assassinated](#), and there were over 800 non-lethal attacks by drug cartels such as Jalisco and Sinaloa, which are trying to ensure that their favored candidates—individuals who will turn a blind eye to the drug trade—take office. Natural disasters continue to wreak havoc around the world; the top contributing country this week was India, which accounted for over one-fifth of international natural disaster alerts. This uptick is more than likely due to the commencement of India's monsoon season, which has led to record levels of [rainfall](#), flooding, and storms this week, as well as extreme heat waves. ZeroFox expects this pattern to continue for the foreseeable future.

Physical Security Intelligence: United States



What happened: In the past week, the top three most-alerted incident subtypes were gun violence, natural disaster, and police activity. Gun violence alerts are instances in which there is a confirmed or likely confirmed victim, whereas shots fired alerts encompass shootings that did not result in a victim. The top two states that had the most gun violence alerts were Illinois and California, which together made up nearly one quarter of this week's nationwide total (24 percent). Gun violence across the United States increased by two percent from the week prior. The top two contributors to natural

disaster alerts this week were Florida and Texas, and natural disaster alerts across the country decreased by 28 percent. Police activity is used for instances in which there is a significant police presence on the scene for unknown reasons, a verbal shooting threat, lockdowns, and evacuations. Police activity alerts increased by 35 percent from the week prior, with the top contributing states being California and Georgia.

- **What this means:** While gun violence and natural disasters remained the top two alerted subtypes, police activity is once again in third place, with cities such as Los Angeles and Atlanta accounting for a significant amount of instances. Densely populated areas such as these are more likely to see higher crime rates, as is also seen in the gun violence instances, many of which occurred in Los Angeles and Chicago. While natural disasters across the nation have decreased, some states have continued to see unsettling weather patterns, with Florida being the top contributor this week; this is likely due to the state's hurricane season officially beginning on June 1. Florida has also issued a 14-day Disaster Preparedness Sales Tax [Holiday](#) running from June 1 through June 14 to encourage citizens to purchase disaster preparedness items. As for Texas, the state has continued to see instances of tornadoes, severe thunderstorms, and [flooding](#).

Interested in more ZeroFox Threat Intelligence? ZeroFox produces timely, relevant, and actionable [intelligence reporting](#) regularly to keep your team informed on developments in the threat landscape.

| 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%