



Weekly Intelligence Brief

Classification: TLP:GREEN

March 25, 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 March 22, 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 – Financial Scams Circulate as U.S. Tax Season Nears End	2
ZeroFox Intelligence Flash Report – Sale of Custom Phishlets for Evilginx3 Tool	2
ZeroFox Intelligence Brief – Social Engineering Series: Search Engine Optimization Poisoning	2
ZeroFox Intelligence Assessment – Influence Campaigns Ahead of the 2024 U.S. Presidential Elections	3
 Cyber Intelligence Key Findings	5
Chinese APT Conducts Widespread Operation; Breaches 70 Organizations Worldwide	5
FTC Warns of Scammers Pretending to Be Agency Staff	5
Spa Grand Prix Email Account Hacked to Phish Banking Info From Fans	6
 Deep and Dark Web Intelligence Key Findings	8
Killnet 2.0 Launches New Botnet	8
New Pro-Russian Hacktivist Group Emerges, Claims Compromise of U.S. Defense Logistics Agency	8
 Exploit and Vulnerability Intelligence Key Findings	11
CVE-2024-1597	11
CVE-2023-41724	12
 Ransomware and Breach Intelligence Key Findings	14
Threat Actors Target Health Services	14
Breach Intelligence: Fujitsu Customer Data Exposed	14
 Physical and Geopolitical Intelligence Key Findings	17
Physical Security Intelligence: Global	17
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 – Financial Scams Circulate as U.S. Tax Season Nears End](#)

As the end of the U.S. tax season nears, ZeroFox Intelligence has observed an increase in tax fraud-related activity taking place in the deep and dark web (DDW). On March 9, 2024, a Russian-speaking threat actor posted in the DDW forum xss, claiming they are able to supply two types of completed, illegitimate Internal Revenue Service (IRS) tax documents. Activity of this nature is very likely to increase in frequency over the coming weeks, with threat actors continuing to evolve their techniques, tactics, and procedures (TTPs) to most effectively leverage illicitly obtained personally identifiable information (PII) that is relatively cheap and easily acquired in DDW forums.

[ZeroFox Intelligence Flash Report – Sale of Custom Phishlets for Evilginx3 Tool](#)

On March 11, the well-regarded threat actor “blackdatabase” announced the sale of custom phishlets for Evilginx3 on the dark web forum xss. The phishlets for sale target multiple companies; prices start at USD 500 and range up to USD 5,000 for phishlets targeting specified financial sector entities. Evilginx3, when used in conjunction with phishlets, could enable attackers to steal session data, facilitate multi-factor authentication (MFA) bypass, and grant seamless access to sensitive data and funds stored in bank accounts.

[ZeroFox Intelligence Brief – Social Engineering Series: Search Engine Optimization Poisoning](#)

While a legitimate practice, SEO is also used for malicious purposes. This is referred to as SEO poisoning, or “black hat SEO,” and like legitimate SEO, it usually relies upon the premise that users of search engines find the top SERP results the most credible and appropriate to their search, increasing the likelihood they will be visited. SEO Poisoning is leveraged by a wide array of threat actors, such as financially-motivated cyber criminals, politically-motivated state actors, ideologically-motivated hacktivists, and organizations seeking a competitive advantage. The threat from SEO poisoning to organizations and individuals will almost certainly increase in 2024 as threat actors continually develop new social engineering methods to entice victims and deploy malicious payloads.

ZeroFox Intelligence Assessment – Influence Campaigns Ahead of the 2024 U.S. Presidential Elections

Harmful information is expected to be produced and promulgated online at an unprecedented scale in the run-up to the U.S. Presidential election in November 2024. Adversarial nation states, politically motivated cyber threat actors, and members of the public will almost certainly be responsible for the dissemination of election-related misinformation, disinformation, and malinformation—exacerbating simmering social, political, and geopolitical issues across all sectors of society. This, either intentionally or unintentionally—is expected to make it increasingly difficult to discern fact from fiction. The extent to which this harmful information is spread to influence the election outcome varies. Some online contributors will almost certainly unwittingly share inaccurate statistics, out-of-date information, or unknowingly engage with posts that the original source knows to be false. However, other threat actors are expected to actively engage in falsifying information, leaking sensitive information, and otherwise trying to shape the outcome of the election.

| Cyber Intelligence |

Cyber Intelligence Key Findings

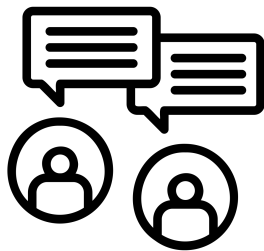
Chinese APT Conducts Widespread Operation; Breaches 70 Organizations Worldwide

What happened: Chinese advanced persistent threat (APT) group Earth Krahang has breached 70 organizations and targeted at least 116 across 45 countries in a sophisticated campaign active since early 2022. The threat group has reportedly compromised 48 government institutions, 10 of which are Foreign Affairs ministries, and targeted another 49 government agencies. The attackers exploit vulnerabilities in internet-connected servers and send spear-phishing emails to trick targets into installing custom backdoors for cyberespionage. Researchers have observed the adversary mainly targeting government, education, and communication sectors extensively.



- **What this means:** Utilizing open-source scanning tools, Earth Krahang targets public-facing servers, exploiting vulnerabilities like CVE-2023-32315 and CVE-2022-21587. Spear phishing emails, often leveraging compromised government accounts, are used to deliver malware like XDealer. The actor establishes persistence, exploits system vulnerabilities, and conducts lateral movement. Earth Krahang hackers misuse their access to hacked government systems to attack other governments. They set up private internet servers on compromised computers and try different password combinations to break into significant email accounts. There are links between Earth Krahang and Earth Lusca— another Chinese threat actor that targets mainly government entities— indicating shared management. To mitigate risks, researchers have urged organizations to prioritize security best practices, including employee education and software patching.

FTC Warns of Scammers Pretending to Be Agency Staff



What happened: The Federal Trade Commission (FTC) is warning the public about scammers pretending to be affiliated with the agency to steal consumers' money. The agency will never ask consumers to move their money, send them to a Bitcoin ATM, demand cash withdrawals, threaten to arrest or deport them, or promise a prize. Scammers may use the names of real employees, offer free money from government grants, or claim that a family member is in trouble and needs money. It is important to learn the signs of a scam and report it immediately. FTC has released an advisory to

help the public identify and avoid imposter scams, including those involving business and government impersonators.

- **What this means:** The FTC has seen a surge in complaints about scammers impersonating agency staff to trick consumers into wiring money. In the advisory, the FTC states that it has finalized the Government and Business Impersonation Rule, empowering them to fight back and reimburse victims. Additionally, the FBI warns against falling for tech support and government impersonation scams, advising against clicking on suspicious links, contacting unknown numbers, downloading software from strangers, or giving them computer access. The FBI's 2023 Internet Crime Report reveals a 22 percent rise in online crime losses, totaling USD 12.5 billion, with BEC, investment fraud, ransomware, and impersonation scams causing the most damage. The FBI also recorded 880,000 complaints, with seniors most affected.

[Spa Grand Prix Email Account Hacked to Phish Banking Info From Fans](#)

What happened: Hackers recently targeted the Belgian Grand Prix event in a phishing attack that lured fans with the promise of a EUR 50 gift voucher to a fake website resembling its official site. The attackers hijacked the official contact email to send victims malicious emails with an embedded link directing them to the site where victims entered their payment information. The phishing attack is being contained as investigations are trying to determine the cause and the scale after SPA GP responded to the attack in a few hours.

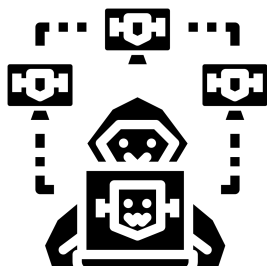


- **What this means:** In this phishing attack, attackers sent out emails that contained the same banner image on the official Belgian Grand Prix website. News sources show that these emails lured victims with the promise of a gift voucher, justifying that this was an “exclusive initiative to celebrate our valued customers like you.” ZeroFox observes a trend in widespread fraudulent activity targeting fans and spectators as it has with the recent U.S. Super Bowl event. As the Grand Prix is one of the world’s most anticipated and viewed sporting events, these events present various opportunities for financially-motivated threat actors to target fans and spectators—both those in attendance and fans watching from afar.

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

Killnet 2.0 Launches New Botnet



What happened: On March 19, 2024, threat actor group Killnet 2.0 claimed to launch their own botnet. This announcement comes after KillNet 2.0 emphasizes they are decentralized and that the group does not only have Russian hackers. KillNet 2.0 will likely attract more international hacktivist groups to join their decentralized efforts. Botnet attacks are far more dangerous than single malware attacks because rather than infecting a single device, botnets infect hundreds, thousands, or even millions of connected devices at once.

- **What this means:** Despite KillNet 2.0 being a separate entity from the original KillNet after it was taken over by Deanon from Kilmilk, they continue to operate similarly to their namesake. The Botnet is announced with 50 million requests per second, more than 20 servers (L4/L7), and more than a dozen attack types. All payment methods are available, and lifetime access is \$500. The announcement of a new botnet will likely involve a multitude of attack angles in different areas of the world, as the group continues to advertise that they are not exclusively composed of Russian hackers. KillNet 2.0 may use this botnet to carry out more sophisticated DDoS attacks on a larger scale.

New Pro-Russian Hacktivist Group Emerges, Claims Compromise of U.S. Defense Logistics Agency

What happened: On March 18, 2024, ZeroFox identified a new pro-Russian hacktivist group called “Russian Evilics.” The group, who made their initial pronouncement on the group’s Telegram site, claims to have been operating for some time in support of Russia’s interests. The group’s stated goal is to “protect the interests of the Russian Federation in cyberspace.” In their initial post, the group claims to have compromised the U.S. Defense Logistics Agency (DLA) site and gained access to “many documents of level A, B, C, D, E, F.” The post states that details of an unnamed American combat vehicle in use in Ukraine will be released in the near future.



- **What this means:** There is no further information on the claimed compromise of the U.S. DLA nor verification of the group’s claim to have sensitive military documents. The Telegram post included a screenshot of a DLA website that included a number of tabs.

However, no sensitive information was visible in the image. Russian Evilics claims to have been in operation for some time, possibly as a ransomware group. It is unclear if the group has any affiliation with known ransomware actors. Russian Evilics' Telegram presence is small and new; however, based on this limited information, it appears their primary tangible goal to date is to affect the battlefield in Ukraine in support of Russian forces. ZeroFox will continue to monitor the group for indications of malicious activity.

| Exploit and Vulnerability Intelligence |

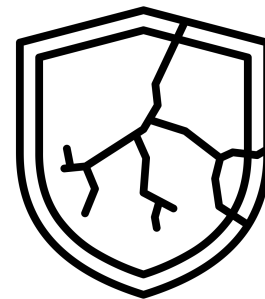
| Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox has observed vulnerabilities disclosed by prominent companies in software solutions, asset management, and network security domains. Google Chrome has released Chrome 123 to [address](#) one high-severity bug, five medium-severity bugs, and one low-severity bug. Fortinet has [released](#) a patch for FortiClient Enterprise Management Server (EMS) software to address the vulnerability tracked as CVE-2023-48788. Mozilla Firefox, another well-known browser, has [released](#) Firefox 124 with patches for several bugs, including six high-severity bugs and one critical severity bug. IT software solutions provider Ivanti has [disclosed](#) a new vulnerability, dubbed CVE-2023-46808, with a CVSS score of 9.8. Ivanti has patched the bug in all supported versions of Ivanti Neurons for ITSM (2023.3, 2023.2, and 2023.1), and all Ivanti Neurons for ITSM Cloud landscapes. The company has [patched](#) another critical bug (CVE-2023-41724; CVSS score: 9.6/10), which allows an unauthenticated threat actor to execute arbitrary commands on the underlying operating system of the appliance within the same physical or logical network. Meanwhile, Atlassian has [announced](#) patches for 24 high-severity vulnerabilities and one critical-severity vulnerability.

Notable vulnerabilities:

[CVE-2024-1597](#)

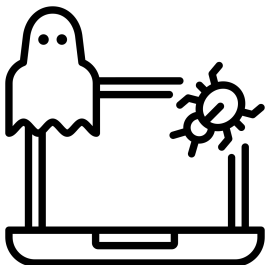
What happened: CVE-2024-1597 SQL injection issue, the critical-severity flaw impacts the org.postgresql:postgresql third-party dependency of Bamboo Data Center and Server. This vulnerability does not affect Bamboo & Other Atlassian Data Center products as they do not use the PreferQueryMode=SIMPLE in their SQL database connection settings. This **CRITICAL** vulnerability has been assigned a CVSS score of 10.



- **What this means:** CVE-2024-1597 could allow an unauthenticated attacker to expose assets in an environment susceptible to exploitation. The exploitation requires no user interaction and will likely have a high impact on confidentiality, integrity, and availability.
- **Affected products:**
 - Bamboo Data Center and Server versions from 9.5.0 to 9.5.1
 - Bamboo Data Center and Server versions from 9.4.0 to 9.4.3
 - Bamboo Data Center and Server versions from 9.3.0 to 9.3.6
 - Bamboo Data Center and Server versions from 9.2.0 to 9.2.11 (LTS)
 - Bamboo Data Center and Server versions from 9.1.0 to 9.1.3
 - Bamboo Data Center and Server versions from 9.0.0 to 9.0.4

- Bamboo Data Center and Server versions from 8.2.0 to 8.2.9
- Any earlier versions of Bamboo Data Center and Server

CVE-2023-41724



What happened: NATO cybersecurity researchers reported a critical remote code execution (RCE) vulnerability (CVE-2023-41724) in Ivanti Standalone Sentry, which has been patched by Ivanti. Although Ivanti has confirmed that no customers have been compromised, Ivanti strongly advises implementing the patch immediately. Standalone Sentry serves as a gateway between devices and an organization's ActiveSync-enabled email or backend resources and can function as a Kerberos Key

Distribution Center Proxy (KKDCP) server. This **CRITICAL** vulnerability has a CVSS score of 9.6.

- **What this means:** Exploiting CVE-2023-41724 could allow an unauthenticated threat actor within the same network to execute arbitrary commands on the appliance's operating system. However, exploiting this flaw from the internet is reportedly limited to threat actors lacking a valid TLS client certificate enrolled through EPMM.
- **Affected products:**
 - Any earlier versions of Ivanti Standalone Sentry 9.17.0
 - Ivanti Standalone Sentry 9.17.0
 - Ivanti Standalone Sentry 9.18.0
 - Ivanti Standalone Sentry 9.19.0

| Ransomware and Breach Intelligence |

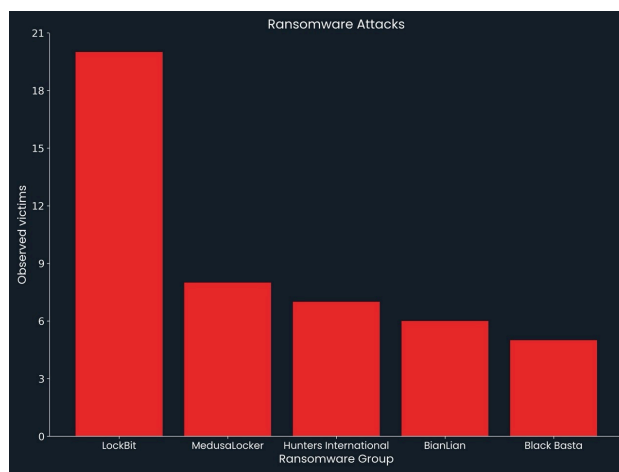
Ransomware and Breach Intelligence Key Findings

Threat Actors Target Health Services

What happened: LockBit and MedusaLocker ransomware groups have been the most active groups in the past week. ZeroFox has observed various ransomware groups targeting healthcare facilities, particularly in North America.

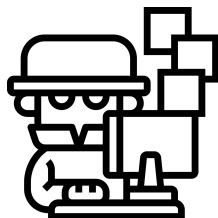
➤ **What this means:** Healthcare providers

have been targeted by ransomware attacks frequently, potentially compromising data from hospital networks. ZeroFox has observed Hunters International ransomware targeting Therapeutic Health Services in the United States. Change Healthcare is reportedly still recovering from the ransomware attack by ALPHV, with consumers and pharmacies reporting ongoing impact, such as not being able to apply coupons that many use to pay for medications. The American Hospital Association (AHA) has released an advisory relating to the cyberattack on Change Healthcare. The Advisory contains guidelines and preventive measures to help them protect themselves. Network defenders can protect and respond to unauthorized activity. In the global scenario, the threat actor “infamous” claimed to sell medical records from the Department of Medical Examination and Treatment Management under Vietnam’s Ministry of Health, and the threat actor “Ynnian” claimed to have leaked a database associated with Moscow Clinical Research Center on the dark web forum BreachForums.



Source: ZeroFox Internal Collections

Breach Intelligence: Fujitsu Customer Data Exposed



What happened: Fujitsu has recently issued an apology for exposing customer data after discovering malware on its computers. The multinational corporation has released a statement saying that it had disconnected the affected business computers immediately after it confirmed the presence of malware and deployed measures to strengthen the monitoring of other business computers. Fujitsu has also reported the incident to Japanese regulators at the Personal Information

Protection Commission. However, it remains unknown how long the data was exposed, and Fujitsu has yet to provide additional details about the breach.

- **What this means:** Cybersecurity researchers have stated they discovered a publicly accessible Microsoft Azure storage bucket associated with Fujitsu named "fjbbackup." The exposed bucket allegedly held private client data, AWS keys, and a CSV file containing passwords extracted from the popular password manager LastPass. A lack of clear protocol for informing about security issues reportedly made it difficult for the researchers to alert the company. Affected individuals and companies should be wary of unsolicited communication involving targeted emails or calls from unknown sources, as threat actors might use the leaked information for spear phishing attacks.



ZEROFOX®

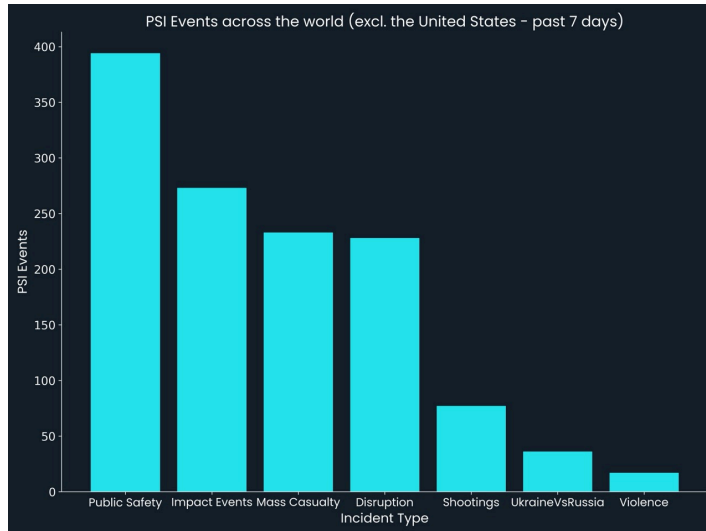
Weekly Intelligence Brief

TLP:GREEN

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global



Source: ZeroFox Internal Collections

What happened: North Korea fired short-range ballistic missiles on March 18, coinciding with U.S. Secretary of State Antony Blinken's visit to Seoul. The missiles traveled about 200 miles from Pyongyang to the East Sea, near Japan and South Korea. On March 19, Hong Kong passed a new national security bill, Article 23, after just two weeks of review. This legislation broadens convictions and imposes harsher penalties for offenses like treason and espionage, with sentences ranging from several years to life imprisonment.

Meanwhile, Nepal's two largest communist parties have formed a new coalition government favoring China over India.

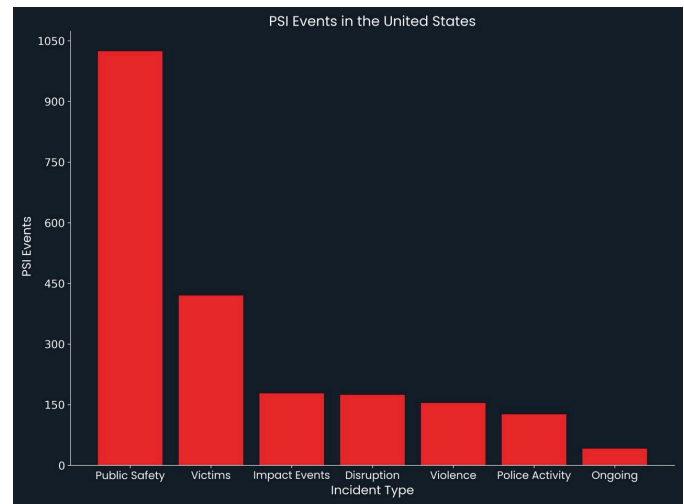
- **What this means:** Hong Kong's rapid approval of the strict Article 23 law raises concerns about its impact on the city's freedom and global financial status. This law broadens convictions and imposes harsher penalties, potentially leading to life imprisonment. It is likely to further restrict free speech, following China's earlier imposition of a national security law. North Korea's recent missile launches come days after the conclusion of joint U.S.-South Korean military exercises, which Pyongyang sees as provocative. Additionally, Nepal's new political alliance, like the Maldives, signals a shift away from Indian influence. The emergence of pro-China leadership in these countries reflects a growing trend, suggesting a shift in geopolitical dynamics and a rising mistrust of India among certain political factions in Nepal.

Physical Security Intelligence: United States

What happened: In the past week, the U.S. Supreme Court had ruled in favor of allowing a Texas law to temporarily take effect, which criminalizes unauthorized entry into Texas from Mexico and mandates state courts to order migrants, regardless of nationality, to return to Mexico. The law's coming to effect suggests differing outcomes for migrants arriving in Texas, compared with those entering other states, such as New Mexico and Arizona. The Mexican government strongly opposes

the law, rejecting any measures allowing U.S. state or local authorities to arrest and deport individuals to Mexican territory, particularly from Texas.

- **What this means:** Senate Bill 4 (SB4) criminalizes unauthorized entry into Texas from any foreign country outside of legal ports of entry. Offenders may face jail time, deportation orders from state court judges, or both. The law extends beyond border areas, potentially affecting individuals residing in Texas cities hundreds of miles away who entered the country unlawfully up to two years prior. This law imposes stricter penalties, including up to 20 years in prison, on individuals illegally entering or reentering Texas. Mexico has criticized the law as anti-immigrant and declared its refusal to accept anyone deported by Texas authorities. At the time of reporting, the 5th Circuit Court of Appeals issued a hold on SB 4, hours after the U.S. Supreme Court had allowed the law to take effect.



Source: ZeroFox Internal Collections

Interested in more ZeroFox Threat Intelligence? ZeroFox researchers produce 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%