



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

September 23, 2024

Scope Note

ZeroFox's Weekly Intelligence Briefing highlights the major developments and trends across the threat landscape, including digital, cyber, and physical threats. ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 12:00 PM (EDT) on September 20, 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 Brief – Underground Economist: Volume 4, Issue 18	2
 Cyber Intelligence Key Findings	4
U.S. Sanctions Key Players in Intellexa Consortium for Predator Spyware Distribution	4
Chinese National Charged for Multi-Year “Spear-Phishing” Campaign	5
CISA Releases Analysis of FY23 Risk and Vulnerability Assessments	6
 Exploit and Vulnerability Intelligence Key Findings	9
CVE-2024-45695	10
CVE-2024-43461	10
 Ransomware and Breach Intelligence Key Findings	13
Ransomware Attacks and Takedowns Across Major Industries	13
Global Data Breaches and Their Far-Reaching Effects	15
 Appendix A: Traffic Light Protocol for Information Dissemination	17
 Appendix B: ZeroFox Intelligence Probability Scale	18

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Brief – Underground Economist: Volume 4, Issue 18

The Underground Economist is an intelligence-focused series illuminating Dark Web findings from the ZeroFox Intelligence Team. On September 15, 2024, actor “mastermind1983” announced in the deep and dark web (DDW) forum Exploit that they are seeking collaborators for the execution of a “worldwide robbery” of Ethereum wallets. So far in September 2024, ZeroFox has observed the emergence and advertisement of two separate brute checker tools designed to target corporate networks. On September 6, 2024, an actor known as “skng” posted in the dark web forum xss advertising a new malicious script that is allegedly designed to target Fortinet software solutions. On September 5, 2024, untested actor “InvaderX” posted in the DDW forum RAMP (where they had registered several days earlier) announcing that they are seeking affiliates for their new InvaderX ransomware-as-a-service (RaaS).

| Cyber Intelligence |

(From the Deep, Dark, and Surface Web)

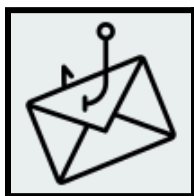
| Cyber Intelligence Key Findings



U.S. Sanctions Key Players in Intellexa Consortium for Predator Spyware Distribution

What happened: The U.S. Treasury Department imposed sanctions on five individuals and one entity tied to the Intellexa Consortium, the developer of Predator spyware and manager of entities supplying spyware tools to foreign governments. The Intellexa Consortium is a complex international web of decentralized companies that built and commercialized a comprehensive suite of highly invasive spyware products, primarily marketed under the “Predator.” The sanctions target the consortium’s efforts to evade previous sanctions and continue selling the spyware through complex corporate structures. In March 2024, the United States issued sanctions against the founder of the Intellexa consortium—a former Israeli military officer who had founded the company—and other entities, including North Macedonia-based Cytrox AD, Hungary-based Cytrox Holdings ZRT and Ireland-based Thalestris Limited, for developing and distributing Predator.

- **What this means:** Since its establishment in 2019, the Intellexa Consortium has served as a brand name for companies specializing in offensive cyber technologies. These companies provide commercial spyware and surveillance tools for both targeted and large-scale surveillance operations, bundled under the brand Predator spyware. The spyware can penetrate various electronic devices through zero-click attacks, which indicates that the spyware does not require any user interaction to infect a device. It is likely deployed in political and strategic schemes against adversarial states. Sanctions imposed on Intellexa are a direct response to its illicit global operations, selling Predator to state actors and governments. Moreover, foreign actors have deployed Predator spyware to covertly monitor government officials, journalists, and policy experts across multiple countries, including within the U.S. government. Its capabilities for zero-click attacks likely allow it to silently infiltrate smartphones and maintain persistent access, threatening individual privacy and state security. Once a device is infected by Predator, malicious actors can use Predator for unauthorized data extraction, tracking the device location, and accessing various applications and personal details such as contacts, call logs, messages, microphone recordings, and media. Despite earlier sanctions, Intellexa continues to sell the spyware. Intellexa, with its global clientele, has contributed to the spread of commercial spyware and surveillance technologies worldwide, including within authoritarian regimes. The U.S. government is working to disrupt the spyware market and deter technical talent from joining this exploitative industry.



Chinese National Charged for Multi-Year “Spear-Phishing” Campaign

What happened: A Chinese national was indicted on charges of wire fraud and aggravated identity theft for a multi-year spear phishing campaign. He allegedly impersonated U.S.-based researchers and engineers to fraudulently obtain restricted computer software and source code from the National Aeronautics and Space Administration (NASA), research universities, and private companies. The accused was employed as an engineer at the Aviation Industry Corporation of China (AVIC)—one of the largest global defense contractors and a major manufacturer of both civilian and military aircraft—and conducted these activities while working there.

- > **What this means:** The accused orchestrated a sophisticated and multi-year spear phishing campaign with the aim of illicitly acquiring specialized software crucial for aerospace engineering and computational fluid dynamics, fields that hold significant industrial and military applications. By creating deceptive email accounts to impersonate legitimate U.S.-based researchers and engineers, the accused exploited the trust within professional and academic circles to target individuals at prominent institutions, including NASA, various branches of the U.S. military, the Federal Aviation Administration, and several major universities and aerospace companies. The motivation behind this scheme was likely driven by a desire to gain unauthorized access to proprietary and restricted software that could be instrumental in advancing technological capabilities in areas such as advanced missile development and aerodynamic design of weapons systems. This breach of security is of grave concern because the stolen software could potentially be used to develop advanced military technologies that undermine national security, exacerbate geopolitical tensions, and jeopardize the safety of defense systems. The strategic nature of the information targeted demonstrates the seriousness of the offense, as it highlights vulnerabilities in the protection of sensitive technological resources and the potential for their misuse to compromise national and international security interests. Another noteworthy point is the fact that the accused was employed as an engineer at AVIC significantly intensifies the gravity of the situation. AVIC's dual role in producing both civilian and military aircraft means that any stolen software could directly enhance China's defense capabilities, potentially giving it a strategic advantage. This raises concerns about industrial espionage and national security, as it implies a targeted effort to undermine U.S. technological supremacy and could strain international relations by highlighting vulnerabilities in global defense and aerospace industries.



CISA Releases Analysis of FY23 Risk and Vulnerability Assessments

What happened: CISA has published an [analysis](#) detailing the findings from the 143 risk and vulnerability assessments (RVAs) conducted across multiple critical infrastructure sectors in fiscal year 2023 (FY23). The analysis details a sample attack path, including tactics and steps a cyber threat actor could follow to compromise an organization with weaknesses representative of those CISA observed in FY23 RVAs. To defend against the abuse of valid accounts, Critical Infrastructure (CI) entities should implement strong password policies and phishing-resistant multi-factor authentication (MFA). Identity Access Management (IAM) solutions and granular access controls should be utilized to protect privileged accounts and credentials. Monitoring access logs for abnormal activity and responding swiftly to detected anomalies is crucial to limiting damage. Additionally, CI entities should deploy intrusion prevention strategies, such as using a centralized cyber threat intelligence platform and adopting a secure, layered network architecture with firewalls, encryption, and segmentation. CISA encourages organizations to tailor these recommendations to their environments to mitigate high-level vulnerabilities.

- **What this means:** After conducting trend analysis on the networks and network defenses of the entities in the 143 RVAs, CISA and the United States Coast Guard (USCG) made high-level observations that would improve the ability of CI organizations to secure and protect their networks. Throughout the assessment lifecycle, Valid Accounts was the most prominent technique used across multiple tactics. Although CISA and the USCG teams do not directly emulate an adversary, they locate any conditions present in the environment or use opportunistic techniques. In previous years, assessors primarily used Valid Accounts to gain initial access to the network. However, in FY23, they found opportunities to use Valid Accounts to move laterally through the network, evade defenses, and escalate privileges, although in many cases, the same accounts can be used in several stages of the ATT&CK framework. Therefore, a threat actor can do a lot with a small number of credentials accessed early on. Valid Accounts can be accessed internal or external to the network through default or stolen administrator accounts, or former employee accounts that have not been removed from the active directory. Threat actors can compromise a valid administrator account if organizations do not change default passwords or through brute force if a weak password is in place. In many cases, this attack technique is possible because the valid account allows unauthorized users to install or execute insecure software (such as unpatched or out-of-date software) on a system or network. In many ways, a successful entry is the first cataloged achievement for a malicious actor. With internal access, attackers are privy to private systems and information. The next step of the

attack, whether it be code execution, mission disruption, gaining increased privileges, or maintaining unauthorized access for future disruption, may not be possible without initial access.

| Exploit and Vulnerability Intelligence |

| Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox has observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in software solutions, industrial control systems (ICS), and cybersecurity domains. Apple [released](#) security updates to address vulnerabilities in multiple Apple products. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system. The vulnerabilities affect several Apple products, including iOS 18, iPadOS 18, Safari 18, macOS Ventura, and watchOS 11. An OS command injection vulnerability (CVE-2024-8190) in Ivanti Cloud Services Appliance versions 4.6 Patch 518 and earlier [allows](#) a remote authenticated attacker with admin privileges to achieve remote code execution. Since Ivanti CSA 4.6 is End-of-Life and no longer receives updates or patches for its OS or third-party libraries, this vulnerability remains unaddressed. On September 6, 2024, an actor known as “skng” [posted](#) in the dark web forum xss advertising a new malicious script that allegedly enables attackers to exploit a critical vulnerability known as [CVE-2022-40684](#), discovered in early October 2022. D-Link has [released](#) updates for five vulnerabilities in its three wireless router models that allow remote attackers to execute arbitrary code or access the devices using hardcoded credentials. Of the five bugs, [CVE-2024-45695](#) and [CVE-2024-45694](#) are critical Stack-based Buffer Overflow vulnerabilities (CVSS score: 9.8/10.0 for both), allowing unauthenticated remote attackers to execute arbitrary code on the device. Broadcom has [addressed](#) a critical (CVSS score: 9.8/10.0) security flaw, CVE-2024-38812, in VMware vCenter Server that could allow attackers to execute remote code on vulnerable servers by sending a network packet. GitLab [released](#) security updates for a critical SAML authentication bypass vulnerability (CVE-2024-45409) affecting self-managed GitLab CE and EE, caused by issues in OmniAuth-SAML and Ruby-SAML libraries. CISA added eight vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog in the past week, across three advisories. One of the advisories [addressed](#) CVE-2024-6670 and CVE-2024-43461. [CVE-2024-6670](#) in WhatsUp Gold versions released before 2024.0.0 is a critical (CVSS score: 9.8/10.0) SQL Injection vulnerability that allows an unauthenticated attacker to retrieve the user’s encrypted password. [CVE-2024-43461](#) is a Windows MSHTML spoofing bug exploited by the Void Banshee APT group. The flaw has been patched in this month’s Microsoft Patch Tuesday. In the second KEV advisory, CISA addressed CVE-2024-27348, CVE-2020-0618, CVE-2019-1069, CVE-2022-21445, and CVE-2020-14644. [CVE-2024-27348](#) is a remote command execution (RCE) vulnerability in Apache HugeGraph-Server. [CVE-2020-0618](#) is an RCE vulnerability that exists in Microsoft SQL Server Reporting Services, while [CVE-2019-1069](#) is an elevation of privilege vulnerability that exists in the way the Task Scheduler Service. [CVE-2020-14644](#) and [CVE-2022-21445](#) are both RCE bugs affecting Oracle products. The third KEV advisory addresses [CVE-2024-8963](#), which is a path traversal bug in the Ivanti CSA before 4.6 Patch 519 allows a remote unauthenticated attacker to access restricted functionality. Another CISA advisory [highlights](#) an OS command injection RCE vulnerability (CVE-2024-8190) in Ivanti Cloud Services

Appliance versions 4.6 Patch 518 and before. CISA also [released](#) six Industrial Control Systems (ICS) advisories on September 19, 2024. These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS.

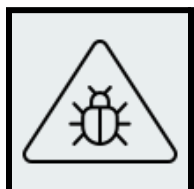


Critical

CVE-2024-45695

What happened: The web service of certain models of D-Link wireless routers contains a Stack-based Buffer Overflow vulnerability, which allows unauthenticated remote attackers to exploit this vulnerability to execute arbitrary code on the device. Additionally, D-Link has [released](#) updates for four more vulnerabilities in its three wireless router models that allow remote attackers to execute arbitrary code or access the devices using hardcoded credentials. This flaw has a CVSS score of 9.8.

- **What this means:** The security flaw in the web service of certain D-Link wireless routers allows unauthenticated attackers to exploit the vulnerability remotely. By doing so, they can execute arbitrary code on the router, which may enable them to take full control of the device. This control could be used to alter router settings, intercept network traffic, or launch attacks on other devices connected to the network. As a result, this vulnerability poses a significant risk to both the integrity and confidentiality of network communications.
- **Affected products:**
 - DIR-X4860 A1 firmware version 1.00, 1.04



High

CVE-2024-43461

What happened: CISA has mandated U.S. federal agencies to secure their systems against this Windows MSHTML zero-day bug recently exploited and targeted by the Void Banshee APT group. Initially classified as not exploited, Microsoft updated its advisory to confirm prior attacks. The vulnerability was part of an exploit chain with CVE-2024-38112, used to deploy information-stealing malware through camouflaged HTA files.

- **What this means:** Exploiting the CVE-2024-43461 can let malicious actors conduct remote code execution, allowing them to deploy malware, steal sensitive information, and gain

unauthorized access to systems. By disguising malicious files as harmless documents, attackers can trick users into executing them, resulting in data breaches, financial theft, and system compromise.

➤ **Affected products:**

- Microsoft has released the complete list of affected products in [this](#) advisory.

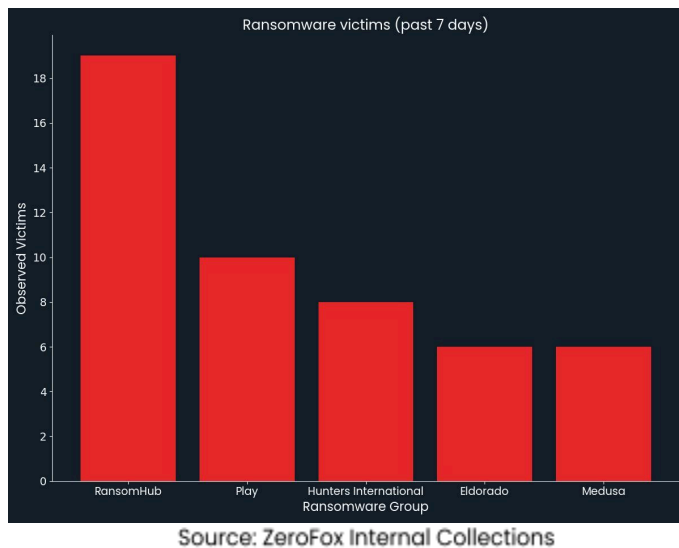
Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings



Ransomware Attacks and Takedowns Across Major Industries

What happened: Researchers have identified that the threat group Vanilla Tempest [deployed](#) INC ransomware for the first time in an attack targeting the U.S. healthcare sector. This attack disrupted the healthcare provider's IT and phone systems, leading to a loss of access to critical patient information databases. Authorities in Germany have been [investigating](#) the ransomware group "Vanir Locker," which steals and encrypts company data, demanding ransom to prevent the data's release. In August 2024, investigators identified the group's server on the TOR network and have now taken control of their page, blocking it to prevent the publication of stolen data. The investigation into the group's identity is ongoing. A threat actor has [unveiled](#) the release of critical C2C tools used by the RobbinHood ransomware group, updated to version 2.0 in 2020. The actor reportedly discovered this data during an attack on a government target, where RobbinHood operators failed to erase their shadow files. The leaked information includes sensitive details such as victim data, the group's Monero (XMR) and Bitcoin (BTC) addresses, operational tools, fake file hosters, and domain information. German authorities have [shut down](#) 47 exchange services that were being used for illegal activities, allowing the exchange of conventional and cryptocurrencies. The operators are accused of facilitating large-scale money laundering by deliberately bypassing legal anti-money laundering requirements, such as the "know-your-customer" principle. The platforms are now deactivated, and the operators face charges of money laundering and running criminal trading platforms. [Cencora](#), a major drug distributor, paid USD 75 million in Bitcoin to the Dark Angels group following a ransomware attack, marking the largest known cyber extortion payment. After discovering a data breach in February, Cencora negotiated the ransom down from the hackers' initial demand of USD 150 million, ultimately paying in three installments in March.



- **What this means:** INC ransomware's use in high-profile attacks highlights the growing danger of ransomware-as-a-service (RaaS) operations. The availability of ransomware source code for sale on dark web forums means more cybercriminals can potentially access these powerful tools, increasing the frequency and severity of attacks. The targeting of critical sectors such as healthcare, education, and manufacturing by threat actors like Vanilla Tempest poses a direct threat to national security. The takedown of the "Vanir Locker" group is significant because it disrupts a ransomware-as-a-service operation that actively recruited affiliates, potentially reducing the number of active cybercriminals in this space. By taking control of their leak site, authorities not only prevent the publication of stolen data but also undermine the group's financial model, which relied on exploiting companies for profit. The group's connections to other notorious ransomware factions highlight the ongoing evolution and collaboration within cybercrime networks, making this intervention crucial in mitigating future attacks and destabilizing such operations. The release of critical C2C tools and 7z file containing 130 MB of uncompressed sensitive data by a threat actor is significant, as it may encourage other threat actors or groups to also release similar tools and data, resulting in widespread exposure of sensitive information, increasing risks for organizations and individuals. Such leaks can enable malicious actors to exploit or replicate the disclosed techniques, exacerbating the threat landscape. The takedown of these 47 illegal exchange services is critical because it not only disrupts platforms facilitating large-scale money laundering but also secures vital user and transaction data that will aid future investigations. While no arrests have been made yet, the seizure of servers and extensive data enables authorities to track cybercriminals involved, even if they are currently out of reach due to protection by their home countries. The operation is likely to significantly hamper criminal networks that rely on these exchanges for illicit activities. Cencora plays a critical role in the healthcare supply chain, and disruptions to its operations can have wide-reaching consequences, potentially affecting the availability of essential medications and patient care. Healthcare companies are especially attractive targets for cybercriminals due to the sensitive nature of the data they handle, including patient records, drug inventories, and confidential business information. These organizations often face immense pressure to pay ransoms quickly to avoid operational disruptions, data exposure, or legal consequences.



Global Data Breaches and Their Far-Reaching Effects

What happened: Breaching data has become alarmingly easy for threat actors, who are increasingly targeting organizations worldwide to exploit vulnerabilities. This surge in attacks not only incurs substantial financial losses but also disrupts operations and leaves individuals at risk of identity theft. This week, several significant data breaches made headlines around the world, with a few incidents highlighted here. High-end British department store Harvey Nichols is [notifying](#) customers that some of their data was compromised in a recent cyberattack. Customers have either received or will soon receive letters detailing the incident, which revealed their names, company information (if provided), phone numbers, and email and home addresses. However, it is believed that highly sensitive information such as passwords and financial details remains unaffected. Threat actor "infamous" [claimed](#) to be selling a database associated with the Thailand Police for USD 1,000 on the dark web forum BreachForums. Allegedly, the leaked database contains information such as names, phone numbers, genders, and ID card numbers. A threat actor on a dark web forum has claimed to be [selling](#) VPN access to one of Spain's largest universities, potentially exposing a network of over 65,000 hosts. This university, operating in the higher education sector, generates approximately USD 800 million in annual revenue. Priced at USD 1,000, the actor asserts that detailed information will only be shared with reputable forum members via ZoomInfo. Hackers are [targeting](#) exposed Foundation accounting servers, commonly used in the construction industry, by brute-forcing passwords for highly privileged accounts. These attacks exploit a combination of accessible services and the failure of users to change default credentials, allowing attackers to breach corporate networks. Threat actor "888" claimed to be selling a [database](#) associated with SAP, a Germany-based software company, on BreachForums. The actor stated that SAP experienced a data breach through a third party in September 2024. The leaked database allegedly contains data on 2,600 users, including first names, last names, job titles, emails, and more. Threat actor "theDbasespremium" claimed to be selling a database [linked](#) to Dubai Municipality. The alleged leaked database reportedly includes information such as personal IDs, employee numbers, full names, dates of birth, and more. Threat actor "Sorb" [claimed](#) to have leaked a database associated with Bharat Petroleum Corporation on BreachForums. Allegedly, the leaked database contains 148 million rows of personal data, including phone numbers, names, delivery addresses, payment information, and order lists. Russian anti-malware firm Doctor Web (Dr.Web) recently [reported](#) a security breach following a cyberattack. In response to signs of unauthorized access to its IT infrastructure, Dr.Web has disconnected all servers from its internal network. Threat actor 303 claimed to have [leaked](#) a database associated with Chunghwa Telecom, a Taiwan-based telecommunications company. The threat actor also claims to have

leaked 400 GB of data that includes sensitive information, documents, and more. Threat actor "holyprix" [claimed](#) to sell a database associated with the Ministry of Human Resources and Social Development in Saudi Arabia. Threat actor "grep" claimed to have leaked a [database](#) associated with AirFinch, a U.S.-based platform developed by Appcodes, for booking rental accommodations and rental cars. The actor alleged that AirFinch experienced a data breach in September 2024. The leaked database contains user ID, first name, email, and more. The same threat actor [claimed](#) to have leaked a database associated with Dell. The actor alleged that Dell experienced a data breach in September 2024. The leaked database contains employee ID, full name, employee internal ID, and more.

- **What this means:** The recent wave of cyberattacks poses serious risks for organizations and their customers. For businesses like Harvey Nichols, the exposure of customer data can lead to a loss of trust and increased vulnerability to phishing scams, which may result in long-term reputational damage. Companies affected by database leaks, such as SAP and Bharat Petroleum, face not only potential financial losses but also regulatory challenges, which could bring legal consequences. The sale of compromised data on dark web forums puts customers at risk of identity theft and other forms of exploitation. Additionally, the targeting of Foundation accounting servers due to default credentials shows a critical weakness in security practices within the construction industry, making these firms more attractive targets for future attacks. Overall, these incidents emphasize the urgent need for organizations to reevaluate their data protection strategies and enhance user awareness to mitigate the risks associated with data breaches. To mitigate the risk of data breaches, individuals and organizations should prioritize strong, unique passwords, and enable two-factor authentication wherever possible. Regularly updating software and systems can help close security vulnerabilities. Users should be educated about phishing scams and the importance of verifying communication before sharing personal information. Additionally, implementing access controls and regularly auditing account permissions can help limit exposure in the event of a breach. Finally, having a comprehensive incident response plan can ensure a swift reaction to any security incidents that do occur.

| 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%