



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

April 29, 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 April 26, 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: Ransomware Threat Landscape Continues to Diversify in 2024	2
ZeroFox Intelligence Flash Report: New Ransomware-as-a-Service Operation Claims Innovative Features	2
 Cyber Intelligence Key Findings	4
North Korean Hackers Target South Korean Defense Industry Entities	4
Hackivist Cyberattack Caused a Water System to Overflow in a Rural Texas City	4
U.S. Government Issues New Guidance on Fortifying Election Infrastructure	5
 Deep and Dark Web Intelligence Key Findings	7
New Ransomware Group Self-Identifying as "APT73" Emerges	7
New Ransomware-as-a-Service "Psoglav" Announced on RAMP	7
Threat Actor "UserSec" Reportedly Preparing for Campaign Targeting NATO	8
 Exploit and Vulnerability Intelligence Key Findings	10
CVE-2022-38028	10
CVE-2024-4040	11
 Ransomware and Breach Intelligence Key Findings	14
Ransomware Threat Landscape Expands	14
Breach Intelligence: Threat Actor Leaks Data from UNDP	14
 Physical and Geopolitical Intelligence 	16
 Physical and Geopolitical Intelligence Key Findings	17
Physical Security Intelligence: Global	17
Physical Security Intelligence: United States	18
 Appendix A: Traffic Light Protocol for Information Dissemination	20
 Appendix B: ZeroFox Intelligence Probability Scale	21

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Brief: Ransomware Threat Landscape Continues to Diversify in 2024

The frequency of ransomware and digital extortion (R&DE) attacks is on an upward trajectory, with the number of observed incidents during Q1 2024 only slightly less than that of the previous quarter, despite Q4 2023 constituting more attacks than any other quarter observed by ZeroFox. An increasingly diverse threat landscape is contributing to the high number of incidents, with a large, growing number of collectives responsible for attacks. This is being propelled in part by several smaller and newer collectives becoming significantly more active.

ZeroFox Intelligence Flash Report: New Ransomware-as-a-Service Operation Claims Innovative Features

On April 19, 2024, positive-reputation threat actor "Bezzle" announced a new ransomware-as-a-service (Raas) operation dubbed "Apos" in the Russian-speaking deep and dark (DDW) community RAMP. Bezzle proclaims Apos is the "fastest" and "most technically advanced" product on the market. Apos purportedly has many software features that are typically only observed amongst the more advanced Raas offerings. The service also includes highly uncommon capabilities, which is very likely indicative of an attempt to separate the Apos service from its competition and appeal to potential affiliates. Raas offerings are very likely to become increasingly competitive during 2024, with collectives offering affiliates more software features, better technical support and digital infrastructure, higher payouts, and loyalty incentives.

| Cyber Intelligence |

Cyber Intelligence Key Findings

North Korean Hackers Target South Korean Defense Industry Entities



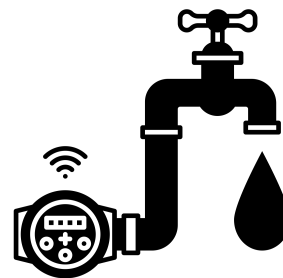
What happened: South Korea's National Police Agency has issued a warning stating North Korean hackers are increasingly targeting the nation's defense industry. Notorious North Korean hacking groups Lazarus, Andariel, and Kimsuky have been associated with successful breaches that have exploited vulnerabilities in both primary companies and their subcontractors. These infiltrations, dating back to late 2022, went unnoticed until a recent investigation. Lazarus targeted network connection systems, Andariel seized employee account data for malware installation, and Kimsuky exploited email server weaknesses.

- **What this means:** Lazarus hackers breached a defense company's network infrastructure, seizing critical data from multiple computers and transferring it overseas. The Andariel group gained access through stolen employee credentials, planting malware on subcontractors' servers and causing significant data breaches. Meanwhile, Kimsuky exploited an email server vulnerability to pilfer large files from a defense subcontractor. To mitigate such threats, Korean authorities advise implementing robust security measures like network segmentation, regular password updates, two-factor authentication, and blocking foreign IP access.

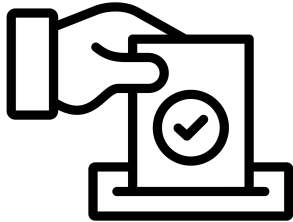
Hacktivist Cyberattack Caused a Water System to Overflow in a Rural Texas City

What happened: Researchers have linked a Russian hacktivist group, tracked as "CyberArmyofRussia_Reborn", to a cyberattack that led to a water system overflowing in the small rural Texas town of Muleshoe.

- **What this means:** This attack was one of three that targeted small towns in the rural Texas Panhandle. Even though attempts to hack into Hale Center systems failed, the attackers managed to cause an overflow in one water system in Muleshoe before city officials took prompt steps to shut it down and took over manually. Local officials have confirmed that the attack did not subject the public to any danger and had no impact on Muleshoe's water disinfectant system. Cybersecurity researchers have identified CyberArmyofRussia_Reborn as one of the groups with suspected ties to the Russian government that is engaging in low-complexity attacks against Ukraine and its allies, including denial-of-service assaults that have briefly disrupted websites.



U.S. Government Issues New Guidance on Fortifying Election Infrastructure



What happened: The U.S. government has released guidance to help election infrastructure stakeholders prepare for and respond to efforts by foreign adversaries to undermine the U.S. election process. The People's Republic of China (PRC), the Russian Federation, and the Islamic Republic of Iran remain the primary nation-state actors involved in hostile efforts by or on behalf of foreign governments to shape U.S. policies, decisions,

and discourse.

➤ **What this means:** The guidance suggests communicating early, promoting transparency, and securing public-facing content to help mitigate the impacts on election operations and maintain public confidence in the security and integrity of the American democratic process.



ZEROFOX®

Weekly Intelligence Brief

TLP:GREEN

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

New Ransomware Group Self-Identifying as “APT73” Emerges

What happened: On April 22, 2024, ZeroFox observed a new ransomware group operating under the name “APT73” on the surface web leak site `hXXp://eraleignews[.]com`. Currently, the only victim listed on the site is a company called Trifecta. Based on a partial description listed on the site, the victim is likely Pennsylvania-based software company Trifecta Technologies, Inc. Additionally, certain sections of the site directly replicate the leak site of notorious ransomware group LockBit, including the “Contact Us,” “How to Buy Bitcoin,” and “Web Security & Bug Bounty” sections.



- **What this means:** While APT73 may be an offshoot of LockBit, it is more likely it is an amateur ransomware group looking to gain a credible foothold in the industry by imitating the language and techniques of a successful and positive-reputation ransomware group. This is further evidenced by the group choosing the name APT73. Advanced Persistent Threats (APTs) are threat groups considered well-resourced and highly sophisticated and are tracked under assigned numbers designated by threat researchers. By following similar naming conventions, APT73 likely hopes to sow confusion amongst users and appear more reputable than it is.

New Ransomware-as-a-Service “Psoglav” Announced on RAMP



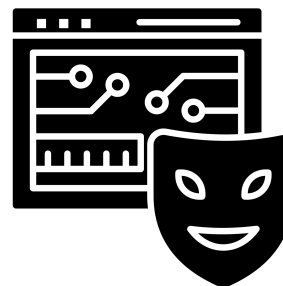
What happened: On April 24, 2024, the untested threat actor “rtgtgth” announced a new RaaS project dubbed “Psoglav” on the RAMP forum. The actor claimed that the new RaaS has the necessary functionality, and they will constantly develop the project based on user feedback. Rtgth also provided a list of features of the ransomware, including that it was written in C#, supports all Windows platforms, has fast file encryption, and deletes shadow copies and itself. Rtgth claimed that the group is only interested in long-term partnerships and that the first three partners will get the first decryptions for free. The actor listed their TOX for contact information.

- **What this means:** While ZeroFox has not yet detected active deployment of Psoglav, the announcement aligns with the recent increase in novel RaaS operations observed, which are likely a result of disruptions to a number of R&DE collectives recently. This announcement also aligns with the recently observed trend of English-speaking actors participating in the typically Russian-led ransomware scene. As these new groups emerge, they appear to build on past ransomware programs and make their own unique

enhancements to them. This suggests that ransomware will continue to become harder to detect and have more security functions, benefitting the affiliates using RaaS services.

Threat Actor “UserSec” Reportedly Preparing for Campaign Targeting NATO

What happened: On April 23, 2024, hacktivist threat actor group “UserSec” announced its intentions to undertake a new campaign targeting European and NATO nations. The group posted the announcement on its Telegram page and included a statement that it will “begin burning the enemies servers soon.”



- **What this means:** UserSec is a credible threat actor group with a proven track record of successfully conducting attacks against NATO nations. The group, which has been active since early 2022 in conjunction with the Russian invasion of Ukraine, has primarily conducted distributed denial-of-service (DDoS) and data leak attacks. Most recently in early April 2024, UserSec successfully leaked data sets from a number of U.S. federal government agencies. In February 2024, UserSec created a pro-Russian hacktivist collective with a number of other known threat actor groups with the stated intent of conducting attacks against Ukraine and NATO states supporting Ukraine. This most recent reported campaign falls in line with that effort.

| 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. Cisco has [released](#) security updates to address ArcaneDoor exploitation of Cisco Adaptive Security Appliances (ASA) devices and Cisco Firepower Threat Defense (FTD) software. A cyber threat actor could exploit vulnerabilities (CVE-2024-20353, CVE-2024-20359, CVE-2024-20358) to take control of an affected system. Security researchers have [observed](#) Russian GRU-linked APT28 (Forest Blizzard / STRONTIUM / Sednit / Fancy Bear) abusing a bug (CVE-2022-38028) in Windows Print Spooler to elevate privileges and steal credentials. The MITRE Corporation suffered a data breach in January 2024 via two Ivanti zero-days ([CVE-2023-46805](#) and [CVE-2024-21887](#)). Cybersecurity researchers have [uncovered](#) vulnerabilities in cloud-based pinyin keyboard apps that could expose users' keystrokes to malicious actors. There is a critical security vulnerability (CVE-2024-27956) in the WP-Automatic plugin for WordPress with a CVSS score of 9.9, [allowing](#) potential site takeovers before version 3.9.2.0. Proof-of-concept exploit code is out for a critical security flaw (CVE-2024-2389) in Progress Flowmon, allowing attackers to [gain](#) unauthenticated remote access and execute system commands via specially crafted API requests.

Notable vulnerabilities:

[CVE-2022-38028](#)



What happened: Security researchers have observed Russian GRU-linked APT28 (Forest Blizzard / STRONTIUM / Sednit / Fancy Bear) abusing a bug (CVE-2022-38028) in Windows Print Spooler to elevate privileges and steal credentials. This vulnerability is tracked as **HIGH** and is assigned a CVSS score of 7.8.

➤ **What this means:** With the weaponized bug, APT28 targeted European and North American governments, non-governmental, education, and transportation entities in attacks, which have continued since around April 2019. Patches for the bug were issued in October 2022. Users are advised to apply the patches as soon as possible to guard their networks against such attacks.

- **Affected products:**

- Windows Server 2016 (Server Core installation)
- Windows Server 2016
- Windows 10 Version 1607 for x64-based Systems
- Windows 10 Version 1607 for 32-bit Systems
- Windows 10 for x64-based Systems
- Windows 10 for 32-bit Systems
- Windows Server 2022

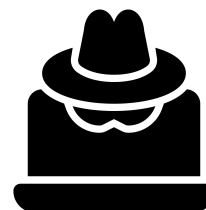
- Windows 10 Version 21H1 for 32-bit Systems
- Windows 10 Version 1809 for 32-bit Systems
- Windows RT 8.1
- Windows 8.1 for x64-based systems
- Windows 8.1 for 32-bit systems
- Windows Server 2012
- Windows 11 Version 22H2 for x64-based Systems
- Windows 11 Version 22H2 for ARM64-based Systems
- Windows 11 Version 21H2 for ARM64-based Systems
- Windows 11 Version 21H2 for x64-based Systems
- Windows 10 Version 20H2 for ARM64-based Systems
- Windows 10 Version 20H2 for 32-bit Systems
- Windows Server 2022 (Server Core installation)
- Windows 10 Version 21H1 for ARM64-based Systems
- Windows 10 Version 21H1 for x64-based Systems
- Windows Server 2019 (Server Core installation)
- Windows Server 2019
- Windows 10 Version 1809 for ARM64-based Systems
- Windows 10 Version 1809 for x64-based Systems
- Windows 10 Version 21H2 for x64-based Systems
- Windows 10 Version 21H2 for ARM64-based Systems
- Windows 10 Version 21H2 for 32-bit Systems
- Windows Server 2012 R2 (Server Core installation)

CVE-2024-4040

What happened: A server side template injection vulnerability in CrushFTP in all versions before 10.7.1 and 11.1.0 on all platforms allows unauthenticated remote attackers to read files from the filesystem outside of the VFS Sandbox, bypass authentication to gain administrative access, and perform remote code execution on the server. The **CRITICAL** vulnerability has a CVSS score of 9.8.

➤ **What this means:** CrushFTP has reportedly warned users to patch their systems against an actively exploited zero-day. Security researchers have observed attackers targeting CrushFTP servers in American organizations, potentially for politically motivated cyber espionage. The bug, which affects CrushFTP v11 versions below 11.1, has been patched in v11.1.0.

- **Affected products:**

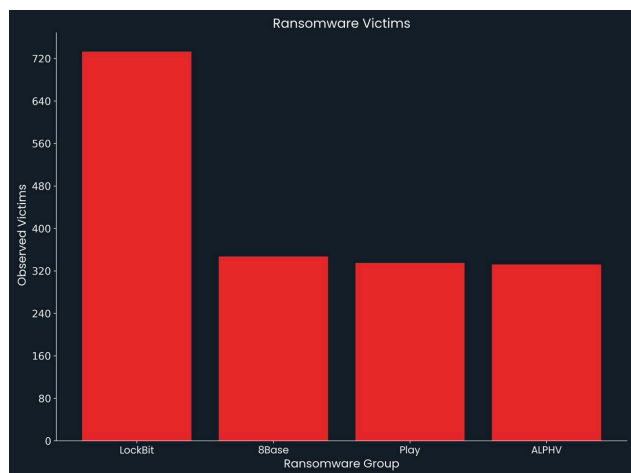


- Versions before 11.1

| Ransomware and Breach Intelligence |

Ransomware and Breach Intelligence Key Findings

Ransomware Threat Landscape Expands



Source: ZeroFox Internal Collections

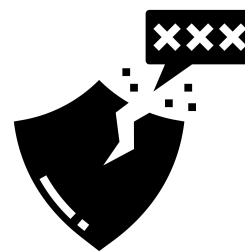
What happened: R&DE collective Hunters International has significantly increased its operational tempo, having so far conducted at least 29 attacks in February 2024. Several smaller threat groups, such as DarkVault, DragonForce, MyData, and Red, have displayed high attack tempos, which are historically atypical for newer collectives. It is very likely that such groups are benefitting from the acquisition of experienced affiliates from LockBit and ALPHV. ZeroFox observed very little change in the industries of targeted

organizations during Q1 2024. Compared to 2023, small increases were noted in the manufacturing, retail, construction, healthcare, and professional services industries. It is very unlikely that these increases are indicative of new targeting patterns; rather, they are likely the result of expected threat landscape fluctuations.

- **What this means:** Manufacturing will very likely remain the most targeted industry over the coming months, though variations will likely be observed as newer and smaller threat collectives establish and adapt their techniques, tactics, and procedures (TTPs). The region of victims also exhibited little variation between 2023 and Q1 2024. Slight increases in the targeting of North America-based organizations are very likely the result of natural fluctuations and not indicative of increased emphasis. North America will almost certainly remain the region most targeted by R&DE attacks over the coming months.

Breach Intelligence: Threat Actor Leaks Data from UNDP

What happened: The MITRE Corporation suffered a data breach in January 2024 via two Ivanti zero-days (CVE-2023-46805 and CVE-2024-21887). A state-backed hacking group hacked one of MITRE's VPNs and bypassed multi-factor authentication (MFA) defenses using session hijacking. The breach was discovered on MITRE's Networked Experimentation, Research, and Virtualization Environment (NERVE) network.



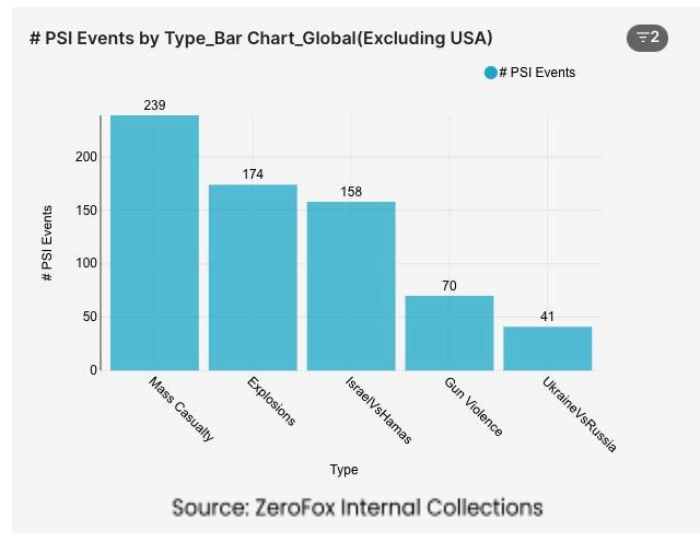
- **What this means:** On discovery of the incident, MITRE took immediate steps to contain the impact of the breach, including taking the NERVE

environment offline. It has also launched an investigation into the attack with assistance from in-house and leading third-party experts. The company has contacted relevant authorities, notified affected parties, and is working on restoring the operational activities. At the time of writing, there is no indication that MITRE's core enterprise network or partners' systems were affected by this incident. 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.

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global



What happened: Excluding the United States, there was a 25 percent increase in mass casualty events this week from the previous week, with the top contributing countries being Palestine, Ukraine, and Lebanon; notably, approximately 73 percent of these events were explosions. Additionally, alerts related to the Israel-Hamas war (including protests, raids, and involvement in neighboring countries) decreased by 37 percent. Conversely, events related to the Ukraine conflict

increased by 28 percent. The top two most-alerted subtypes were explosions, which saw a 4 percent increase from the previous week, and gun violence, which decreased by 14 percent.

- **What this means:** While the conflict in Palestine does not have a foreseeable conclusion at this time, this last week saw a decrease in alerts surrounding it. This may potentially be due to the Jewish holiday of Passover occurring this week, the recent resignation of Israeli Maj. Gen. Aharon Haliva, and the military operations in Gaza slowing ahead of a possible offensive on Rafah, Palestine. Lebanon is a top contributor to mass casualty alerts due to Hezbollah's growing participation in the conflict; Hezbollah is also backed by Iran and has many more resources than Hamas. As for Ukraine, the United States recently approved USD 61 billion to be sent in aid to the country, which has notably coincided with the increase in alerts related to this conflict. Among the capabilities included in the new package are ammunition for High Mobility Artillery Rocket Systems (HIMARS), artillery rounds, RIM-7 and AIM-9M air defense missiles, Bradley Infantry Fighting Vehicles, and Stinger anti-aircraft missiles.¹

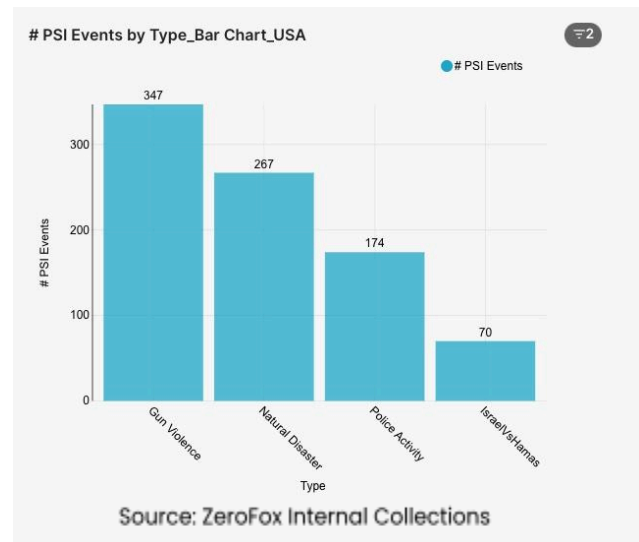
¹ <https://www.cnn.com/2024/04/24/politics/biden-signs-foreign-aid-bill/index.html>

Physical Security Intelligence: United States

What happened: In the past week, the top three most-alerted incident subtypes were gun violence, natural disasters, and police activity; notably, these are the same top three as the week prior. Gun violence alerts are instances in which there is a confirmed or likely confirmed victim (i.e., not simply shots fired). The top two states that had the most gun violence alerts were California and Illinois, which together made up over 20 percent of this week's nationwide total. Gun violence across the United States decreased by approximately 17 percent from the week prior. As structure fires and wildfires currently fall under the natural disaster scope, the majority of natural

disasters alerted this week consist of these events. The top two contributors to the natural disaster alerts this week were Texas and California. The police activity subtype is used to alert evacuations, lockdowns, and heavy police presence for which the reason is not yet known at the time of alerting; California and Florida were the top two contributing states this week. Nationwide protest activity as a whole did not increase or decrease from the week prior, but the percentage of protests related to the conflict in Palestine increased by 57 percent, making up over one-third of all protest activity this week.

- **What this means:** For the past two weeks, ZeroFox has witnessed the same top three incident subtypes, with gun violence being the most alerted. What causes this pattern is frequently debated and, while correlation does not necessarily equal causation, areas with a larger volume of and easier access to firearms typically see higher levels of shootings.² Gun violence often occurs in major cities such as Los Angeles and Chicago, which elucidates why California and Illinois contribute a significant amount to overall gun violence instances. However, nationwide there was a decrease in gun violence instances, and, The National Weather Service earlier this week issued frost and freeze alerts for several regions of the country.³ As mentioned in the previous week's intelligence briefing, colder temperatures are correlated with less reports of crime, including shootings. Conversely, Texas and California, the top two contributors to natural disaster alerts this week, have experienced wildfires as well as structure fires, possibly due to drier climates in those particular areas. For protest activity, the drastic increase in protests regarding the



² <https://giffords.org/lawcenter/resources/scorecard/>

³ <https://www.foxweather.com/weather-news/late-season-frost-weekend-lows>

conflict in Palestine may be explained by universities such as Columbia University, New York University, and Yale University hosting protests this week, sparking controversy with regards to student arrests and threats to deploy the National Guard to subdue the demonstrators.

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%