ZEROFOX INTELLIGENCE

Brief

The Underground Economist: Volume 6, Issue 5

B-2026-02-27a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Deep and Dark Web, Threat Actor, Data Breach

February 27, 2026

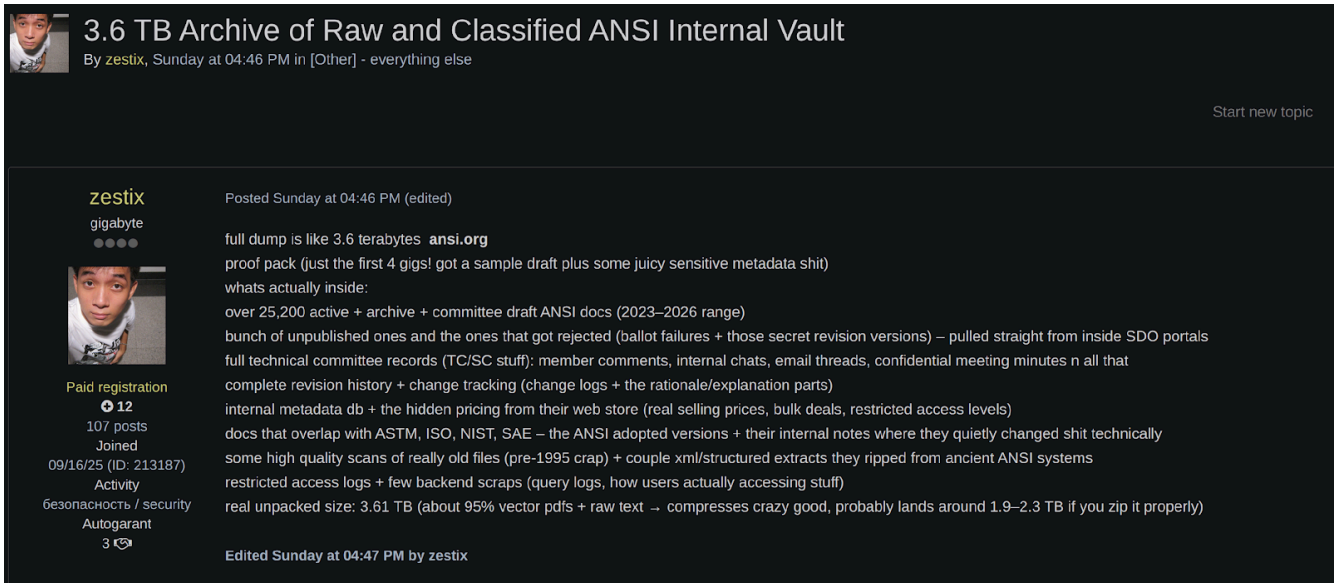
ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot 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 7:00 AM (EST) on February 26, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | The Underground Economist: Volume 6, Issue 5

| Zestix Advertises Data from ANSI

On February 22, 2026, moderately credible threat actor "zestix" advertised a 3.6 TB dataset allegedly containing raw, classified data from the American National Standards Institute's (ANSI) internal database on the dark web forum Exploit. The post has been deleted since at least February 26, indicating the threat actor likely found a buyer.

- ANSI is a U.S.-based, non-governmental organization (NGO) that oversees standards and conformity assessment activities for products, services, and personnel in the United States.
- Zestix has not publicly shared any data samples. However, they have stated they are willing to share a 4 GB sample with any interested buyer.
- The actor joined Exploit in September 2025 and has a favorable reputation, with 107 posts, 12 positive reactions, and at least one completed escrow-backed transaction. Escrow is used on dark web forums to ensure payment and reduce fraud risks.



zestix's advertisement on Exploit
Source: ZeroFox Intelligence

Zestix claims the data bundle contains standardization intelligence and strategic data, including over 25,200 active archives from 2023 to 2026, rejected drafts, and organizational metadata. Because industrial standards take years to update, this leaked information is likely still relevant and actionable.

- The standardization data supposedly includes regulatory documents with requirements, test methods, or terminologies derived from standards established by standards development organizations, including ANSI-adopted versions, along with internal technical notes.
- The metadata allegedly contains hidden pricing information from ANSI's web store, including actual selling prices, bulk agreements, and restricted access levels.

The rejected drafts, metadata, and standards-related documents are likely to enable financially motivated actors to orchestrate several types of cyberattacks, to include supply-chain compromise, zero-day attacks, and persistent social engineering campaigns.

- Access to internal metadata and restricted access logs would likely reveal details about vendors and other downstream companies. A buyer is likely to use this information to infect a sub-tier supplier's network with a malware payload disguised as a "confidential revision update."

There is a roughly even chance of threat actors reviewing the rejected drafts or active archives, detecting any compromise in standards, and thereafter weaponizing it as a vulnerability. Given zestix's reputation and the likelihood that the dataset was sold within a few days, the seller's claims are likely legitimate.

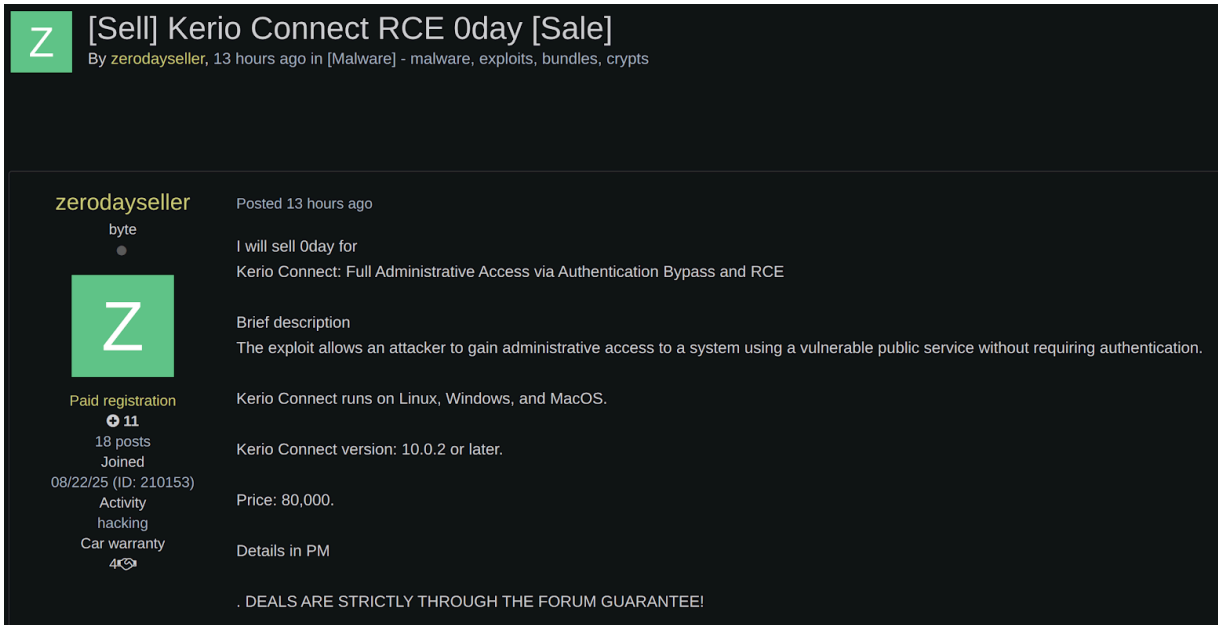
Kerio Connect Zero-Day Allegedly for Sale on Exploit

On February 18, 2026, credible actor "zerodayseller" advertised the sale of a zero-day exploit affecting Kerio Connect on the dark web forum Exploit. According to the seller, the zero-day vulnerability enables full administrative access through authentication bypass combined with remote code execution; the listed price is USD 80,000.

- Kerio Connect is a widely deployed email and collaboration platform developed by GFI Software and used by more than 30,000 companies globally—meaning this vulnerability, if legitimate, would almost certainly impact millions of users.
- The exploit allegedly affects Kerio Connect versions on Linux, Windows, and MacOS systems; the threat actor claims that version 10.0.2 and newer are affected.

In the post, zerodayseller stated that details (likely technical details of the alleged zero-day exploit and how to deploy it) are available through private messaging. This is a typical seller procedure observed on dark web forums—very likely to aid operational security and filter out unserious buyers.

- The actor is considered a vetted seller of zero-day vulnerabilities and exploits on the Exploit forum, which will almost certainly increase the perceived legitimacy of the offer.



zerodayseller's post on Exploit
Source: ZeroFox Intelligence

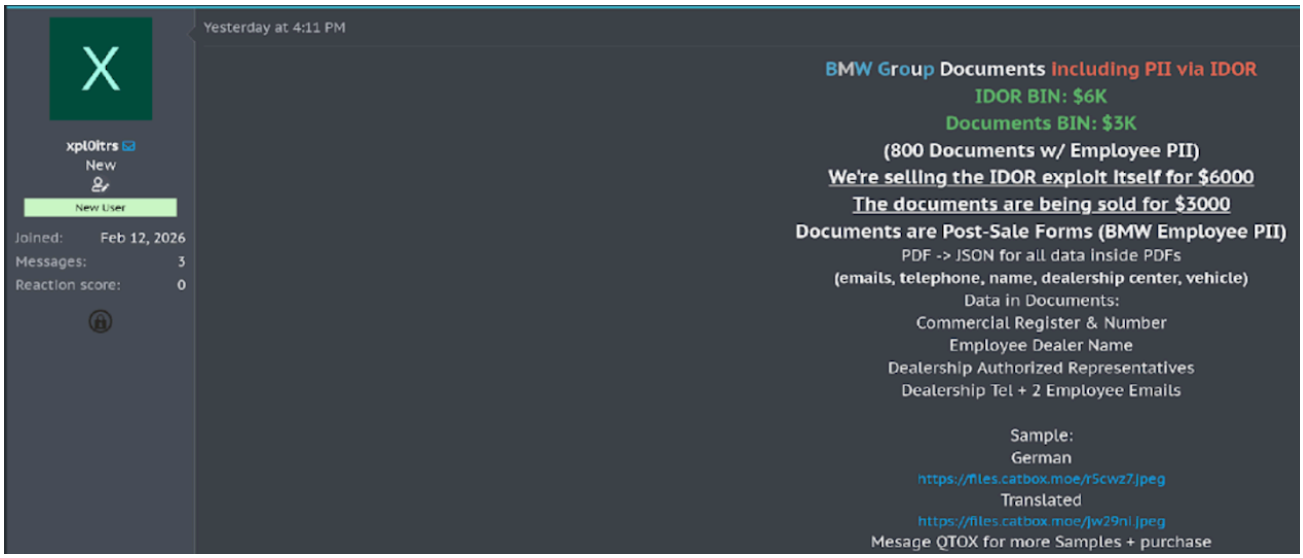
If the zero-day exploit proves legitimate, such a vulnerability would very likely impact a large number of organizations, as attackers can obtain full administrative access in Kerio Connect. This would almost certainly allow for persistent presence in a target network, which would very likely lead to exploitation of email accounts and almost certainly result in significant exposure of corporate data.

Threat Actor Advertises BMW-Related PII and Web Application Exploit

On February 17, 2026, newly registered and untested threat actor "xpl0itrs" advertised 800 leaked documents related to BMW Group and an insecure direct object reference (IDOR) exploit on the Russian and English-language dark web forums Rehub and DarkForums. The documents are priced at USD 3,000, and the exploit is advertised for USD 6,000. The actor claims to have accessed the documents using the IDOR exploit.

- IDOR is a web application flaw that enables attackers to access unauthorized data by modifying parameters due to missing or improper authorization checks.

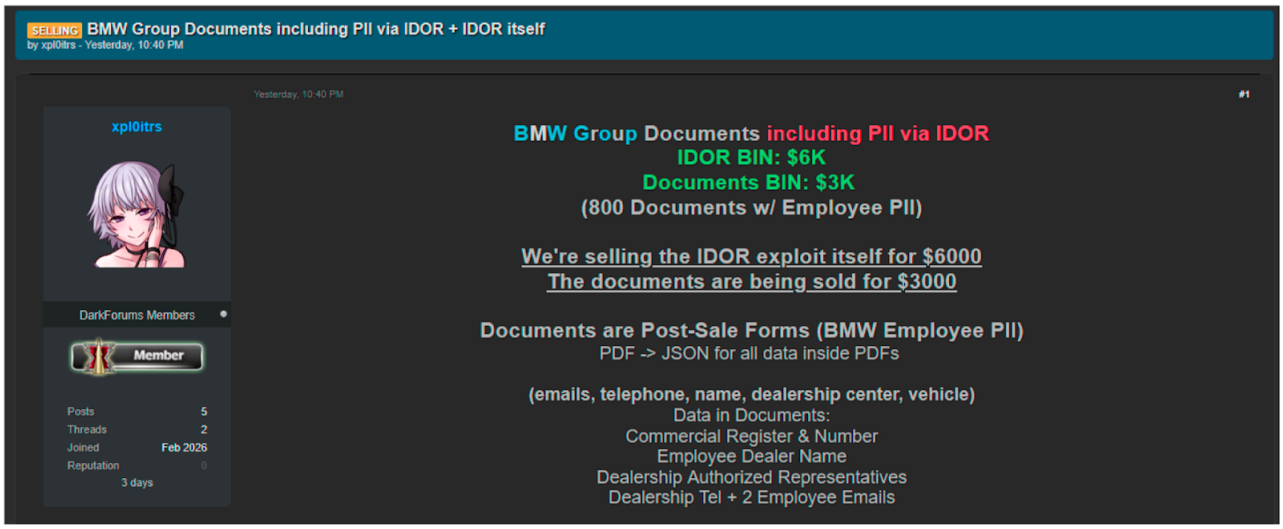
- BMW has not officially confirmed an IDOR-related vulnerability or any breach at the time of writing.
- The actor joined ReHub and DarkForums in February 2026 and has a reaction score of zero on both platforms.



xpl0itrs' advertisement on ReHub
Source: ZeroFox Intelligence

In the post, xpl0itrs provided two links to the documents (one in the original German and the other translated to English), but they were not functional at the time of writing. It is very likely that the original documents were translated to English to appeal to a wider audience of threat actors.

- BMW Group is a German multinational automotive manufacturer that provides premium vehicle manufacturing, financial services, and connected-car digital services, among other services.



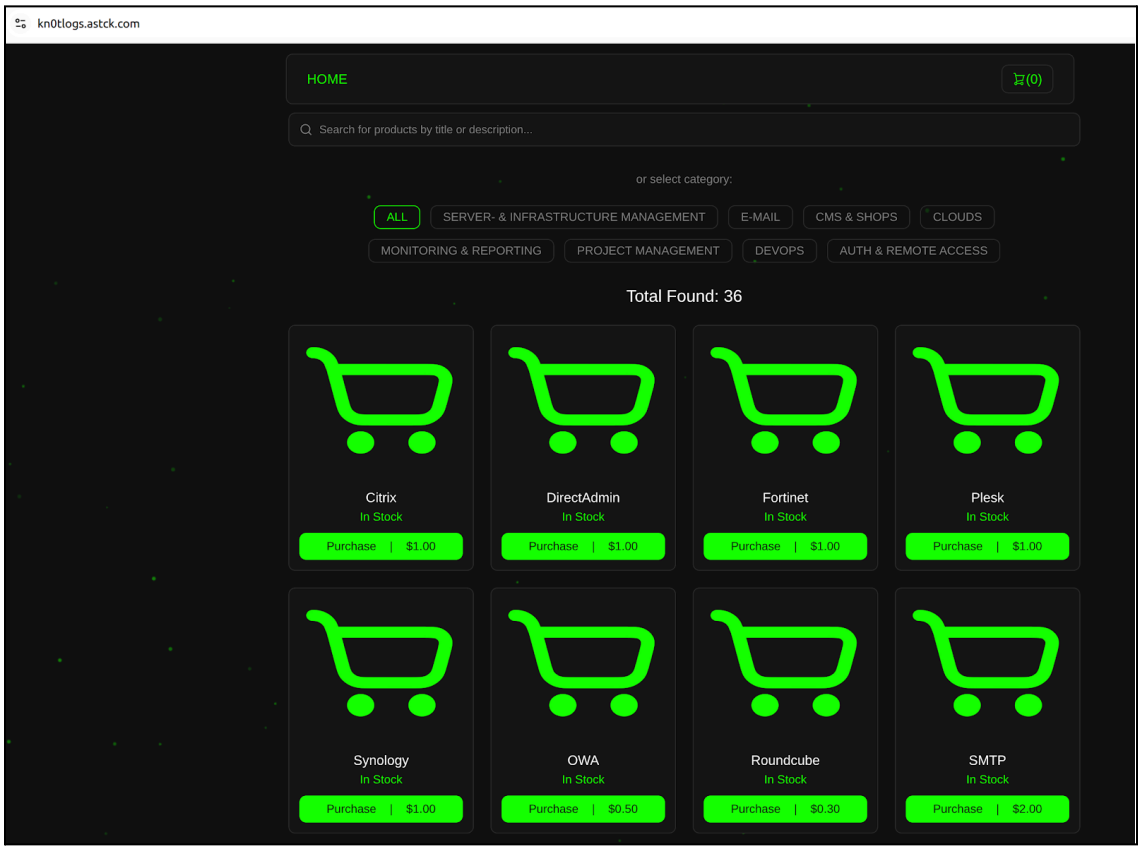
xpl0itrs's advertisement on DarkForums
Source: ZeroFox Intelligence

According to the actor's advertisement, the documents include post-sale PDF forms containing BMW Group employees' personally identifiable information (PII), such as names, email addresses, and phone numbers, as well as other data about dealership centers, commercial registration information, authorized representatives, and dealer contact information. If the actor's claims are true, the documents are likely to give buyers enough information to carry out convincing business email compromises, create relevant phishing lures, pose as customer support, and utilize other social engineering tactics to gather information about intellectual property, PII, and corporate data to sell on dark web forums. The exploit likely lowers the barrier to entry for opportunistic actors to conduct scalable, automated data harvesting. Multiple buyers can reuse the same exploit simultaneously, multiplying its impact.

Announcement of New Infostealer Log Online Store

On February 15, 2025, a newly registered, positively trending threat actor known as "CapitalAA" announced a new online shop offering infostealer log data at hXXps://kn0tlogs.astck[.]com on the dark web forum Exploit. The actor included thousands of free URL:login:password (ULP) entries in the post, likely in an effort to build a legitimate reputation as a botnet log-derived information seller.

- The shop offers logs at prices ranging from USD 0.30–USD 2 per entry, with each including the full ULP.



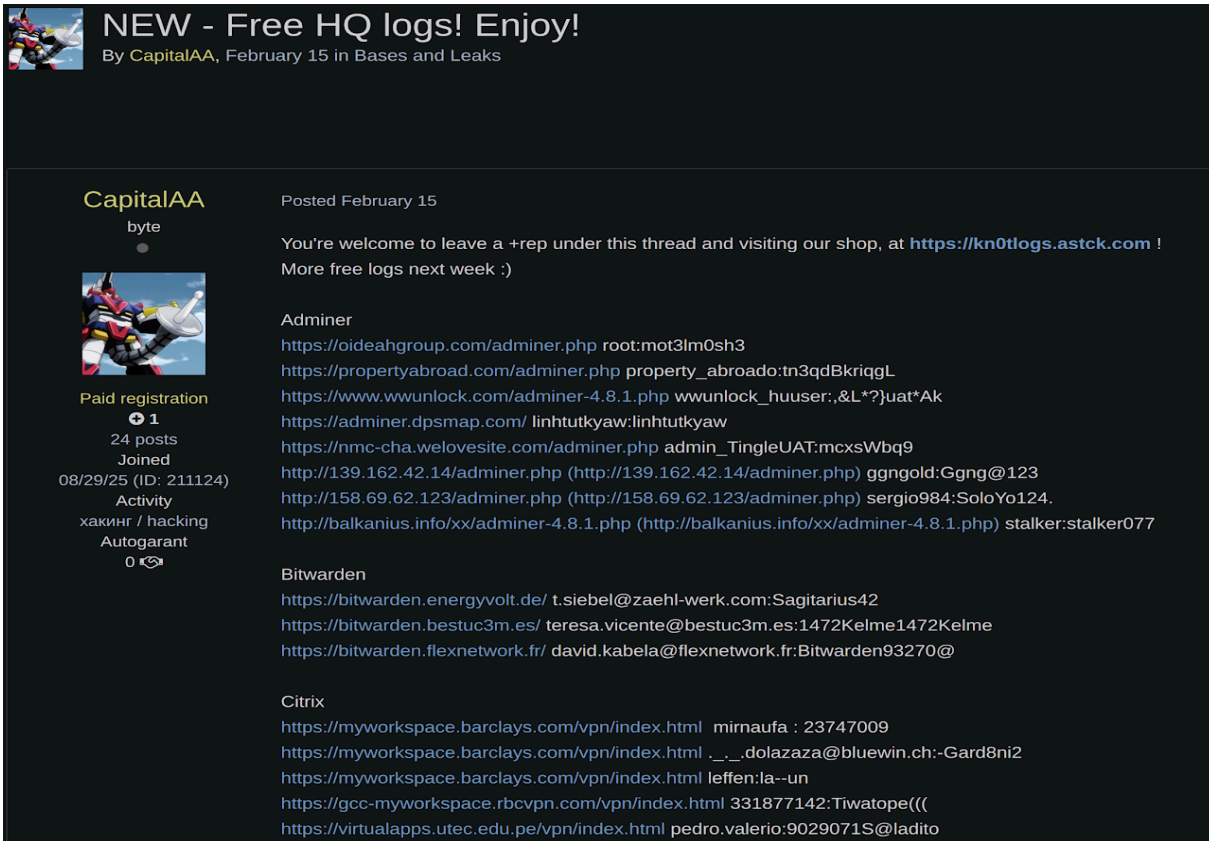
Front page of CapitalAA's log market, hXXps://kn0tlogs.astck[.]com
Source: ZeroFox Intelligence

CapitalAA compiled all of the compromised accounts by the specific web services and service types the credentials supposedly belong to—likely to enable buyers to easily find and purchase access to the particular systems in which they are interested. The actor also divided the logs by perceived importance, primarily focusing on credentials related to infrastructure accounts.

- ZeroFox observed the following services and categories within the shop: Adminer, Bitwarden (password vault logins), cPanel (web hosting control panels), Citrix (remote access environments), Confluence, DirectAdmin, Fortinet and GlobalProtect (VPN access portals), FTP, GitLab (code repository accounts), Grafana, Guacamole, Jenkins, Jira (project management systems), Joomla,

Kibana, Magneto, Metabase, NextCloud, Odoo, SSH, Synology, WordPress (website administrator logins), and Zabbix.

- All of the logs are further segmented into eight different categories: server and infrastructure management, e-mail, CMS and shops, web clouds, monitoring and reporting, project management, DevOps, and authentication and remote access.



CapitalAA's post on Exploit
Source: ZeroFox Intelligence

CapitalAA joined the Exploit forum on August 29, 2025; the actor has made 24 posts and garnered at least one positive reaction score. While this does not significantly impact ZeroFox's determination of actor legitimacy, it does indicate that CapitalAA is positively trending on the forum to date.

- The actor's offer of free ULPs and apparent efforts to categorize the data by importance are very likely aimed towards professionalizing and organizing their online shop and services.

Posts such as these demonstrate the evolving dynamics of the cybercriminal underground ecosystem, where fraudsters and attackers can gain facilitated access to numerous resources that are likely to lead to the compromise of victims' infrastructure or be used in large-scale fraud campaigns.

Similar to other marketplaces on the deep and dark web (DDW), CapitalAA's platform also provides replacements for invalid credentials. Although the exploitation of credentials obtained from botnet logs is not new, ZeroFox assesses that the operators of this service have likely established an account-checking infrastructure to verify the validity of the aforementioned web resources.

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Implement secure password policies, phishing-resistant multi-factor authentication (MFA), and unique credentials.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in DDW forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).

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%