ZEROFOX INTELLIGENCE

Brief

The Underground Economist: Volume 6, Issue 9

B-2026-04-23b

Classification: TLP:CLEAR

Criticality: LOW

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

April 23, 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 (EDT) on April 23, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | The Underground Economist: Volume 6, Issue 9

| ShinyHunters Discloses Database with Anonymous Users' Records from DarkForums

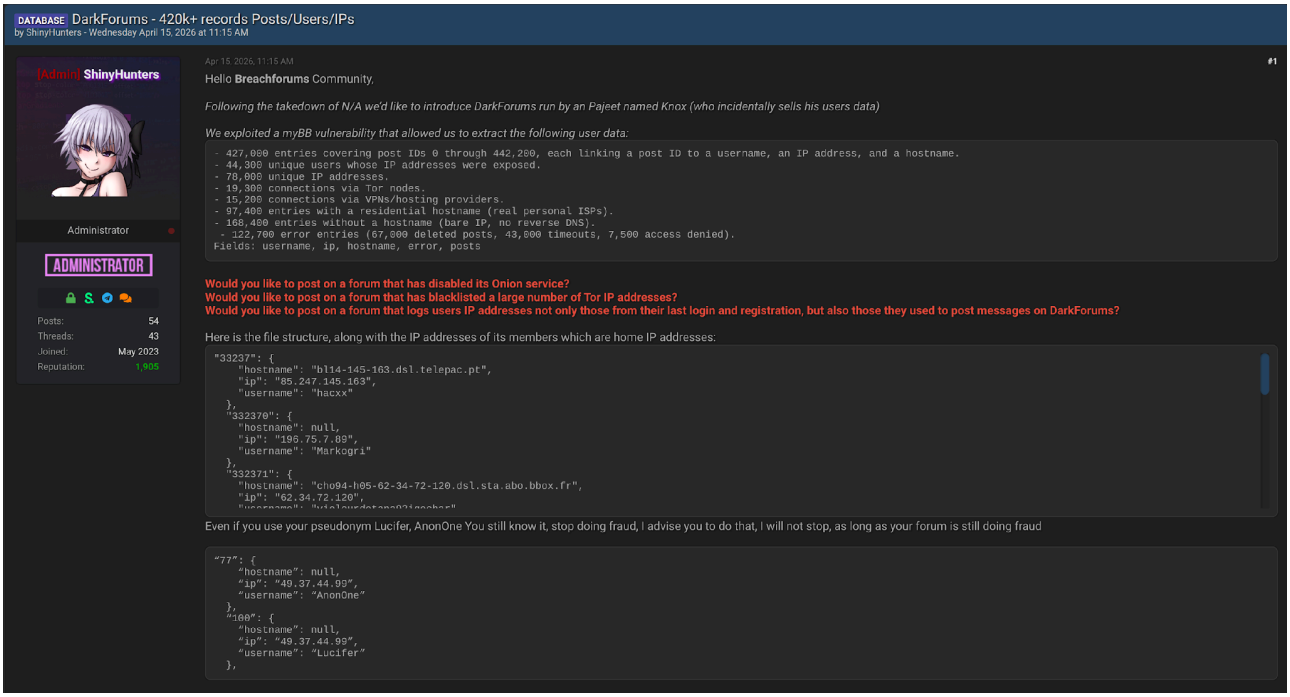
On April 15, 2026, the established and high-profile data breach collective ShinyHunters (which operates the dark web forum BreachForums and its associated clearnet leak site) disclosed an alleged database of its competitor, DarkForums. The actors claimed to have gained access to the database by exploiting a myBB vulnerability, which allegedly led to the extraction of nearly one million private records of DarkForums' anonymous users.

- DarkForums was created after disruptions and the alleged law enforcement (LE) seizure of BreachForums throughout 2025. It was designed nearly identically to BreachForums and very likely intended to serve as its replacement.
- DarkForums subsequently gained popularity and absorbed a significant amount of BreachForums' users, making these forums direct competitors with similar illicit offerings.

The DarkForums database leaked by ShinyHunters includes:

- 427,000 entries with post IDs (each with a link to a post, username, IP address, and hostname)
- 44,300 unique users whose IP addresses were exposed

- 78,000 unique IP addresses
- 19,300 connections via Tor nodes
- 15,200 connections via VPNs /hosting providers
- 97,400 entries with a residential hostname (real personal ISPs)
- 168,400 entries without a hostname (bare IP, no reverse DNS)
- 122,700 error entries (67,000 deleted posts, 43,000 timeouts, 7,500 access denied)



ShinyHunters' post on BreachForums

Source: ZeroFox Intelligence

ShinyHunters claimed they conducted this attack against DarkForums because DarkForums' owner (who is known as "Knox", "Lucifer", and "AnonOne") is committing fraud. ShinyHunters stated they would continue to target Knox for as long as DarkForums is involved in fraudulent activity.

- ZeroFox assesses that ShinyHunters' accusation against DarkForums' administrator is likely in retaliation for abusing their position by scamming DarkForums community members and selling false data under fake usernames.

This is not the first time that rival forum owners or administrators have attacked each other; in January 2026, a disgruntled self-described "legendary hacker" who claimed to have mentored several collectives, including ShinyHunters, published a database with over 300,000 records exposing BreachForums users.[1] DarkForums was created after a LE seizure of BreachForums, and it was designed nearly identically to BreachForums to serve as its replacement.

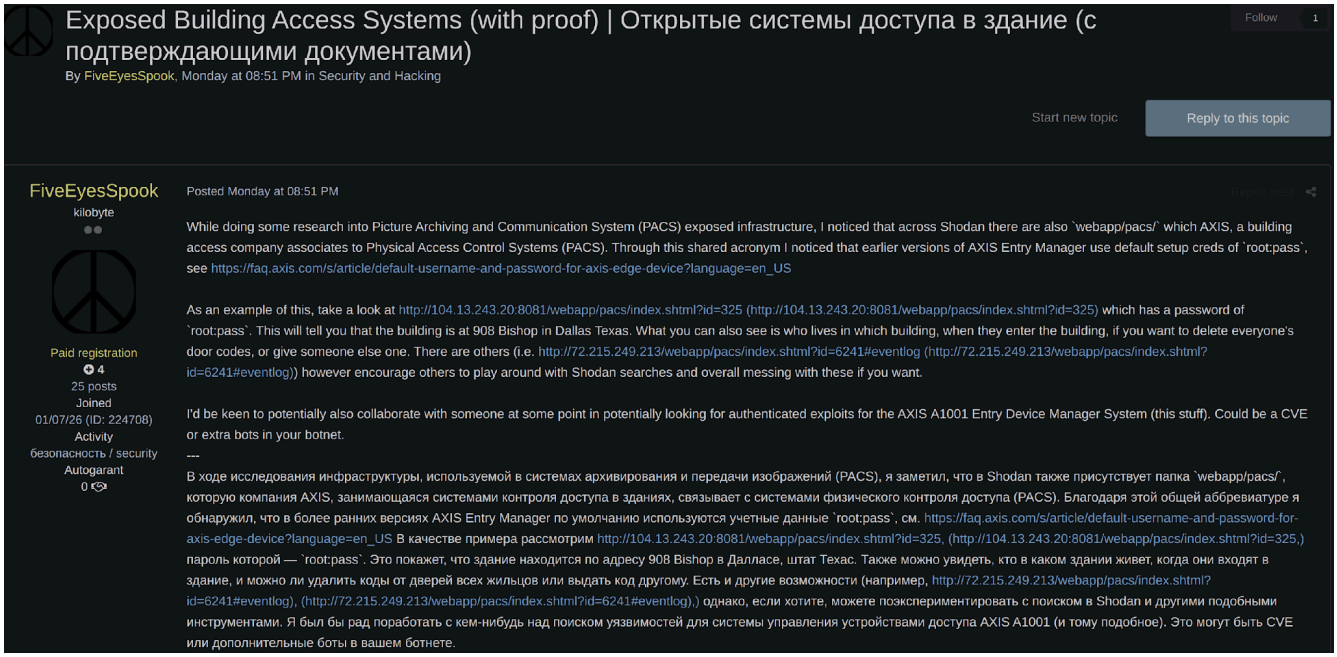
These two forums, and their respective operators, will very likely continue to engage in exfiltrating and releasing each other's data. This is likely to backfire, as such data can be used by LE to locate and disrupt actors' illicit operations, ultimately degrading these forums' credibility and anonymity.

FiveEyesSpook Reveals Publicly Exposed Building Access Controls

On April 13, 2026, untested threat actor "FiveEyesSpook" posted on the dark web forum Exploit, claiming access to multiple internet-exposed systems in buildings running AXIS Entry Manager using default credentials. The actor is soliciting collaboration to further investigate the company's systems and identify potential vulnerabilities, including authenticated exploits, in the AXIS A1001 Entry Manager system.

- Axis Communications is a Sweden-based company that specializes in intelligent security solutions and manufactures IP-based network cameras, surveillance software, access control systems, intercoms, and audio devices used for security.
- Axis Communications sells AXIS Entry Manager, an IP-based physical access control software that manages physical access control systems (PACS)—systems that control and monitor who can physically enter a building or restricted area using doors, keycards, PIN codes, and entry logs.

[1] hXXps://www.darkreading[.]com/threat-intelligence/breachforums-breached-exposing-324k-cybercriminals

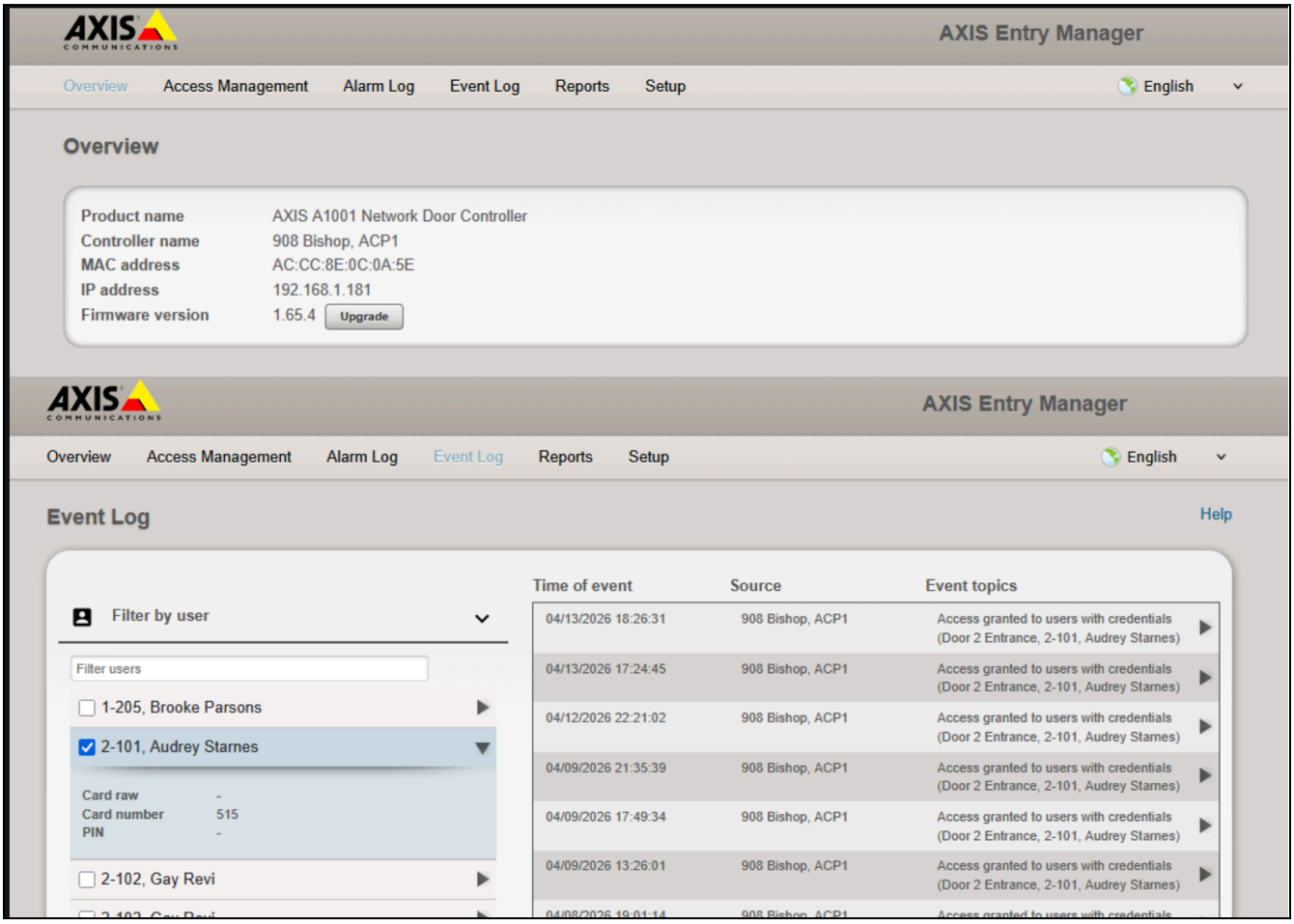


FiveEyesSpook's post on Exploit about exposed building access

Source: ZeroFox Intelligence

According to FiveEyesSpook, they used Shodan to identify internet-exposed AXIS Entry Manager interfaces associated with PACs. They then gained access by logging in with publicly documented default credentials.

- The actor claims they were able to access sensitive information such as building details, resident/user data, and entry logs, potentially allowing them to modify or control door access.



FiveEyesSpook's access to Axis Entry Manager

Source: ZeroFox Intelligence

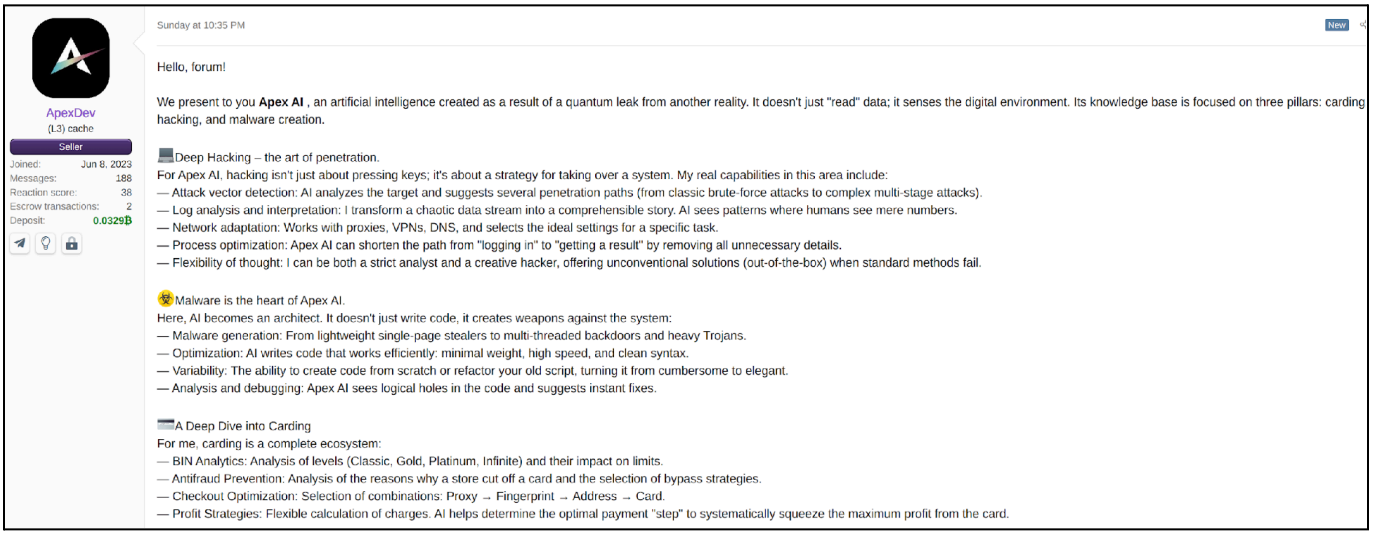
FiveEyesSpook is likely looking for a deeper and wider range of access than they were able to achieve using Shodan. By collaborating with and leveraging others' expertise to identify loopholes in AXIS Entry Manager and scale exploitation beyond opportunistic exposure, the actor is likely seeking more sustained access.

Sustained access, if secured, is likely to enable the actor and other possible collaborators to view users' names and entry logs, as well as delete or reassign door access codes, granting control over building entry systems. Such exposure is likely to compromise sensitive residential or workplace information and pose significant physical security risks for occupants in buildings using AXIS Entry Manager.

Multifunctional AI-Based Hacking Tool Advertised on Dark Web

On April 12, 2026, positively trending threat actor "ApexDev" advertised a new artificial intelligence (AI) tool called Apex AI on the Russian-language dark web forum XSS. The tool—touted to be an unrestricted AI system designed to support illicit activity like carding, hacking, and malware development—was set to be released on April 20.

- Apex AI is allegedly a multifunctional tool intended to assist with offensive operations, including system intrusion, malware creation, and carding-related workflows.
- ApexDev claims the software was built using multiple large language models (LLMs), but it is not based on the leaked Claude Code Agent AI.
- While there have been several recent examples of unrestricted LLM-enabled tools marketed for fraudulent or malicious use, Apex AI allegedly combines three capabilities in a single offering.



ApexDev's post on XSS
Source: ZeroFox Intelligence

ApexDev emphasizes the tool's multifaceted functions (including automated analysis, code generation, and workflow optimization) in the advertisement to frame it as an all-in-one platform for cybercrime operations.

- The actor claims the tool can analyze targets, suggest penetration paths, interpret logs, and optimize network configuration for proxy, VPN, and DNS use.
- Apex AI is also allegedly an automated development assistant capable of generating stealers, backdoors, and Trojans, as well as debugging and refactoring code.
- As for its carding capabilities, the actor describes Apex AI as a complete ecosystem covering BIN analysis, antifraud bypass, checkout optimization, and profit calculation.

If ApexDev's claims are accurate, there is a roughly even chance of Apex AI lowering the skill threshold for actors seeking to conduct fraud, develop malicious code, and operationalize stolen payment data at scale. A tool that combines these capabilities is likely to enable less sophisticated actors to shift rapidly from reconnaissance to execution.

- The tool is very likely to gain traction with amateur, financially motivated threat actors, who do not have high technical expertise and are looking for a tool to quicken and scale-up their efforts.
- It is unlikely to attract more experienced actors, who typically exercise more caution in purchasing tools. However, if ApexDev can prove the tool's capabilities, experienced actors are likely to leverage it to automate repetitive tasks and increase throughput.
- Given ApexDev's moderately high reputation score after three years in the forum, it is likely that the tool exists and the advertisement will draw interest.

However, as of writing, the threat actor has not yet published any proof of the tool's release or effectiveness, which is a likely indication that its capabilities have been exaggerated.

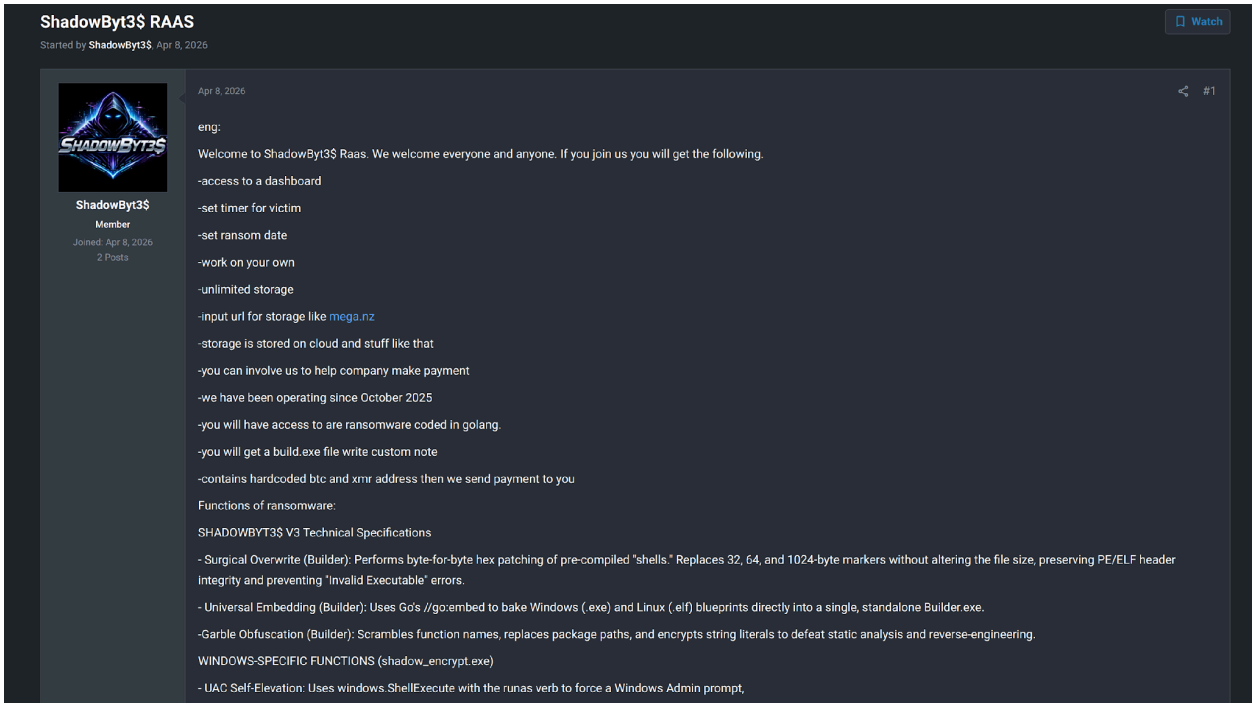
New Version of ShadowByt3$ RaaS Advertised

On April 8, 2026, an untested actor using the alias “ShadowByt3$” announced a new version of the ransomware-as-a-service (RaaS) platform ShadowByt3$ on the dark web forum TierOne. The new version is dubbed V3 and reportedly shares similarities with LockBit and BlackCat RaaS projects, although enough differences remain that ZeroFox considers ShadowByt3$ a unique RaaS threat.

- ShadowByt3$ was previously advertised on the seized RAMP dark web forum.

The latest build has a sophisticated architecture likely intended to maintain persistence in a target network and avoid detection by security measures. Some of the specific features of ShadowByt3$ V3 include:

- Surgical Overwrite: A highly advanced evasion technique, it replaces internal markers (like Affiliate IDs) without changing the file size or the executable's headers, preventing "Invalid Executable" errors that often tip off security software.
- 60MB Binary Bloat: Purposely appends junk data to exceed network scan size limits, triggering a "timeout" bypass that allows the malware to run unscanned and avoid forensic detection.
- The Melt: Hinders post-attack investigation by spawning a background process that waits a few seconds after encryption is finished to permanently delete the original executable from the disk, leaving investigators with no binary to analyze.
- Universal Embedding: Uses a feature to store both Windows (.exe) and Linux (.elf) blueprints inside a single "Master Builder" file. This allows an attacker to generate payloads for any operating system from one interface.
- Garble Obfuscation: "Scrambles" the code's internal logic, replacing package paths and encrypting text, which defeats "Static Analysis"—the method security researchers use to read the code without running it.



Original post on TierOne forum

Source: ZeroFox Intelligence

Additionally, the latest version of ShadowByt3$ moves beyond simple file-locking and targets the heart of the victim's business. This is accomplished by explicitly shutting down the target network's ability to run virtual machines, killing enterprise databases such as SQL and sabotaging the network's data recovery apparatus.

The scale of attacks associated with this RaaS platform have thus far been relatively insignificant. However, with the release of the latest version, there will very likely be a notable increase in attacks from ShadowByt3$ and its affiliates.

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 deep and dark web (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%

Appendix C: ZeroFox Intelligence Threat Actor Reputation Scale

Untested	Moderately Credible	Well-regarded	Prominent
Has garnered no reputation; credibility cannot be determined.	Has made up to 10 transactions; has been active on forum for at least three months.	Has at least 10 transactions; has been active on forum for three months to one year.	One of the most well-known and credible threat actors on the site; long-term, established presence on the forum of more than one year.