ZEROFOX INTELLIGENCE

Brief

The Underground Economist: Volume 6, Issue 13

B-2026-06-19a

Classification: TLP:CLEAR

Criticality: LOW

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

June 19, 2026

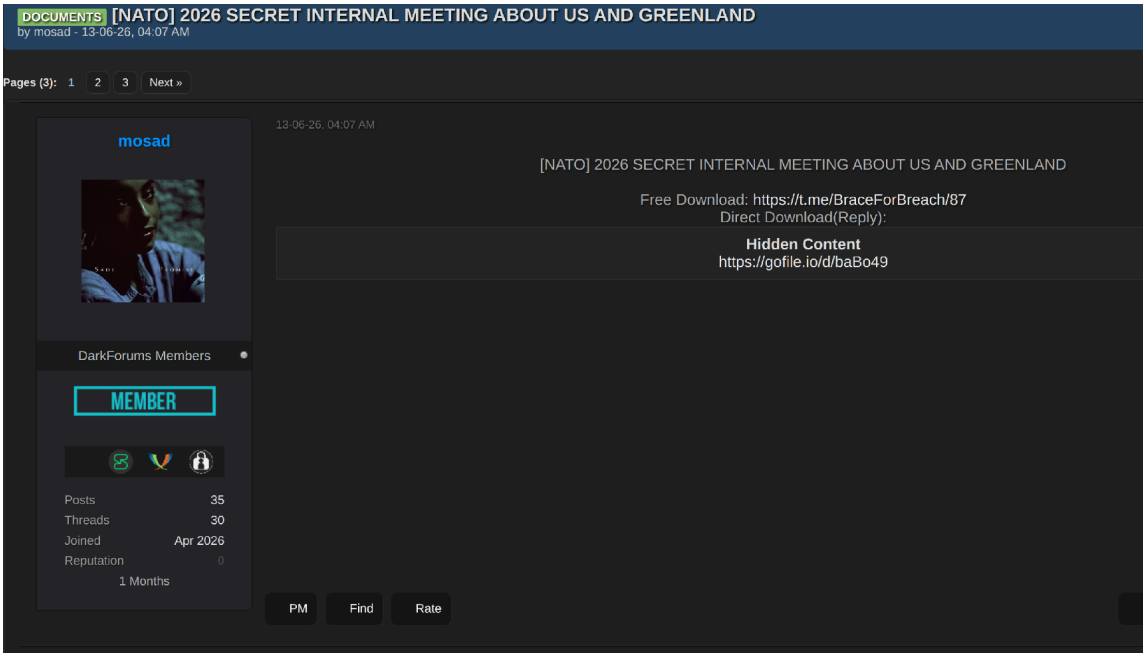
ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot 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 June 19, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | The Underground Economist: Volume 6, Issue 13

| Alleged NATO Greenland Meeting Document Shared on DarkForums

On June 13, 2026, untested threat actor "mosad" shared a PDF document on the dark web forum DarkForums that allegedly originated from a North Atlantic Treaty Organization (NATO) internal meeting held in 2026 concerning Greenland. The contents ZeroFox reviewed suggest there is a roughly even chance that the document is associated with the U.S.–Denmark talks about Greenland held in early 2026.

- The PDF includes information about alleged European Union (EU) security assistance measures and strategic considerations related to Greenland.
- The document contains details regarding alleged internal discussions, assessments, probable policies, attendees, and meeting agenda points.

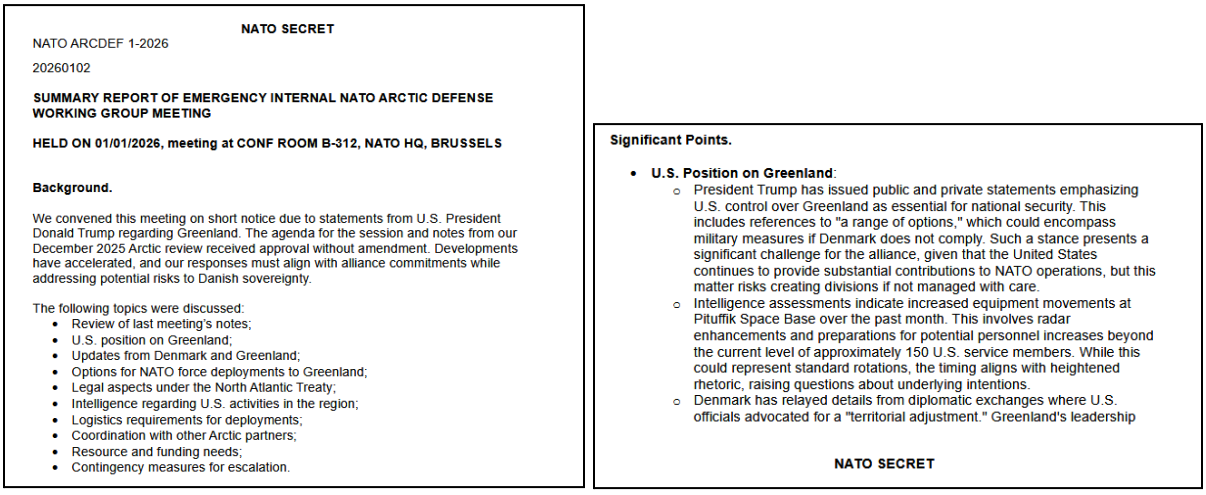


mosad's advertisement on DarkForums

Source: ZeroFox Intelligence

Mosad's post does not include details about how the document was obtained and provides no further evidence that the document is authentic, nor does it include any amplifying information to substantiate the claim it originates from NATO channels. At the time of writing, ZeroFox cannot independently verify the authenticity or origin of the document.

- Greenland is an autonomous territory within the Kingdom of Denmark and is strategically important in the Arctic region because it houses the Pituffik Space Base, a vital American military base that facilitates space monitoring and NATO missile defense operations.



NATO SECRET

NATO ARCDEF 1-2026

20260102

SUMMARY REPORT OF EMERGENCY INTERNAL NATO ARCTIC DEFENSE WORKING GROUP MEETING

HELD ON 01/01/2026, meeting at CONF ROOM B-312, NATO HQ, BRUSSELS

Background.

We convened this meeting on short notice due to statements from U.S. President Donald Trump regarding Greenland. The agenda for the session and notes from our December 2025 Arctic review received approval without amendment. Developments have accelerated, and our responses must align with alliance commitments while addressing potential risks to Danish sovereignty.

The following topics were discussed:

- Review of last meeting's notes;
- U.S. position on Greenland;
- Updates from Denmark and Greenland;
- Options for NATO force deployments to Greenland;
- Legal aspects under the North Atlantic Treaty;
- Intelligence regarding U.S. activities in the region;
- Logistics requirements for deployments;
- Coordination with other Arctic partners;
- Resource and funding needs;
- Contingency measures for escalation.

Significant Points.

- **U.S. Position on Greenland**:
  - President Trump has issued public and private statements emphasizing U.S. control over Greenland as essential for national security. This includes references to "a range of options," which could encompass military measures if Denmark does not comply. Such a stance presents a significant challenge for the alliance, given that the United States continues to provide substantial contributions to NATO operations, but this matter risks creating divisions if not managed with care.
  - Intelligence assessments indicate increased equipment movements at Pituffik Space Base over the past month. This involves radar enhancements and preparations for potential personnel increases beyond the current level of approximately 150 U.S. service members. While this could represent standard rotations, the timing aligns with heightened rhetoric, raising questions about underlying intentions.
  - Denmark has relayed details from diplomatic exchanges where U.S. officials advocated for a "territorial adjustment." Greenland's leadership

NATO SECRET

Samples from the document uploaded by mosad

Source: ZeroFox Intelligence

Mosad joined DarkForums in April 2026 and has since created 35 posts but has garnered no reputation points as of writing. Given mosad's reputation on the forum and the lack of substantial evidence to support their claims, it is likely the document contains very basic information rather than sensitive or confidential data. The content likely primarily comprises publicly available data released via press conferences or other media sources.

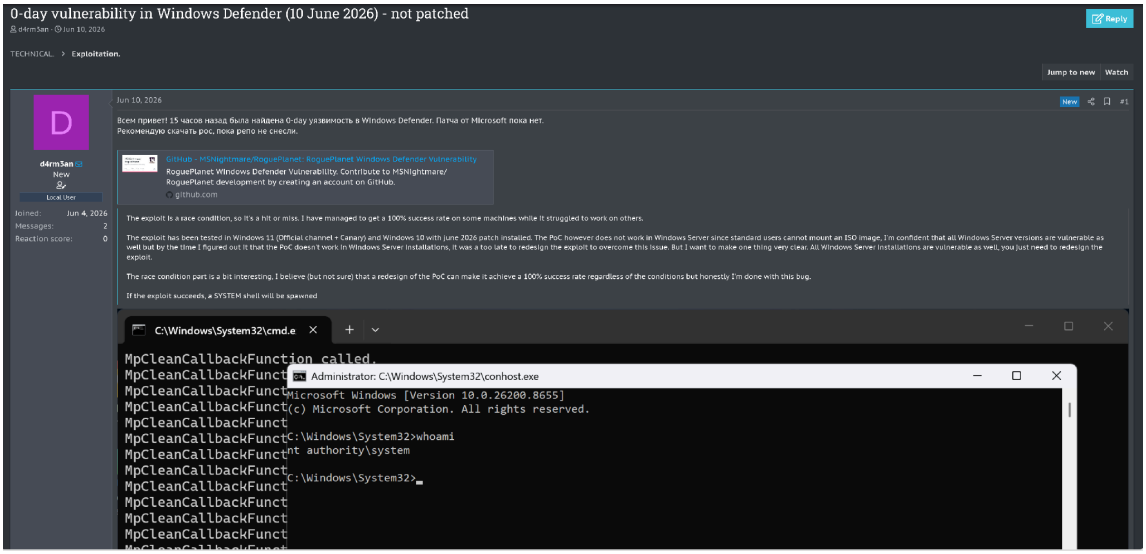
- ZeroFox observed that the pages of the document do not carry an official signature, emblem, or label to indicate its authenticity.
- Some of the information is likely fabricated and designed to attract politically motivated actors or state-nexus actors, who generally seek strategic data that favors their nation-state in the geopolitical landscape.

Unpatched Windows Defender Vulnerability

On June 10, 2026, an untested threat actor using the alias "d4rm3an" on the ReHub dark web forum claimed to have identified an unpatched vulnerability affecting Windows Defender. The actor shared a proof-of-concept (PoC) exploit through a GitHub repository and encouraged other users to download it before its potential removal.

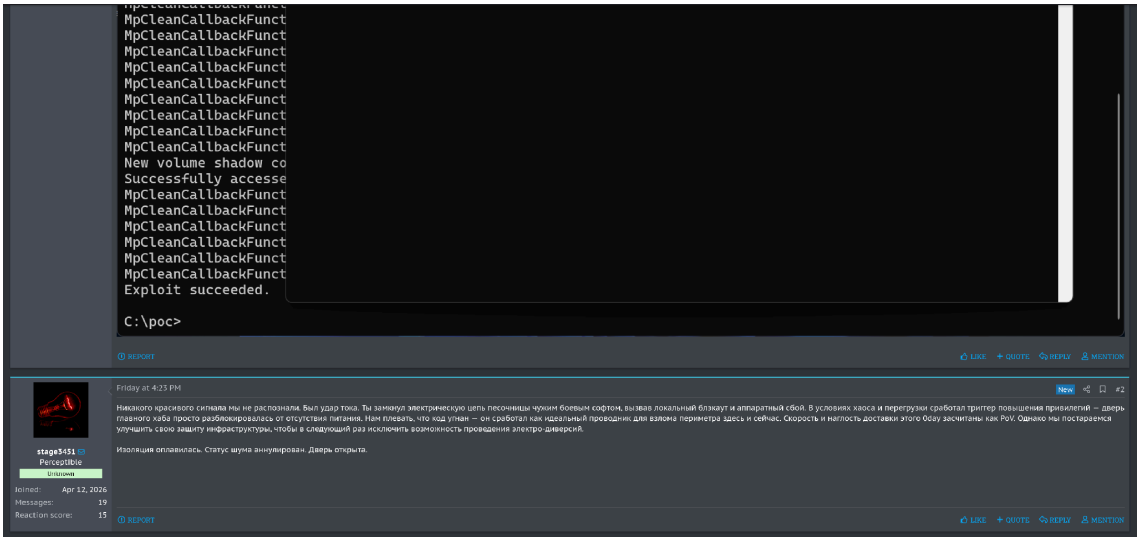
According to d4rm3an's advertisement, the exploit demonstrated varying success rates across targeted systems. The actor stated that testing achieved a 100 percent success rate on certain target machines, while other systems were not successfully compromised.

- Tests were allegedly run against Windows 11 and Windows 10 systems that had already completed the June 2026 security updates.
- The Proof of Concept (PoC) did not function on Windows Server environments, likely because standard users are unable to mount ISO files by default. The actor indicated uncertainty regarding the vulnerability's impact across all Windows Server versions, noting that the exploit was not redesigned to address this limitation.



Original post on ReHub
Source: ZeroFox Intelligence

Another forum user, "stage3451," responded to the discussion and questioned d4rm3an's characterization of the vulnerability, stating that the described technique appeared to involve a breakdown of isolation boundaries rather than a sophisticated covert channel or intentionally designed exploitation mechanism.



Comment from stage3451
Source: ZeroFox Intelligence

Although ZeroFox has not independently validated the exploit methodology and vulnerability details, the continued availability of the PoC very likely presents a significant risk to Windows environments. Organizations using affected Windows versions should monitor for further analysis, vendor updates, and potential exploitation attempts.

Purported List of Iranian Operatives in Gulf States

On June 10, 2026, a well-regarded actor using the alias “SebastianDAlex” advertised a dataset for sale on the Exploit dark web forum that allegedly contains information about 26,300 individuals described as Iranian spies operating in Gulf countries. According to the seller, these individuals are located in Qatar, Bahrain, Saudi Arabia, the United Arab Emirates (UAE), Oman, and Iraq. The complete dataset is being offered for USD 11,000.

SebastianDAlex claims the subjects included in the database are individuals affiliated with both the Islamic Revolutionary Guard Corps (IRGC) and the Iranian Ministry of Intelligence and Security (MOIS). According to the advertisement, the dataset includes the following information:

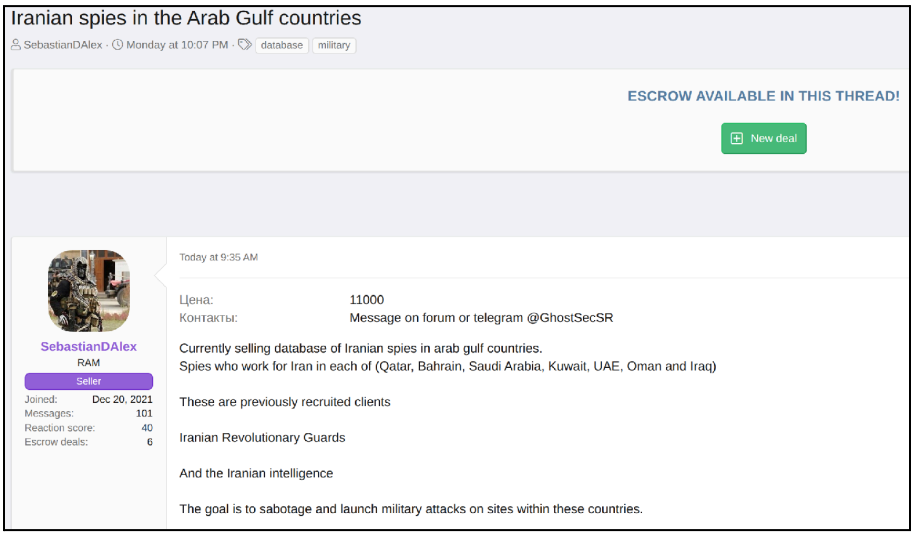
- Full names and titles

- Unique or serial identifiers (likely service numbers, government ID numbers, or the like)
- Mothers' names
- Phone numbers
- Organizational affiliations
- Detailed mission or operational locations (very likely a reference to the associated Iranian embassy or consulate)
- Purpose of presence or assignment
- Year of birth
- Place of birth
- Residence information

Based on the actor's description, the primary objective of the alleged operatives is almost certainly to conduct sabotage activities and facilitate military attacks against targets within the listed countries.

- Given the alleged activities of the supposed dataset subjects, ZeroFox assesses that references to the IRGC are very likely meant to indicate the IRGC's Qods Force (IRGC-QF), the IRGC unit responsible for operations outside of Iran.[1]

[1] hXXps://www.cfr[.]org/backgrounders/irans-revolutionary-guards



SebastianDAlex's post on Exploit
Source: ZeroFox Intelligence

The seller has vetted status on the forum, which likely increases the credibility of the advertised dataset; the source of the data has not been disclosed. There is a roughly even chance that insiders were the source of the alleged leak.

ZeroFox further assesses that, if the dataset is authentic, it is almost certainly significantly undervalued given its potential intelligence value and the possible implications for ongoing geopolitical tensions and security concerns within the Gulf region.

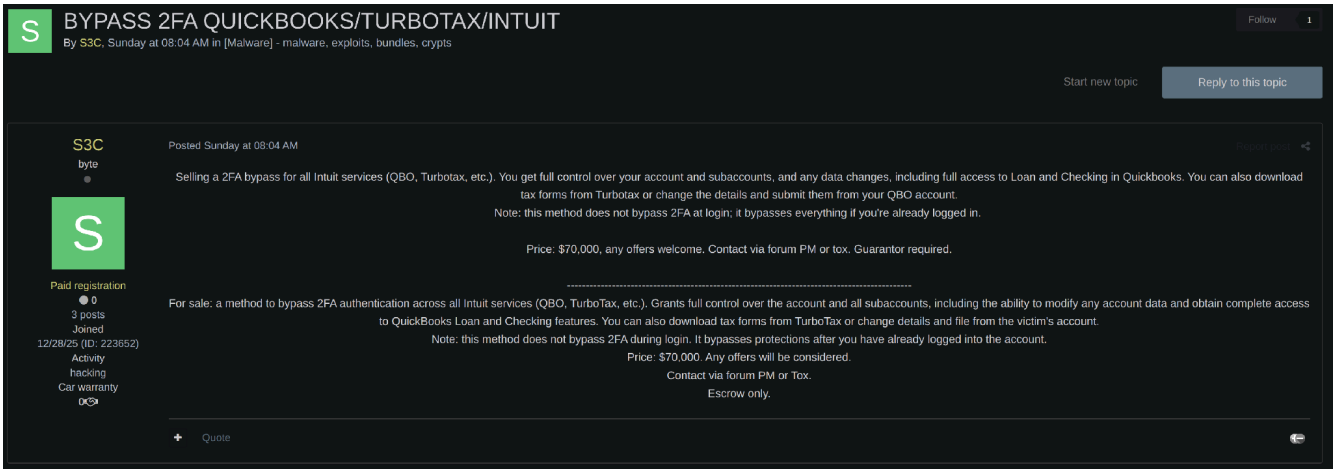
2FA Bypass "Method" Targeting Intuit Services Advertised on Exploit Forum

On June 6, 2026, untested threat actor "S3C" advertised a method to bypass two-factor authentication (2FA) solutions for multiple Intuit services, including QuickBooks Online (QBO) and TurboTax, on dark web forum Exploit. The alleged solution is priced at USD 70,000 and is intended for sale to a single buyer. S3C claims the purchase includes additional QuickBooks features, other protection bypasses, and implementation guidance.

- Intuit is a U.S.-based global financial technology company.

- According to the post, S3C requires the transaction to be conducted through a guarantor/escrow service.
- The actor joined Exploit in December 2025 and has a reaction score of zero at the time of writing.

The seller claims the solution provides full control over victim accounts and subaccounts, enabling attackers to modify account settings, add administrators, manage employees, alter banking details, and access QuickBooks financial services. The actor further alleges that the method for sale enables downloading, modifying, and submitting tax documents through TurboTax.



S3C advertising 2FA bypass method on Exploit

Source: ZeroFox Intelligence

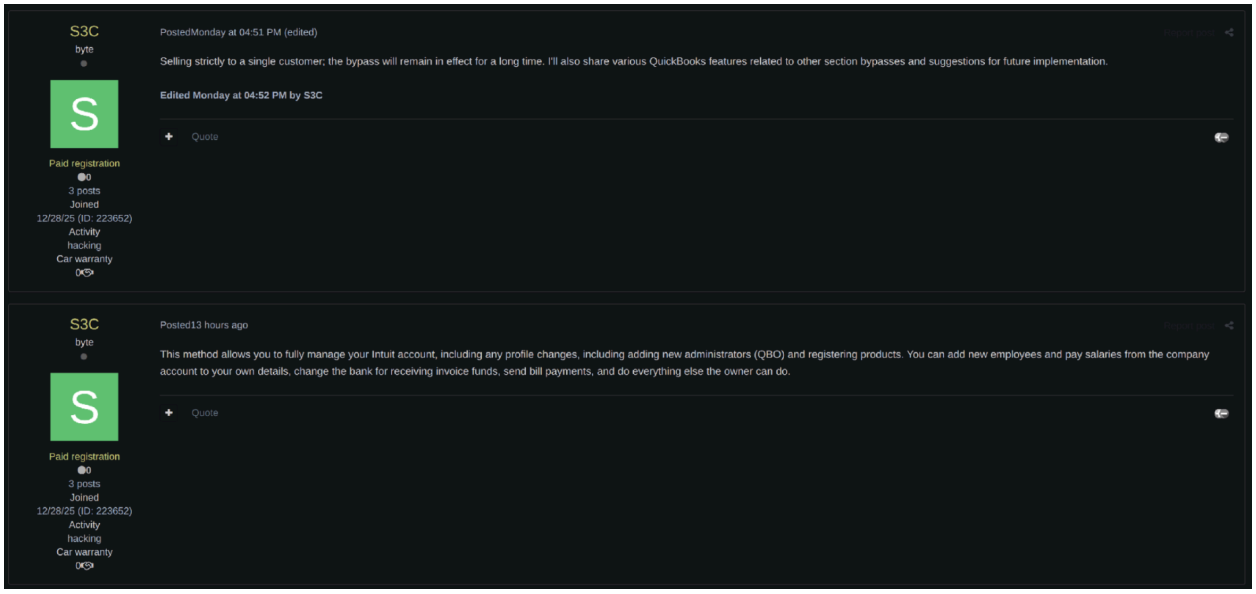
S3C's claims in the advertisement are somewhat vague. The actor does not explicitly identify the solution being advertised and instead refers to it as "a method to bypass 2FA." Additionally, they claim that the "bypass will remain in effect for a long time," which suggests the actor believes the exploit is either unpatched, difficult to detect, or unlikely to be remediated in the near term.

- The actor's words, unspecified method of bypass, and a lack of included proof is likely to raise questions about their credibility. It is likely that the post is a call for attention to generate traffic and raise S3C's reaction score on Exploit.

Moreover, the actor claims that the method offered for sale does not bypass login-time 2FA. From SC3's perspective, the advertised capability likely does not bypass 2FA during

authentication but instead enables unauthorized access to accounts by circumventing post-authentication security controls, such as through session hijacking or token theft, thereby rendering 2FA protections ineffective. If a valid authenticated session exists, the actor will likely gain access or perform actions as that user without needing to pass multi-factor authentication (MFA) themselves.

- Activities such as modifying account settings, accessing financial services, and manipulating tax documents can likely be enabled through the abuse of a valid authenticated session, enabling attackers to adopt the same privileges and permissions as the legitimate user while bypassing the need to re-authenticate.



S3C's follow up posts on Exploit
Source: ZeroFox Intelligence

If SC3's claims are legitimate, this solution is likely to be attractive to phishing-as-a-service (PhaaS) operators—particularly those utilizing adversary-in-the-middle (AiTM) techniques—as it likely enables the abuse of authenticated sessions to facilitate account takeover, financial fraud, and tax fraud without requiring attackers to bypass MFA directly.

If the advertised method works, interested buyers are likely to access Intuit accounts to conduct fraudulent activities (including payroll diversion, invoice payment redirection, fraudulent bill payments, and unauthorized transfers to attacker-controlled accounts),

as well as to create fraudulent employee or administrator accounts to establish persistence.

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 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.