ZEROFOX INTELLIGENCE

Brief

The Underground Economist: Volume 6, Issue 7

B-2026-03-26b

Classification: TLP:CLEAR

Criticality: LOW

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

March 26, 2026

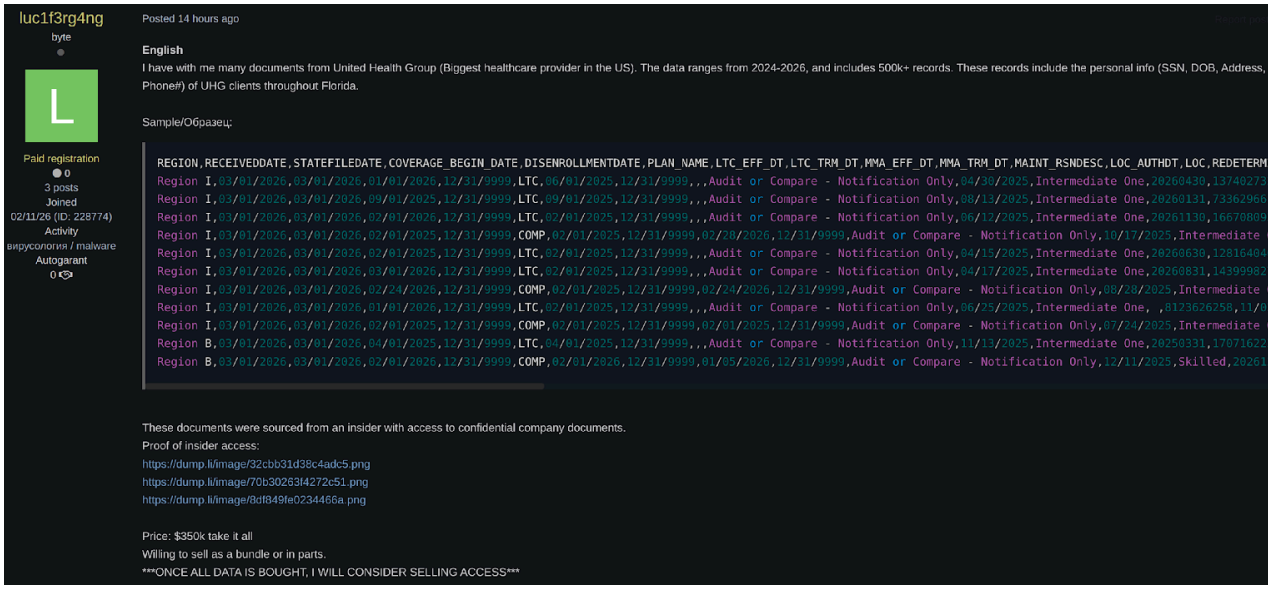
ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot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

| Brief | The Underground Economist: Volume 6, Issue 7

| Large Data Breach of U.S.-Based Health Insurance Company

On March 24, 2026, untested threat actor "luc1f3rg4ng" posted on the dark web forum Exploit announcing a breach of UnitedHealth Group. The entire dataset was allegedly obtained via an insider and purportedly includes a host of personally identifiable information (PII). The breached dataset is priced at USD 350,000, although it is available for purchase in segments as well.

- UnitedHealth Group is a U.S.-based multinational health insurance and services company. It has frequently ranked as the largest healthcare company in the world by revenue in recent years.



luc1f3rg4ng's Exploit post
Source: ZeroFox Intelligence

According to the actor, the data was exfiltrated in March 2026 and contains more than 500,000 records from the 2024–2026 period. The data allegedly includes PII such as Social Security numbers (SSNs), birth dates, home addresses, and phone numbers of UnitedHealth Group customers located across the state of Florida. Additionally, tluc1f3rg4ng indicated they may sell the insider access once the database is purchased.

- Although the exfiltrated data does not cover all records held by UnitedHealth Group, it still represents one of the most significant healthcare breaches reported so far in 2026.

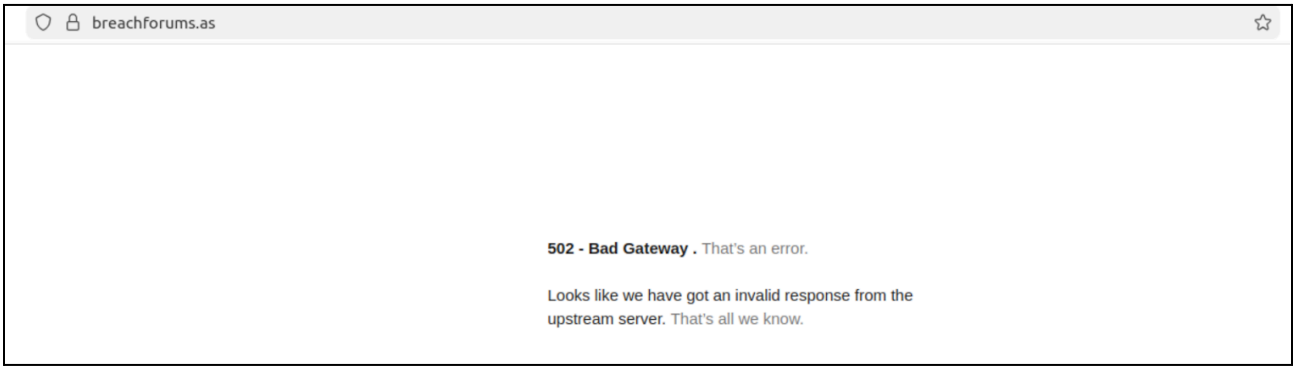
The actor provided samples in the post, which ZeroFox researchers analyzed and that appear to confirm the legitimacy of the data. The actor also shared screenshots that include what appears to be internal messages and databases related to UnitedHealth Group, providing insight into their likely credibility and the legitimacy of the alleged insider access being offered.

ShinyHunters Announced Sale of BreachForums

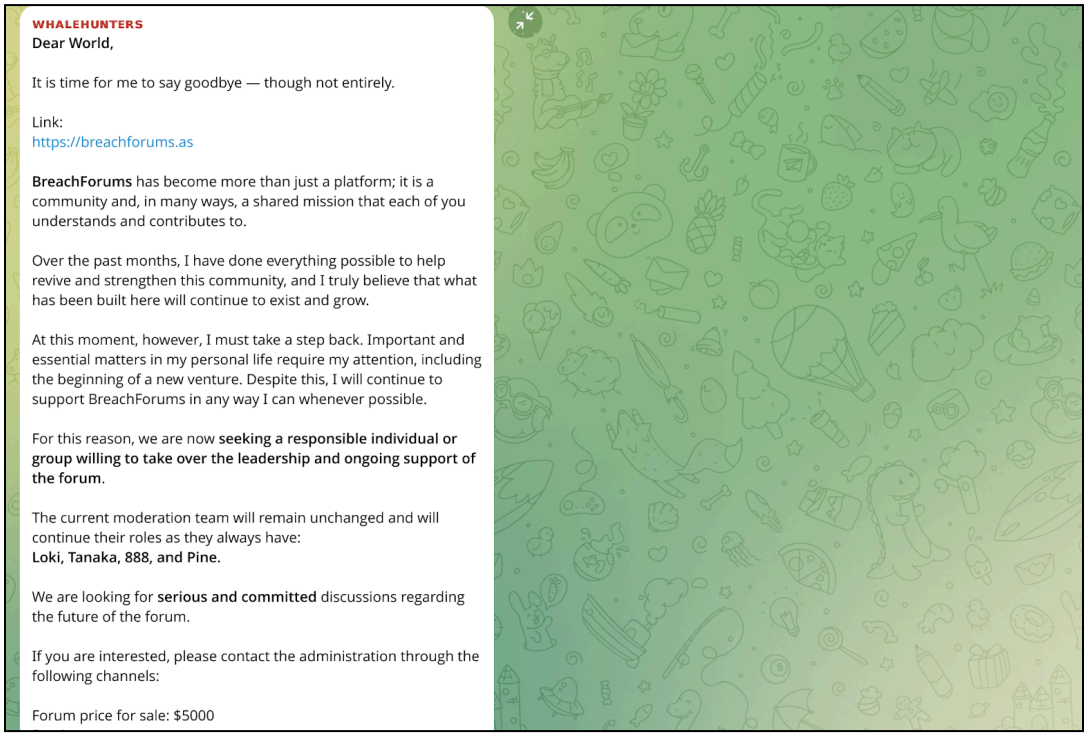
On March 16, 2026, ShinyHunters, the established and high-profile data breach collective that operates the dark web forum BreachForums and its associated clearnet leak site, announced on its Telegram channel that it will put the forum up for sale. ShinyHunters stated that the administrative team running the forum—Loki, Tanaka, 888, and Pine—will remain unchanged through the sale, as it only seeks to replace the forum's leadership.

- The asking price for the forum, including its source code and infrastructure, is USD 5,000. Notably, this is not the first time BreachForums has been listed for sale.
- BreachForums is known as one of the platforms that has significantly saturated the data-leak marketplace on the dark web.

ZeroFox assesses that, due to the recent arrests of alleged ShinyHunters members, the remaining members of the group have likely decided to step down from their roles as owners. BreachForums has previously been targeted by international law enforcement agencies, making it a potentially unstable asset for future owners.



Official URL of BreachForums displaying a 502 error
Source: ZeroFox Intelligence

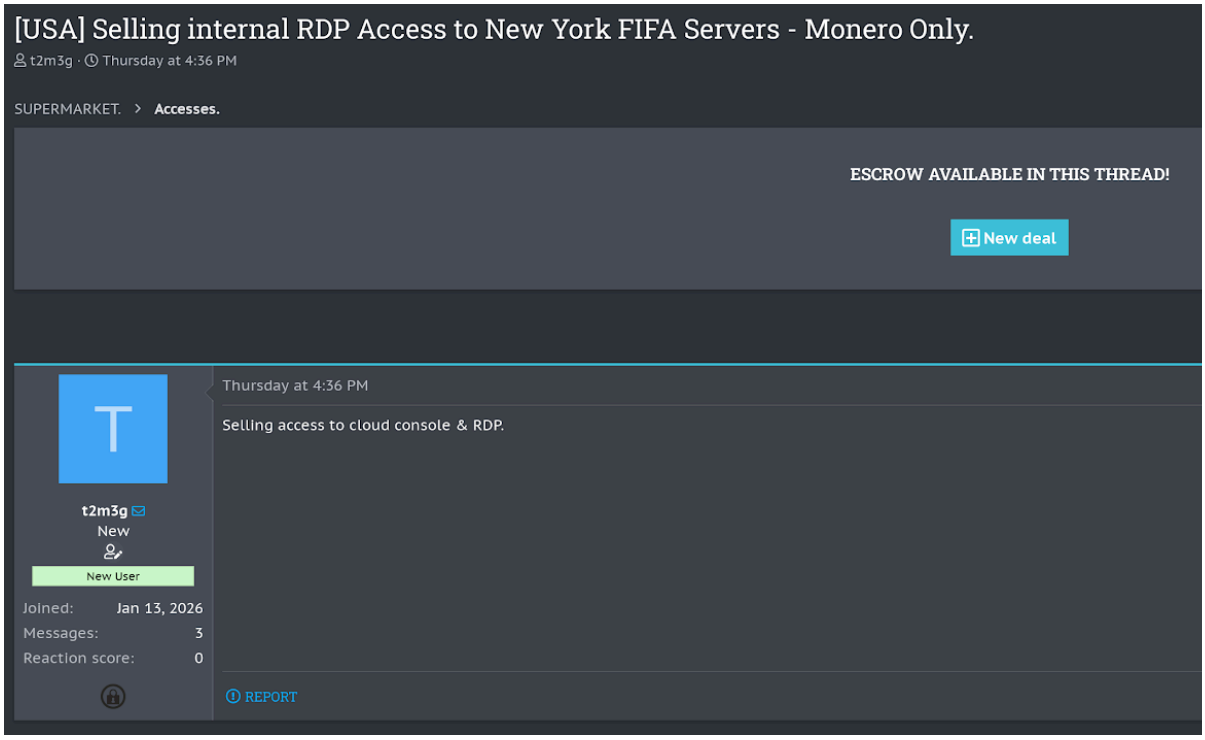


Original post from the WhaleShinyHunters Telegram Channel
Source: ZeroFox Intelligence

Alleged RDP Access to FIFA Systems Advertised on Darkweb Forum

On March 12, 2026, newly registered and untested actor “t2m3g” advertised alleged access to internal remote desktop protocol (RDP) systems of FIFA servers located in New York on the predominantly Russian-language dark web forum ReHub. The actor stated that the offer includes access to a cloud console and RDP connectivity.

- RDP is a Microsoft protocol that enables remote access to systems that are frequently targeted by threat actors for initial access and lateral movement.
- The actor has not provided any supporting evidence, such as screenshots or proof-of-access, as of reporting.
- Two separate forum users have already expressed interest in the offer, indicating early-stage engagement despite limited verification.



t2m3g's ReHub post

Source: ZeroFox Intelligence

The actor has provided minimal details regarding the scope and level of access, which restricts ZeroFox's ability to independently evaluate the veracity of the offering. The lack of pricing and technical specifications is likely an effort to manage disclosure and thoroughly vet prospective buyers before communicating sensitive information.

- The price was not disclosed in the advertisement, suggesting that transaction details are almost certainly intended to be negotiated privately between the seller and potential buyers.
- T2m3g joined ReHub in January 2026 and has a reaction score of zero.

Given the actor's nascent account age on the forum, their low reputation score, the limited information provided, and the absence of verifiable proof, it is likely that the t2m3g's claims are exaggerated or false.

- Newly observed threat actors on underground forums frequently post high-value or high-visibility claims to establish credibility, attract attention, or initiate private negotiations with interested buyers.

Moreover, with the FIFA World Cup scheduled to begin in June, t2m3g's advertisement is likely an attempt to capitalize on the heightened interest around the event; threat actors are likely to increasingly target FIFA's digital infrastructure for either political or financial gain in the run-up to this event.

Alleged U.S. Top-Secret Intelligence Documents for Sale

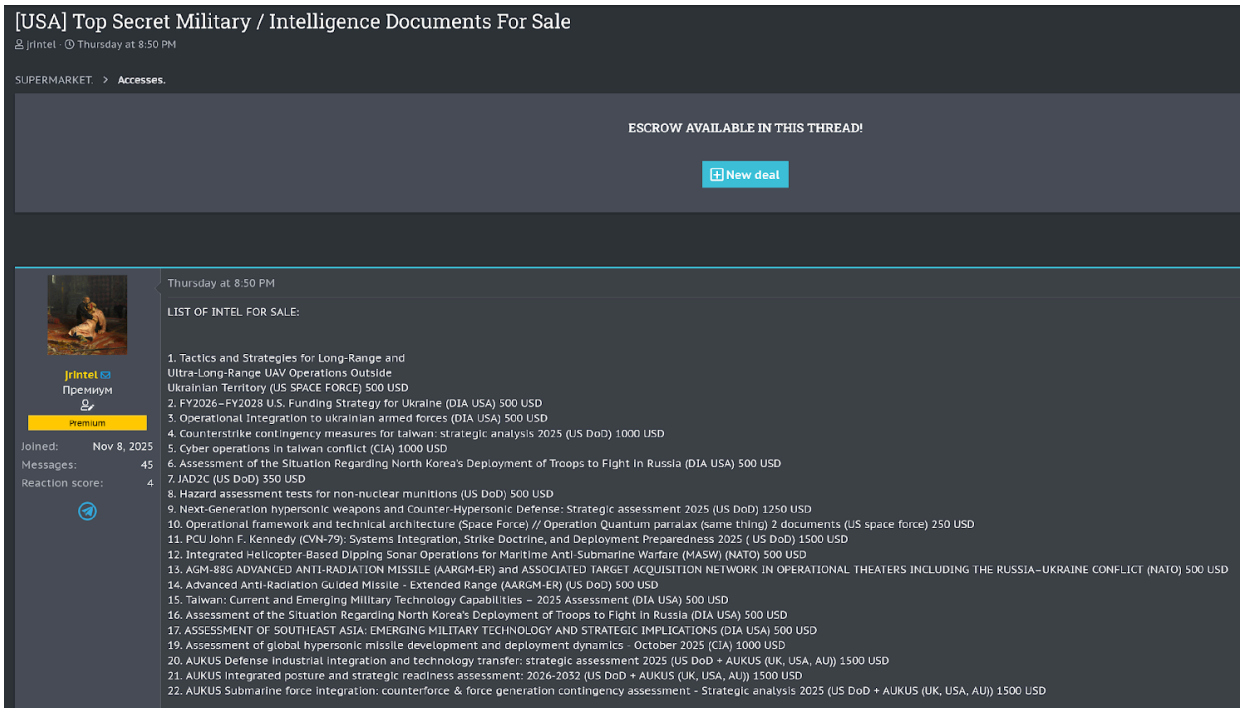
On March 12, 2026, a newly registered and positively trending actor known as "jrintel" announced the sale of an allegedly extensive trove of top-secret U.S. military and intelligence documents on the predominantly Russian-language dark web forum ReHub. The list of available documents shared by the seller contains 22 items, which can be purchased separately at prices ranging from USD 250 to USD 1,500 each. The documents allegedly for sale include:

- U.S. Space Force
    - Tactics and Strategies for Long-Range and Ultra-Long-Range UAV Operations Outside Ukrainian Territory
    - Operational framework and technical architecture
    - Operation Quantum Parallax
- U.S. Defense Intelligence Agency
    - FY2026–FY2028 U.S. Funding Strategy for Ukraine
    - Operational Integration to Ukrainian armed forces
    - Assessment of the Situation Regarding North Korea's Deployment of Troops to Fight in Russia
    - Taiwan: Current and Emerging Military Technology Capabilities – 2025 Assessment

- Assessment of the Situation Regarding North Korea's Deployment of Troops to Fight in Russia
- ASSESSMENT OF SOUTHEAST ASIA: EMERGING MILITARY TECHNOLOGY AND STRATEGIC IMPLICATIONS

- U.S. Department of Defense (War)
  - Counterstrike contingency measures for Taiwan: strategic analysis 2025
  - JAD2C
  - Hazard assessment tests for non-nuclear munitions
  - Next-Generation hypersonic weapons and Counter-Hypersonic Defense: Strategic assessment 2025
  - PCU John F. Kennedy (CVN-79): Systems Integration, Strike Doctrine, and Deployment Preparedness 2025
  - Advanced Anti-Radiation Guided Missile – Extended Range (AARGM-ER)
  - AUKUS Defense industrial integration and technology transfer: strategic assessment 2025 (UK, USA, AU)
  - AUKUS integrated posture and strategic readiness assessment: 2026-2032 (UK, USA, AU)
  - AUKUS Submarine force integration: counterforce & force generation contingency assessment – Strategic analysis 2025 (UK, USA, AU)
- U.S. Central Intelligence Agency
  - Cyber operations in Taiwan conflict
  - Assessment of global hypersonic missile development and deployment dynamics – October 2025
- NATO-related
  - Integrated Helicopter-Based Dipping Sonar Operations for Maritime Anti-Submarine Warfare (MASW)

- AGM-88G ADVANCED ANTI-RADIATION MISSILE (AARGM-ER) and ASSOCIATED TARGET ACQUISITION NETWORK IN OPERATIONAL THEATERS INCLUDING THE RUSSIA–UKRAINE CONFLICT



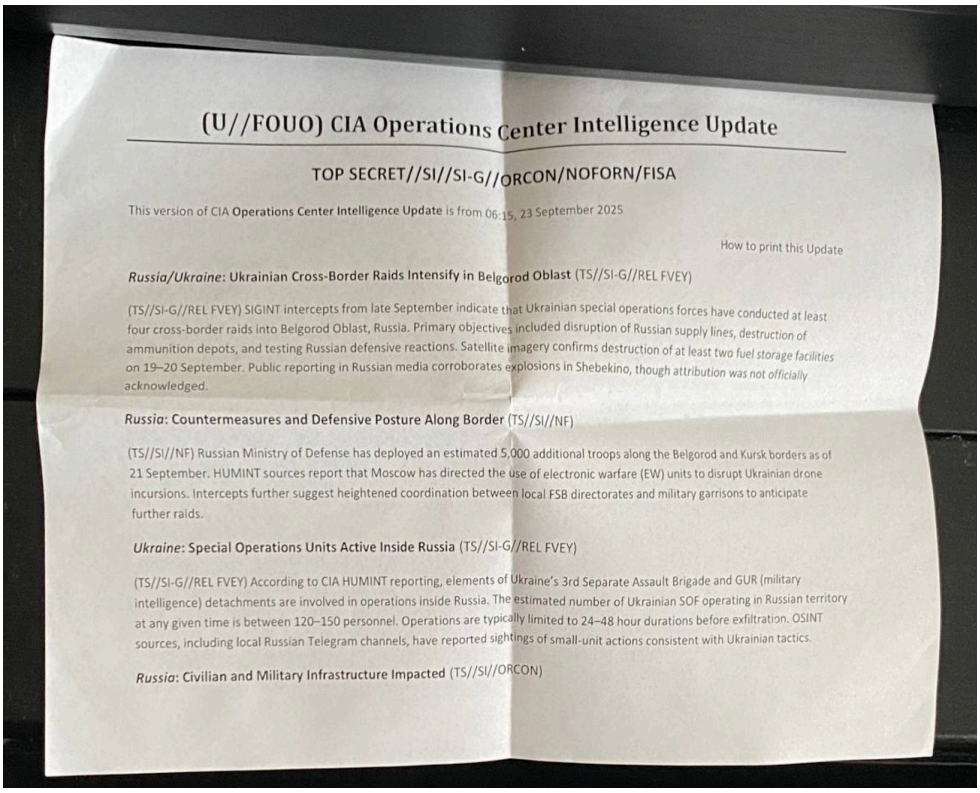
jrintel's ReHub post
Source: ZeroFox Intelligence

The threat actor claims that this is not an exhaustive list of the materials in their possession related to critical U.S. military and intelligence documents. Jrintel is known as an actor who discloses government documents and data on military contractors.

- The United States is not the only target; the seller also provides information on European defense contractors, as well as military organization documents related to Russia and China. Therefore, ZeroFox cannot conclude that jrintel is solely a broker of leaked intelligence information exfiltrated from American targets.

The actor also included sample documents in their post, which appear to be printed slideshow sheet-like documents with classification markings. While the pages and markings provided as samples do not appear to be authentic and are very unlikely to be real, there is a roughly even chance that at least some of the documents allegedly in

jrintel's possession are authentic as they are generally known to be a credible threat actor. Further, providing false samples would very likely hinder jrintel's ability to sell the advertised documents and harm their reputation.



(U//FOUO) CIA Operations Center Intelligence Update

TOP SECRET//SI//SI-G//ORCON/NOFORN/FISA

This version of CIA **Operations Center Intelligence Update** is from 06:15, 23 September 2025

How to print this Update

***Russia/Ukraine*: Ukrainian Cross-Border Raids Intensify in Belgorod Oblast** (TS//SI-G//REL FVEY)

(TS//SI-G//REL FVEY) SIGINT intercepts from late September indicate that Ukrainian special operations forces have conducted at least four cross-border raids into Belgorod Oblast, Russia. Primary objectives included disruption of Russian supply lines, destruction of ammunition depots, and testing Russian defensive reactions. Satellite imagery confirms destruction of at least two fuel storage facilities on 19–20 September. Public reporting in Russian media corroborates explosions in Shebekino, though attribution was not officially acknowledged.

***Russia*: Countermeasures and Defensive Posture Along Border** (TS//SI//NF)

(TS//SI//NF) Russian Ministry of Defense has deployed an estimated 5,000 additional troops along the Belgorod and Kursk borders as of 21 September. HUMINT sources report that Moscow has directed the use of electronic warfare (EW) units to disrupt Ukrainian drone incursions. Intercepts further suggest heightened coordination between local FSB directorates and military garrisons to anticipate further raids.

***Ukraine*: Special Operations Units Active Inside Russia** (TS//SI-G//REL FVEY)

(TS//SI-G//REL FVEY) According to CIA HUMINT reporting, elements of Ukraine's 3rd Separate Assault Brigade and GUR (military intelligence) detachments are involved in operations inside Russia. The estimated number of Ukrainian SOF operating in Russian territory at any given time is between 120–150 personnel. Operations are typically limited to 24–48 hour durations before exfiltration. OSINT sources, including local Russian Telegram channels, have reported sightings of small-unit actions consistent with Ukrainian tactics.

***Russia*: Civilian and Military Infrastructure Impacted** (TS//SI//ORCON)

Alleged sample document provided in jrintel's ReHub post
Source: ZeroFox Intelligence

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.