ZEROFOX INTELLIGENCE

Brief

The Underground Economist: Volume 6, Issue 11

B-2026-05-21b

Classification: TLP:CLEAR

Criticality: LOW

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

May 21, 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 May 21, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | The Underground Economist: Volume 6, Issue 11

| BreachForums Partners with The Gentlemen RaaS

On May 16, 2026, "diencracked," the owner of dark web forum BreachForums, announced a new partnership with ransomware-as-a-service (RaaS) collective The Gentlemen. The announcement also specified BreachForums is seeking affiliates, penetration testers, and initial access brokers (IABs). Affiliates will reportedly retain 90 percent of ransom payments generated through the operation.

The Gentlemen and BreachForums partnership announcement

Source: ZeroFox Intelligence

- The Gentlemen has been active on the deep and dark web (DDW) since at least September 2025 and has claimed at least 346 victims globally as of April 2026.
- The collective averages approximately 43 claimed attacks per month across the healthcare, manufacturing, education, financial services, and government sectors.
- The Gentlemen explicitly prohibits attacks targeting Commonwealth of Independent States (CIS) countries, a long-standing operational convention among Russian-language cybercriminal actors.

The partnership announcement suggests BreachForums is likely moving beyond conventional ransomware activity promotion towards a more active role in cybercrime operations. While dark web forums usually advertise ransomware kits and services, the creation of dedicated infrastructure and the seeking of direct affiliate recruitment

support suggest a closer operational alignment between forum administrators and ransomware operators.

- The advertised revenue-sharing structure is similar to The Gentlemen's previously observed 90/10 affiliate split and broader monetization strategy.

The Gentlemen employs a double extortion model with a silent encryption mode (as indicated by the file encryptions and ransom notes in confirmed attacks) that is likely intended to reduce visible indicators of compromise. The group also appears to maintain structured affiliate-management and operational security practices likely designed to limit law enforcement exposure and improve affiliate confidence.

- The collective reportedly preserves file names and timestamps during encryption while sourcing credentials and network access through underground markets and infostealer ecosystems.
- Affiliate communications are handled through encrypted platforms such as Tox, while onboarding deposits and target disclosures likely function as anti-infiltration measures.
- The Gentlemen introduced a 97/3 split for data-only extortion campaigns and deployed a same-day patch following the release of a public decryptor in April 2026.

While relationships between cybercrime forums and ransomware operators are not unprecedented, the promotional activity around BreachForums' operational involvement with The Gentlemen exceeds what is commonly observed across similar partnerships.

- ReHub administrators have previously been associated with DragonForce ransomware promotion, while T1erOne has publicly supported Anubis' ransomware operations.

This partnership very likely reflects broader consolidation trends across the ransomware ecosystem, where forums increasingly function as integrated operational hubs rather than passive marketplaces. RaaS operations, such as The Gentlemen, are increasingly likely to seek opportunities to expand attack scalability by combining affiliate

recruitment, access brokerage, infrastructure support, and extortion coordination within a single environment.

FortiGate Symlink Bypass for Sale on Exploit Forum

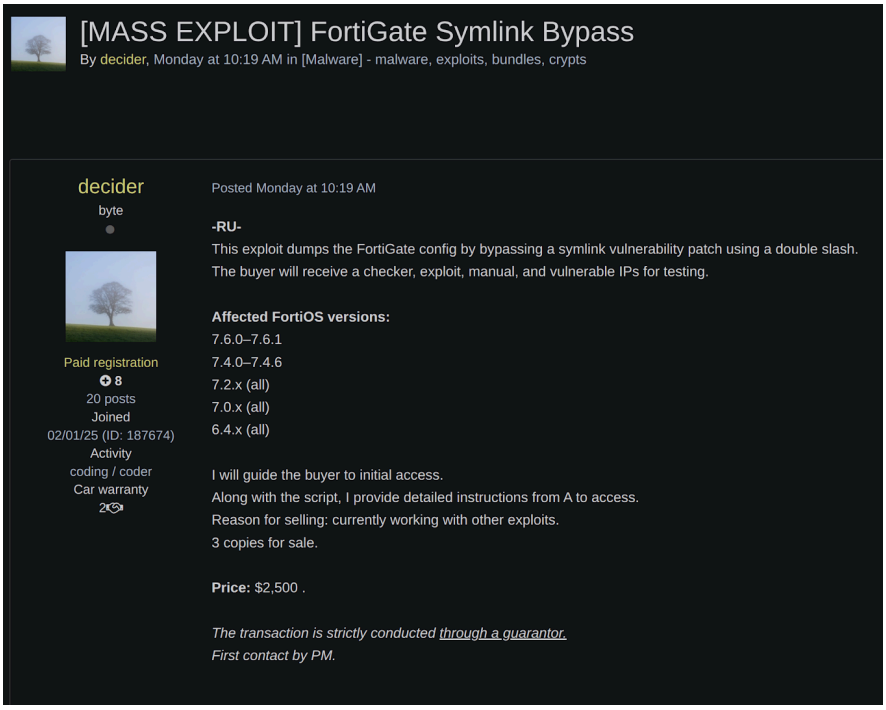
On May 11, 2026, a moderately credible threat actor known as "decider" announced the sale of a FortiGate Symlink Bypass exploit on the Exploit forum. According to the actor, the exploit is capable of dumping the FortiGate configuration by bypassing a symlink vulnerability patch using a "double snatch" technique.

- The double snatch technique uses two-stage file retrieval to snatch protected files twice in sequence to bypass a previous symlink mitigation.
- In April 2025, Fortinet, the developer of FortiGate, acknowledged that attackers were able to maintain read-only access to vulnerable FortiGate devices—even after security patches were installed on the breached devices.[1]
- FortiGate is Fortinet's next-generation firewall (NGFW) and purports to provide enhanced security for modern hybrid data environments. The service reportedly has a 50 percent market share in the NGFW sector.

According to the seller, buyers of the exploit will receive a checker, the exploit itself, a handbook, and a list of vulnerable IP addresses for testing purposes. The affected FortiOS versions are:

- 7.6.0–7.6.1
- 7.4.0–7.4.6
- 7.2.x (all versions)
- 7.0.x (all versions)
- 6.4.x (all versions)

[1] hXXps://thehackernews[.]com/2025/04/fortinet-warns-attackers-retain.html



decider's post on Exploit forum

Source: ZeroFox Intelligence

According to the post, three copies of the exploit are being sold for USD 2,500 each. The seller also claims they will assist buyers in achieving initial access and provide a script with detailed instructions.

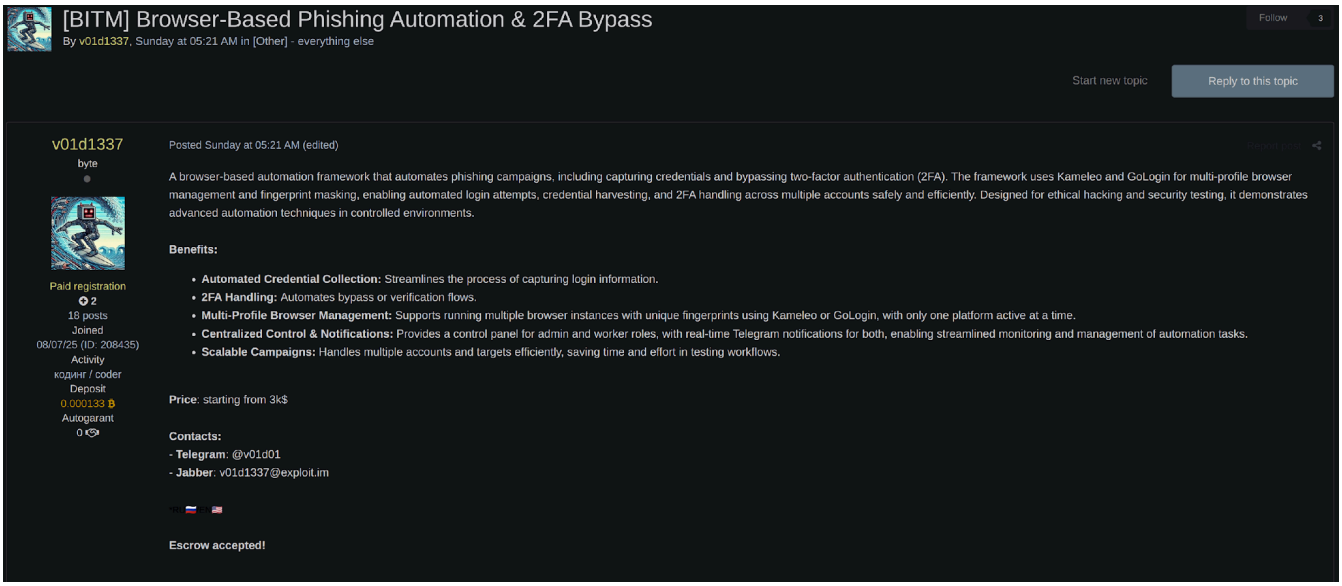
This exploit is the latest in a series of security incidents involving Fortinet products. Fortinet has experienced so many incidents between early 2023 and early 2026 that insurers are reportedly charging double premiums for organizations deploying them.[2] Given Fortinet's vulnerability track record, it is very likely the exploit that decider is offering is legitimate and presents a significant threat to FortiGate users.

[2] hXXps://thesmallbusinesscybersecurityguy[.]co[.]uk/blog/fortinet-security-failures-vpn-breaches-uk-2026/

Threat Actor Advertises Automated Phishing Framework

On May 9, 2026, untested threat actor "v01d1337" advertised a browser-based phishing automation framework on the dark web forum Exploit. The framework allegedly automates phishing campaigns at scale, steals credentials, bypasses two-factor authentication (2FA), and operates across multiple browser instances and targets.

- The actor claims that the phishing framework operates as a browser-in-the-middle (BitM) solution, leveraging legitimate anti-detect browser tools Kameleo and GoLogin for their browser fingerprint-spoofing capabilities.



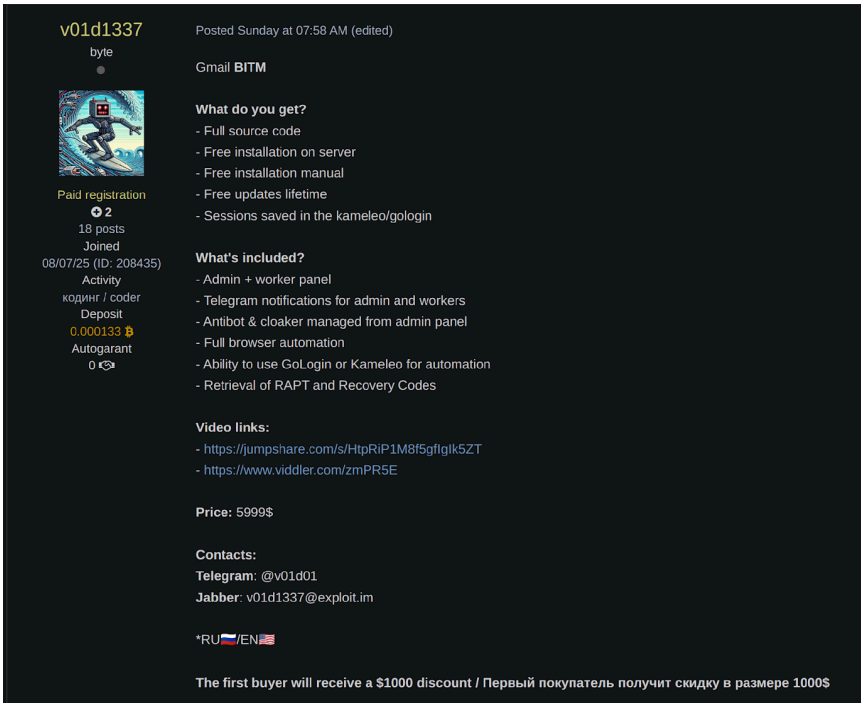
v01d1337's post on Exploit

Source: ZeroFox Intelligence

The actor has provided a starting price of USD 3,000, along with two dedicated solutions: one for targeting Gmail accounts (USD 5,999) and the other for targeting blockchain-related services (USD 7,499).

- The Gmail BitM package allegedly includes full source code, free server installation, lifetime free updates, session storage in Kameleo/GoLogin, admin and worker panels, Telegram notifications, anti-bot and cloaking features, and code-retrieval.

- The blockchain-focused solution includes the same functions as the Gmail package, except it includes proxy-based authentication tied to the victim's geographic location.



Features of v01d1337's offering

Source: ZeroFox Intelligence

On May 4, 2026, v01d1337 had also advertised custom Evilginx phishlets targeting major media and retail websites. The two advertisements very likely suggest v01d1337 is building a reputation as a phishing-as-a-service (PhaaS) operator, offering tiered phishing tools at different price ranges. There is a roughly even chance that the offers are legitimate given the technical details provided in the advertisements.

- If legitimate, the fully automated BitM phishing operation is very likely to reduce the technical threshold required for carrying out phishing campaigns, contributing to an increase in the volume of phishing attacks. However, the high price tag is likely to act as a barrier for lower-level individual actors, making cybercriminal groups the more probable buyer demographic (which is also supported by the centralized admin panel design).

Western European Healthcare Information for Sale

On April 30, 2026, an untested actor identified as "TitanCaller" posted on the dark web forum Exploit seeking buyers interested in personally identifiable information (PII), including protected health information (PHI) and healthcare-related data from the medical sector in Western Europe. The actor claimed to possess more than 500 GB of compromised data consisting of:

- Professional, citizen, and clinical data
- Source code, including more than 200GB of intellectual property
- PHI documents for more than 1.5 million users
- Private keys related to European vaccination cards, allegedly enabling direct API queries and potential access escalation across multiple countries

At the time of writing the data remained available for sale; TitanCaller also expressed interest in partnerships or alternative methods of monetization. The source of the data remains unconfirmed; however, the alleged inclusion of leaked source code indicates the data was very likely exfiltrated from a centralized healthcare system. There is a roughly even chance that the leak is the result of insider-related compromise.

The leak, if confirmed, would almost certainly represent a significant risk to affected individuals. Critical medical information related to celebrities or high-profile political figures is very likely to be leveraged in extortion campaigns.

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%

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.