ZEROFOX INTELLIGENCE

Brief

The Underground Economist: Volume 6, Issue 12

B-2026-06-04b

Classification: TLP:CLEAR

Criticality: LOW

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

June 4, 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 4, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | The Underground Economist: Volume 6, Issue 12

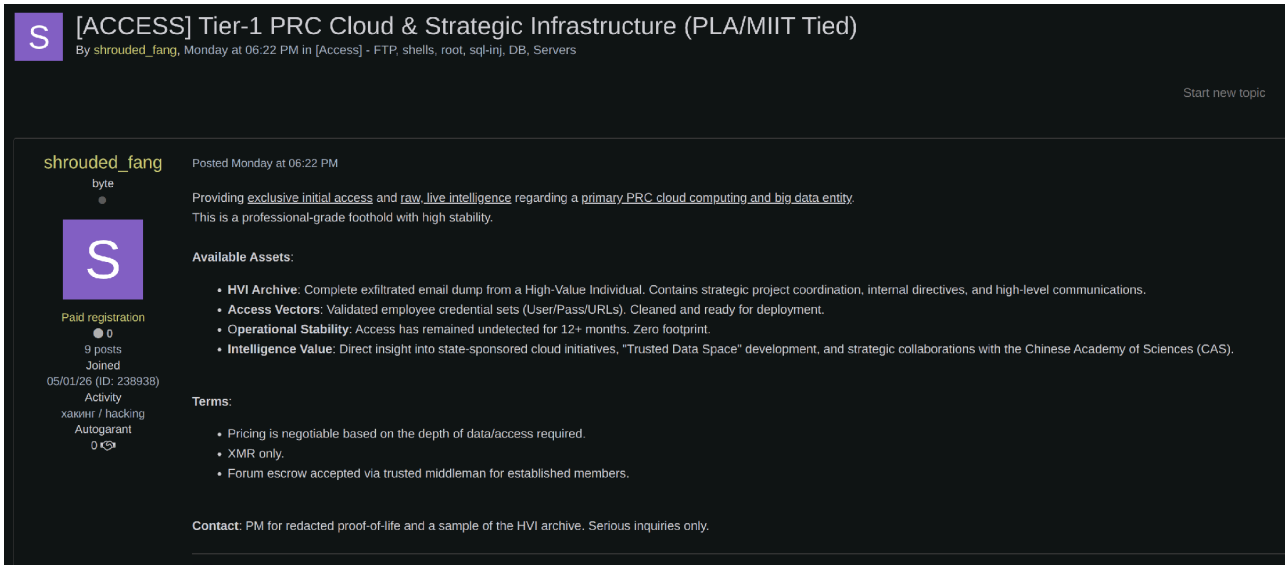
| Intelligence-Focused Access to a Cloud and Data Entity

On June 1, 2026, untested and newly registered threat actor "shrouded_fang" posted on the dark web forum Exploit, advertising alleged access to an unspecified cloud and strategic infrastructure entity. The actor claimed to possess a long-term foothold within this unspecified major Chinese cloud and data organization, exfiltrated communications from an alleged high-value individual, and validated employee credentials.

- If authentic, the offering would very likely provide buyers with both operational access and strategic intelligence, making it desirable to cybercriminal, espionage, and intelligence-gathering actors.

Notably, the actor emphasizes intelligence value rather than technical capability in this offer. The seller is marketing access based on the alleged sensitivity of the information available, including insight into cloud initiatives, data infrastructure projects, and collaborations tied to the People's Liberation Army (PLA), Ministry of Industry and Information Technology (MIIT), and the Chinese Academy of Sciences.

- Unlike typical access broker advertisements that focus on network size or privilege level, this post attempts to justify value through geopolitical and strategic relevance.



shrouded_fang's post on Exploit

Source: ZeroFox Intelligence

The seller further asserts that the access has persisted undetected for over a year. Regardless of the claim's veracity, the advertisement characterizes the foothold as a mature and enduring intelligence resource rather than a recently breached environment.

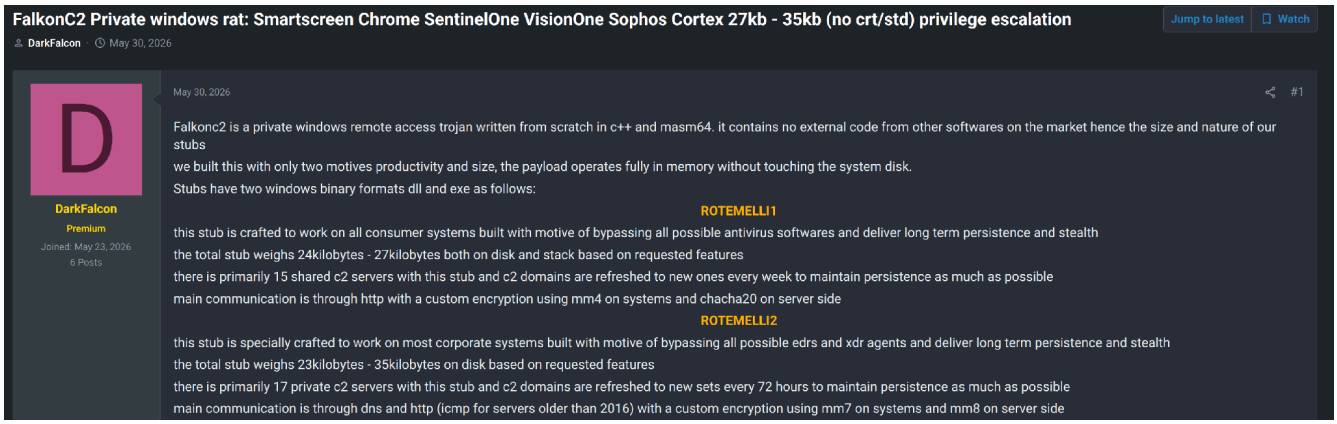
Actor shrouded_fang joined the forum in May 2026 and has yet to garner any reactions or reputational score. However, the advertisement aligns with the trend of specialized initial access brokers (IABs) marketing access to strategic organizations rather than simply selling credentials in bulk.

- The combination of purported long-term persistence, executive-level communications, and intelligence-focused marketing suggests the seller is likely targeting a niche buyer base interested in espionage, competitive intelligence, or high-value cyber operations.
- Furthermore, the actor's apparent preference for negotiated pricing over a fixed rate very likely indicates that they perceive the access as a premium intelligence asset rather than a commodity offering.

New Private Windows RAT Advertised on Dark Web

On May 30, 2026, vetted threat actor "DarkFalcon" posted on the private-access dark web forum T1erOne, advertising a new private Windows remote access trojan (RAT) strain called Falkonc2, which the actor claims has unique features compared to other popular RAT families.

- The actor claims the malware operates entirely in memory without writing to disk and is available in separate consumer (ROTEMELLI1) and enterprise (ROTEMELLI2) editions. As of June 1, 2026, DarkFalcon reported that slots for ROTEMELLI2 had been sold out.



DarkFalcon's post on T1erOne

Source: ZeroFox Intelligence

DarkFalcon claims that the malware can operate across a broad range of Windows devices and environments. It also reportedly includes persistence, remote access, reconnaissance, and security control evasion. Additionally, the enterprise edition supposedly includes environment-aware features, such as Active Directory discovery and accounting software identification.

- The features also allegedly include a dedicated management infrastructure and frequent command-and-control (C2) rotation mechanisms.
- The consumer and enterprise editions allegedly utilize different communication methods and infrastructure models tailored to their respective target environments.

The inclusion of dedicated infrastructure, regularly rotated C2 servers, and reconnaissance capabilities tailored to specific victim types likely indicates an effort to make the malware more effective and easier to deploy against either individual users or corporate networks. These features distinguish Falkonc2 from the other popular malware advertisements that promote a single malware variant.

- The combination of persistence, remote access, reconnaissance, and claimed evasion capabilities indicates that the platform is designed to function either as an initial access tool or as a post-compromise utility within broader intrusion operations.

The fast sale of the enterprise edition of the malware and the actor's vetted reputation very likely indicate that the claims about the malware's features are true. It has likely gained traction among financially motivated actors or IABs seeking a flexible framework for establishing and maintaining access to compromised systems while collecting information about the target environment.

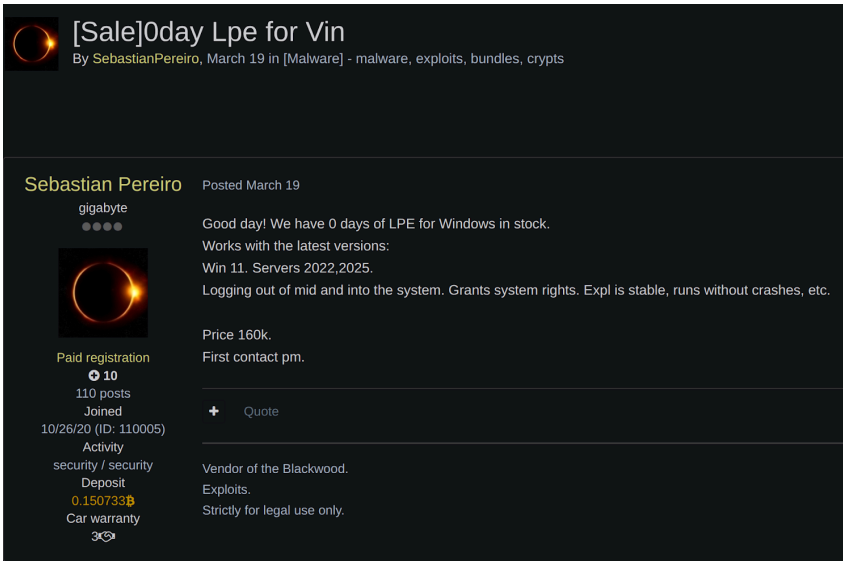
Windows Local Privilege Escalation Vulnerability Advertised on Exploit Forum

On May 27, 2026, moderately credible threat actor "Sebastian Pereiro" updated a post on the Exploit forum announcing the sale of an exploit for a zero-day Local Privilege Escalation (LPE) vulnerability for Windows servers. Based on previous posts by Sebastian Pereiro, it very likely affects Windows 11 and Windows Server 2022/2025 systems. The listed price for the exploit was USD 160,000.

- In the original post from March 19, 2026, the actor had posted the sale of an exploit for an almost identical vulnerability. In that post, the actor explained the exploit enabled privilege escalation from a medium integrity or standard user context to SYSTEM/root-level privileges.
- The previous exploit allegedly operated without causing system crashes, indicating that it can very likely elevate a standard user process to full SYSTEM privileges without disrupting the affected system.

Sebastian Pereiro is likely seen as a credible actor by other users on Exploit, as they have been on the platform since 2020, completed three transactions through the automated escrow system, and accumulated 10 reputation points. Additionally, they have a security deposit of BTC 0.15 (approximately USD 10,000, as of writing) with the platform administrators; this method is very likely used as a security measure to ensure transactions are carried out without fraud.

These types of exploits are almost certainly very valuable to threat actors who leverage compromised credentials obtained through infostealer logs, phishing campaigns, or other means. Successful use of this exploit would very likely enable attackers to escalate privileges across targeted Windows environments.



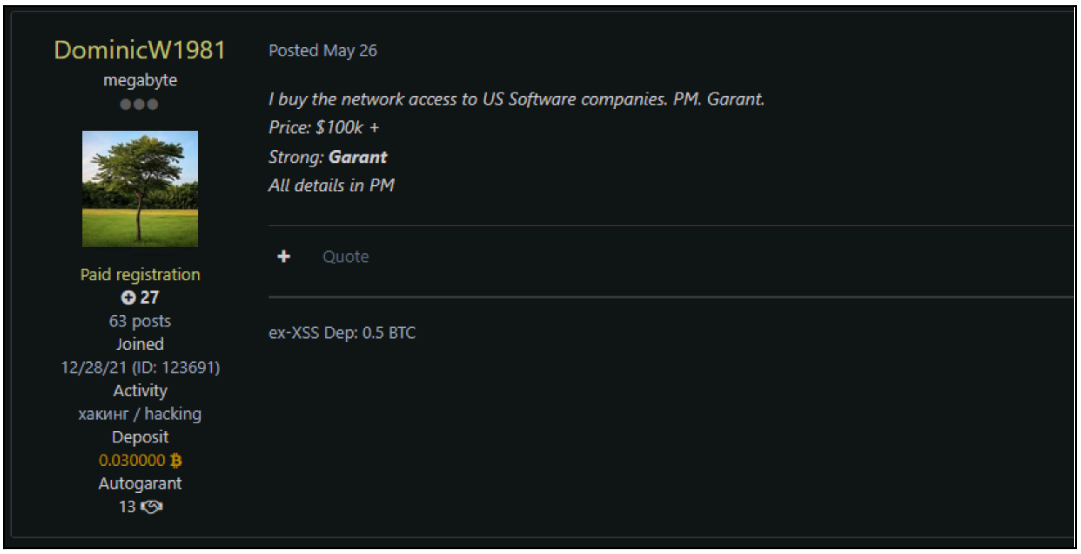
Sebastian Pereiro's post on Exploit

Source: ZeroFox Intelligence

Threat Actor Seeks Network Access to U.S. Software Companies

On May 26, 2026, well-regarded threat actor "DominicW1981" posted on Exploit, seeking to purchase access to networks of U.S.-based software companies, likely to conduct financially motivated, unauthorized intrusion and cybercriminal activities.

- The actor disclosed a budget of USD 100,000 or more for valid access—a higher than normal amount for network access, likely reflecting DominicW1981's genuine interest in the ask.
- The actor has also specified that they strongly prefer the transaction be carried out through the forum's middleman service.
- Additionally, they have stated they will communicate all other details via private message.



DominicW1981's post on Exploit

Source: ZeroFox Intelligence

The actor's longevity on the forum—combined with a positive reputation score and transaction history, indicating credible standing within Exploit—is likely to gain traction from members who sell such access, including IABs.

- The actor is a well-established member of Exploit and has been active on the forum since 2021.
- The account has accumulated 25 reputation points and completed 13 escrow-backed transactions.

While DominicW1981 did not specify the intended use for the access, they will likely leverage it for financially motivated activity, including ransomware operations, compromise of business-critical systems, and reconnaissance operations to establish a more persistent presence in the system and sell the refined access to other ransomware groups.

The post demonstrates the continued demand for initial network access across underground communities. If acquired, such access is likely to enable follow-on activity, including ransomware deployment, data theft, espionage, or attacks against downstream organizations. The actor's high stated budget likely also indicates previous success in monetizing similar access opportunities.

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.