ZEROFOX INTELLIGENCE

Brief

The Underground Economist: Volume 6, Issue 18

B-2026-08-27b

Classification: TLP:CLEAR

Criticality: LOW

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

August 27, 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 August 27, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

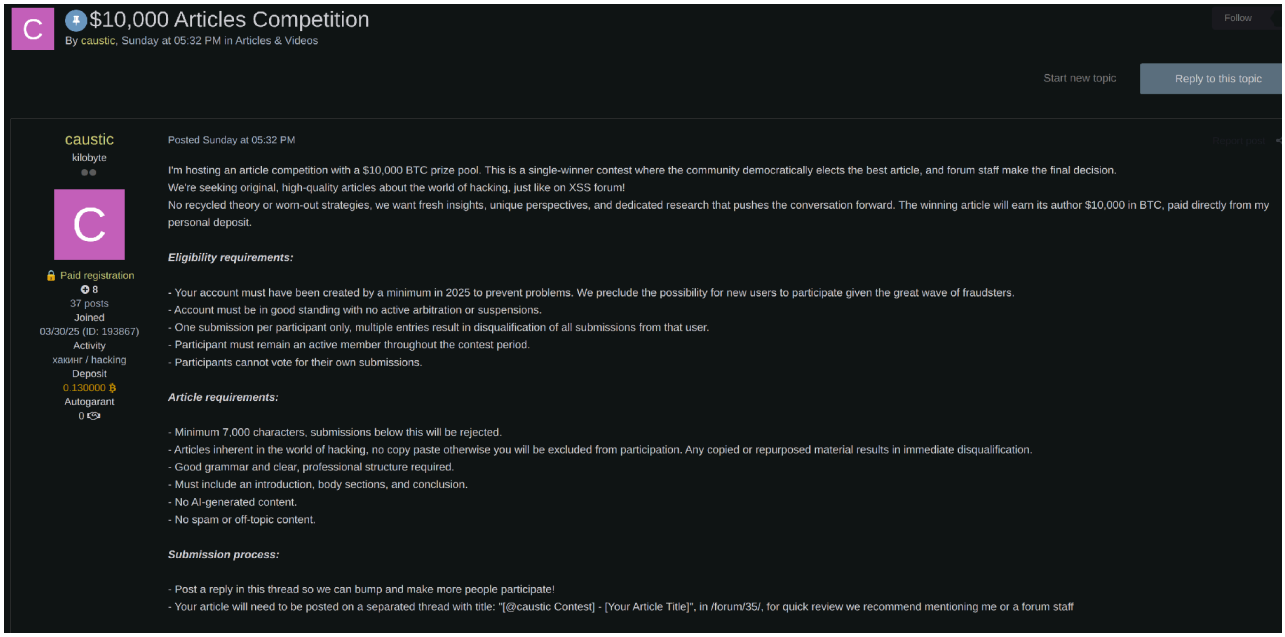
| Brief | The Underground Economist: Volume 6, Issue 18

| Dark Web Hacking Research Article Competition

On August 22, 2026, vetted threat actor "caustic" posted on the dark web forum Exploit announcing a hacking-focused article competition offering a USD 10,000 prize in Bitcoin (BTC). The contest seeks original, research-oriented submissions of at least 7,000 characters. Acceptable subject matter includes phishing, malware development, web exploitation, artificial intelligence (AI)-driven cyberattacks, botnet operations, operational security (OPSEC), and illicit monetization strategies. Submissions are due by September 6, 2026, and will undergo community voting followed by a final assessment from forum administrators.

- Caustic explicitly bans plagiarism, the use of AI to generate content, redundant entries, and any attempt to manipulate voting outcomes.
- Furthermore, participants must have accounts in good standing.

ZeroFox assesses that analogous hacking competitions that have emerged on dark web forums such as XSS, ReHub, and T1erOne indicate an established underground trend aimed at incentivizing and uncovering sophisticated technical intelligence. This initiative likely encourages forum participants to develop and share innovative cybercrime research, which will very likely facilitate the spread of advanced offensive methodologies throughout the deep and dark web (DDW) ecosystem.



$10,000 Articles Competition
By caustic, Sunday at 05:32 PM in Articles & Videos

Follow

Start new topic | Reply to this topic

caustic
kilobyte

Paid registration
8
37 posts
Joined
03/30/25 (ID: 193867)
Activity
хакинг / hacking
Deposit
0.130000 ₿
Autogarant
0

Posted Sunday at 05:32 PM

I'm hosting an article competition with a $10,000 BTC prize pool. This is a single-winner contest where the community democratically elects the best article, and forum staff make the final decision.
We're seeking original, high-quality articles about the world of hacking, just like on XSS forum!
No recycled theory or worn-out strategies, we want fresh insights, unique perspectives, and dedicated research that pushes the conversation forward. The winning article will earn its author $10,000 in BTC, paid directly from my personal deposit.

Eligibility requirements:

- Your account must have been created by a minimum in 2025 to prevent problems. We preclude the possibility for new users to participate given the great wave of fraudsters.
- Account must be in good standing with no active arbitration or suspensions.
- One submission per participant only, multiple entries result in disqualification of all submissions from that user.
- Participant must remain an active member throughout the contest period.
- Participants cannot vote for their own submissions.

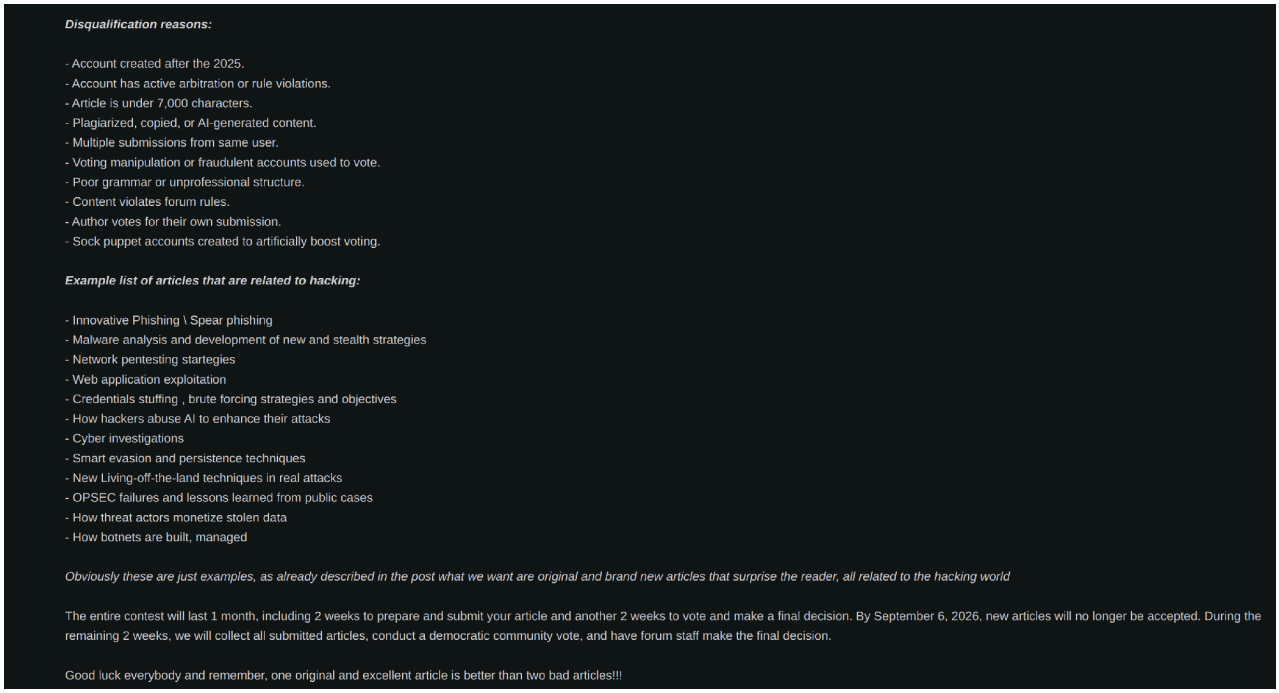
Article requirements:

- Minimum 7,000 characters, submissions below this will be rejected.
- Articles inherent in the world of hacking, no copy paste otherwise you will be excluded from participation. Any copied or repurposed material results in immediate disqualification.
- Good grammar and clear, professional structure required.
- Must include an introduction, body sections, and conclusion.
- No AI-generated content.
- No spam or off-topic content.

Submission process:

- Post a reply in this thread so we can bump and make more people participate!
- Your article will need to be posted on a separated thread with title: "[@caustic Contest] - [Your Article Title]", in /forum/35/, for quick review we recommend mentioning me or a forum staff

Caustic's post on Exploit
Source: ZeroFox Intelligence



Disqualification reasons:

- Account created after the 2025.
- Account has active arbitration or rule violations.
- Article is under 7,000 characters.
- Plagiarized, copied, or AI-generated content.
- Multiple submissions from same user.
- Voting manipulation or fraudulent accounts used to vote.
- Poor grammar or unprofessional structure.
- Content violates forum rules.
- Author votes for their own submission.
- Sock puppet accounts created to artificially boost voting.

Example list of articles that are related to hacking:

- Innovative Phishing \ Spear phishing
- Malware analysis and development of new and stealth strategies
- Network pentesting startegies
- Web application exploitation
- Credentials stuffing , brute forcing strategies and objectives
- How hackers abuse AI to enhance their attacks
- Cyber investigations
- Smart evasion and persistence techniques
- New Living-off-the-land techniques in real attacks
- OPSEC failures and lessons learned from public cases
- How threat actors monetize stolen data
- How botnets are built, managed

Obviously these are just examples, as already described in the post what we want are original and brand new articles that surprise the reader, all related to the hacking world

The entire contest will last 1 month, including 2 weeks to prepare and submit your article and another 2 weeks to vote and make a final decision. By September 6, 2026, new articles will no longer be accepted. During the remaining 2 weeks, we will collect all submitted articles, conduct a democratic community vote, and have forum staff make the final decision.

Good luck everybody and remember, one original and excellent article is better than two bad articles!!!

Caustic's post on Exploit (continued)
Source: ZeroFox Intelligence

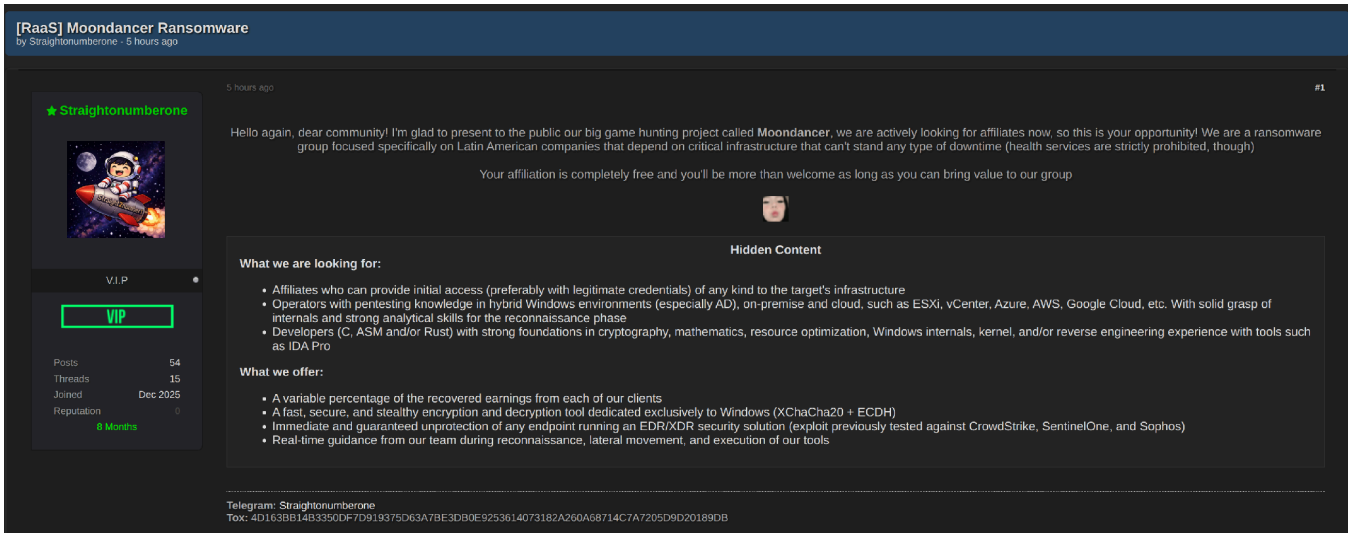
Ransomware Group Recruiting Affiliates to Target Latin America

On August 19, 2026, untested threat actor "Straightonumberone" announced that they were recruiting affiliates for their new ransomware-as-a-service (RaaS) operation, Moondancer, on the predominantly English-language dark web forum DarkForums. According to Straightonumberone, the group is targeting Latin American critical infrastructure entities, excluding healthcare services.

Straightonumberone joined DarkForums in December 2025 and has made 54 posts so far; however, ZeroFox did not observe any activity indicative of the actor's credibility within the forum. As of writing, the post has received 35 responses, most of which are generic comments such as "Ty" and "wow," while some users expressed interest in joining the operation.

Straightonumberone is allegedly recruiting affiliates who can provide:

- Initial access of a varied kind, likely for multiple targets
- Pentesting knowledge in certain hybrid operating system environments and major cloud platforms for reconnaissance
- Expertise in C, Assembly, or Rust; cryptography; and reverse engineering



Straightonumberone's post on DarkForums

Source: ZeroFox Intelligence

Straightonumberone claims that affiliation is free and that they offer affiliates ransomware tools designed to encrypt and decrypt files in return, along with capabilities allegedly intended to evade or disable security software used to detect and block cyberattacks. The actor also claims they will provide real-time operational guidance during reconnaissance, lateral movement, and execution, and that affiliates will receive a percentage of recovered ransom payments.

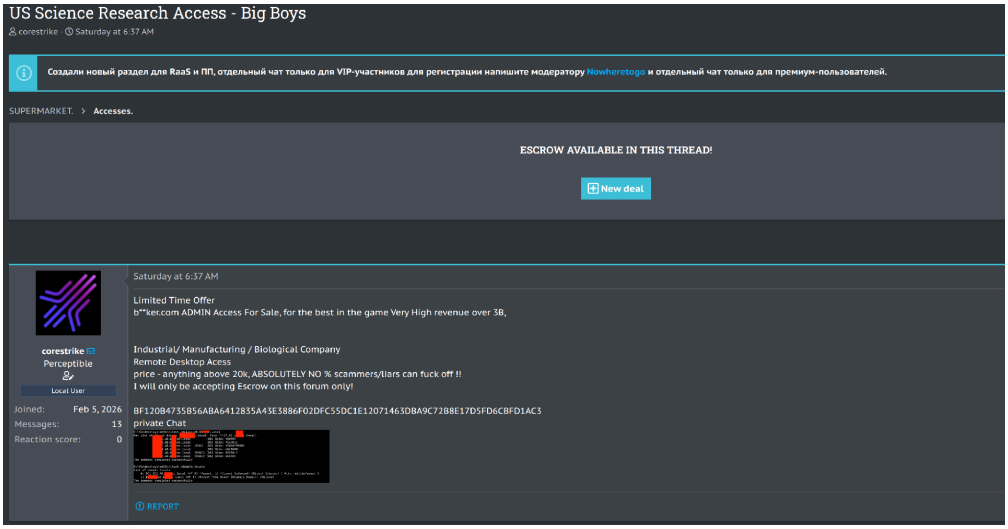
- This affiliate-based model, combined with the recruitment of initial access brokers and technically skilled operators, likely suggests an effort to build a more capable and scalable operation rather than conduct attacks independently.

Mexico is likely to remain a key area of interest given Straightonumberone's reported history of targeting Mexican organizations, while the group's claimed focus on critical infrastructure indicates potential expansion across other Latin American countries and sectors. The immediate threat level remains uncertain, as Moondancer's claims about its capabilities remain unverified, and there is no clear evidence yet of successful attacks under the new RaaS brand. However, ZeroFox assesses that the recruitment activity warrants continued monitoring for new affiliates, initial access sales, and reported victims, particularly among Latin American critical infrastructure organizations.

Initial Access to Research Company for Sale on ReHub

On August 15, 2026, untested threat actor “corestrike” announced unauthorized access to a U.S.-based scientific research company for sale on the dark web forum ReHub. The actor described the target company as operating in the industrial, manufacturing, and biological research sectors and allegedly generating more than USD 3 billion in annual revenue. Further, the actor partially disclosed the company's name (“b**ker[.]com”).

- Based on the available information, ZeroFox assesses that the target is likely Bruker Corporation, headquartered in Billerica, Massachusetts.
- Bruker provides scientific instruments and analytical solutions for life science, clinical, and materials research, with an annual revenue reportedly in the range of USD 3.4–3.5 billion.



Corestrike’s post on ReHub
Source: ZeroFox Intelligence`

Corestrike stated that the buyer would receive Remote Desktop Protocol (RDP) access to the company's network environment with administrative privileges. The actor indicated that offers below USD 20,000 would not be accepted.

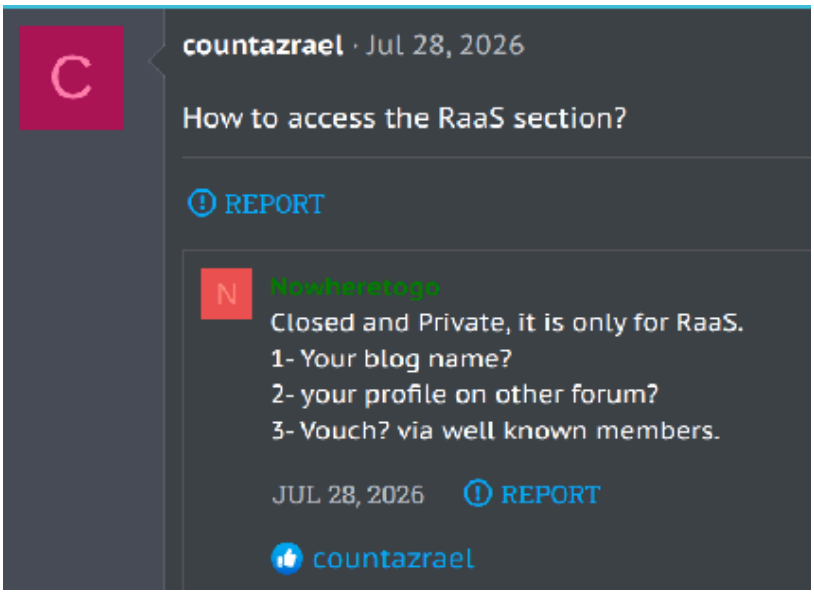
- This very likely represents an unusual initial access offering, as the seller disclosed sufficient information about the target for the company to be readily identifiable.

- There is currently no information indicating whether the actor has successfully sold the access.

Although the target will almost certainly be able to identify and investigate the advertised access, this does not necessarily eliminate the underlying risk. If the access is legitimate and remains active, threat actors would very likely use it as an initial foothold for network intrusion, data exfiltration, or ransomware deployment. Awareness of the advertised access also does not guarantee that the affected access path or vulnerable network segment will be identified and remediated.

New Ransomware Section for VIP Members on ReHub

On July 28, 2026, actor "Nowheretogo", who is a member of the ReHub forum's moderator team, announced that the forum had created a new section entirely dedicated to RaaS and Partnership Programs (PP) accessible only to VIP members.



Nowheretogo's post on ReHub
Source: ZeroFox Intelligence

- To gain access to this section, Nowheretogo stated that applicants must provide their blog name, their profiles on other forums, and vouches from established forum members.

ZeroFox assesses that the purpose of this action is to limit the presence of researchers and law enforcement, as well as to protect vetted RaaS collectives and other members from unverified scammers. There is a roughly even chance the ReHub community already has enough trusted actors capable of conducting illicit RaaS activity to support this closed section. Such a move from public to private activity represents a serious shift in the conventional DDW RaaS environment.

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.