ZEROFOX INTELLIGENCE

Brief

The Underground Economist: Volume 6, Issue 17

B-2026-08-13b

Classification: TLP:CLEAR

Criticality: LOW

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

August 13, 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 13, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | The Underground Economist: Volume 6, Issue 17

| Insider Access Advertised and Insider Recruitment on DarkForums

On August 9, 2026, untested threat actor "naloxone" offered insider access services at two large companies, DoorDash and T-Mobile, on the dark web forum DarkForums. According to the actor, two insiders can allegedly provide personally identifiable information (PII) held by either company associated with an email or phone number provided by the buyer, as well as other smaller services upon request.

- The actor noted that, if the targeted T-Mobile account chosen is SIM-protected or has any advanced account protection features enabled, the insiders will not be able to access information from those accounts; in these cases, the actor claims a refund will be issued to the buyer.

Interested buyers can receive the following information from the alleged DoorDash insider access:

- Full name
- Email and phone number
- Recent orders
- Home address
- Last four of a credit/debit card number used on the account

Interested buyers can receive the following information from the alleged T-Mobile insider access:

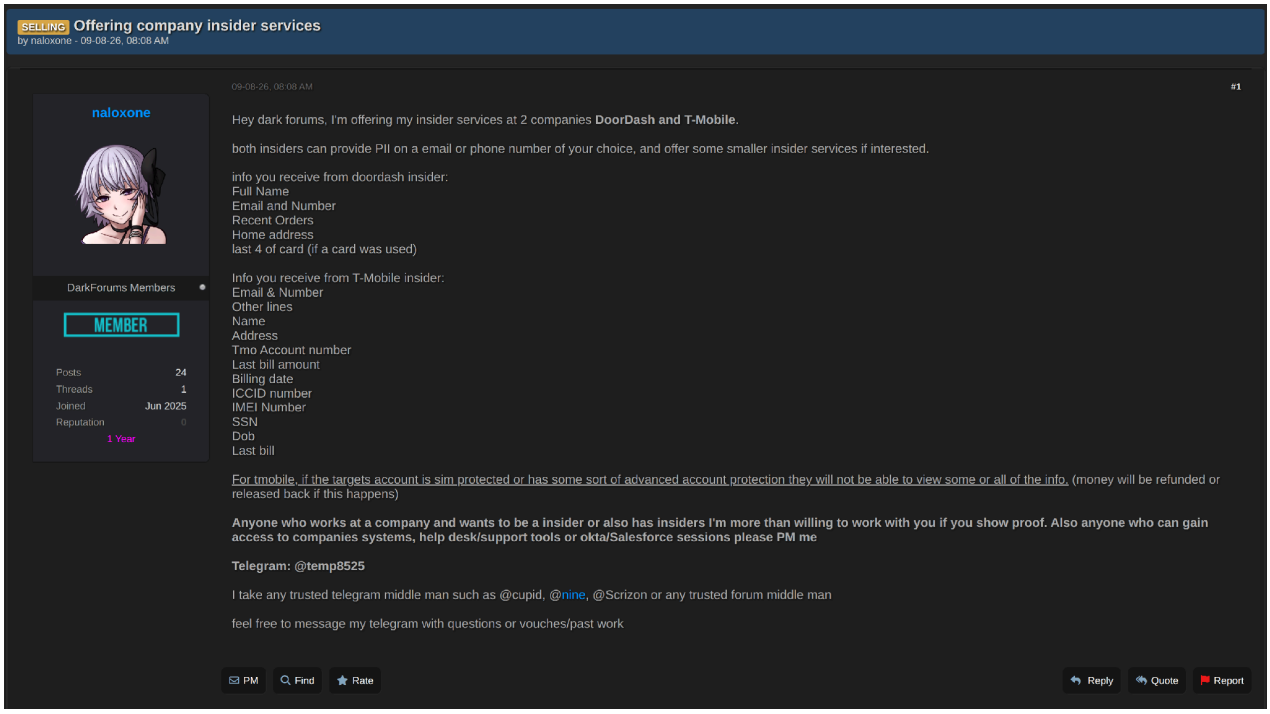
- Email and phone number
- Name
- Address
- T-Mobile account number
- Last bill amount
- Billing date
- Integrated Circuit Card Identifier (ICCID) number (unique serial number to identify specific SIM cards or eSIM profile globally)
- International Mobile Equipment Identity (IMEI) number (unique code to identify devices digitally on mobile networks)
- Social Security number
- Date of birth
- Last bill

The actor also solicited interested insiders with proof of access to any companies to contact them about potentially working together, almost certainly to sell their privileged insider information through naloxone once verified. The actor specifically requested insiders with access to company help desks, support tools, or OKTA/Salesforce accounts.

- ZeroFox has increasingly observed this sort of cooperative collaboration between insiders and threat actors on dark web marketplaces. The technique fosters an enhanced relationship whereby insiders very likely function as continuous, on-demand operators directly providing active, sustained, and real-time operational support for an actor's illicit campaign.

Naloxone is an untested threat actor with no reputation established on the forum, despite having joined in June 2025. However, this does not rule out the possibility that the actor possesses connections to insiders at DoorDash and T-Mobile at this time.
PII from major U.S.-based telecommunications and food delivery companies almost certainly could be used in social engineering campaigns. Specifically, information from

the alleged T-Mobile access is very likely to be used in SIM swapping scams, which would likely have a significant impact on victims.



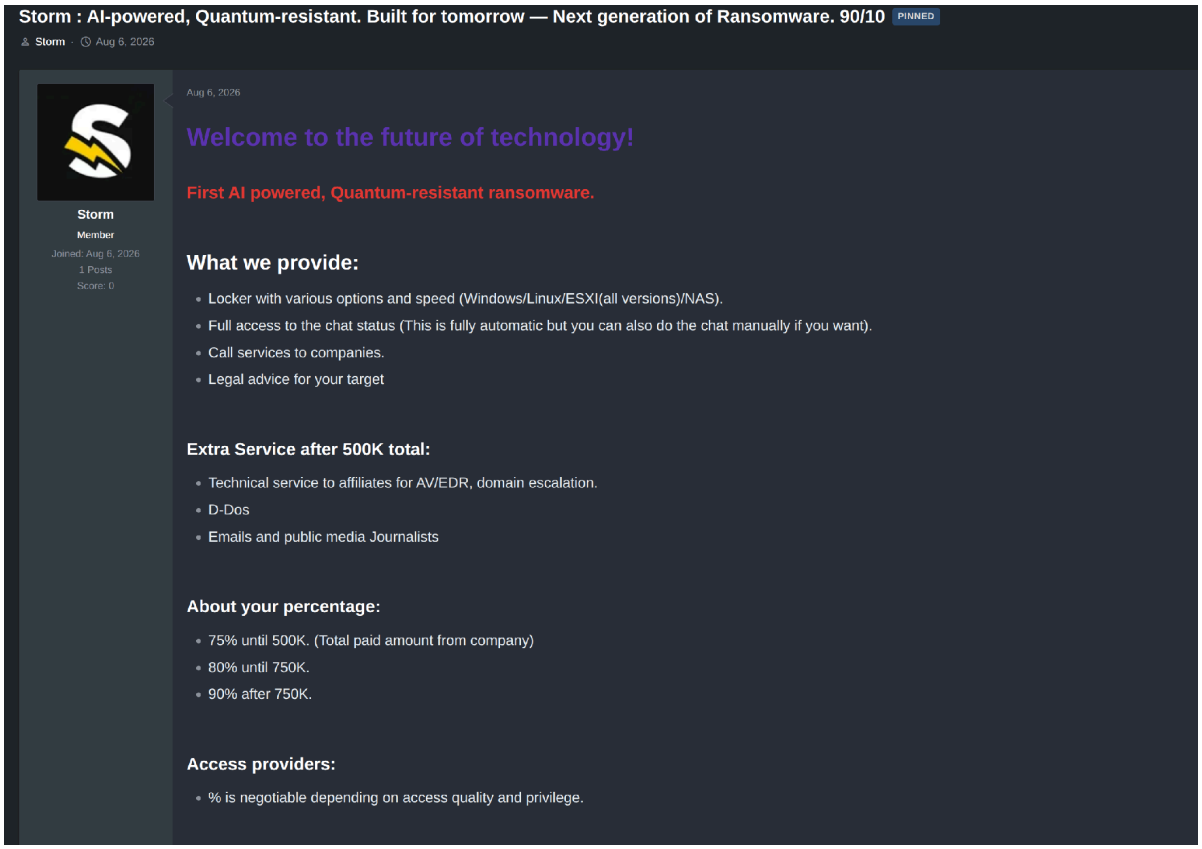
naloxone's original post on DarkForums
Source: ZeroFox Intelligence

Ransomware Operation Advertised as AI-Powered and Quantum-Resistant

On August 6, 2026, untested threat actor "Storm" advertised a new ransomware operation on the dark web forum T1erOne, describing it as the first artificial intelligence (AI)-powered, quantum-resistant ransomware. The actor had registered on the forum the same day, made no prior posts, and garnered no reputation score at the time of observation.

The advertisement additionally offers a range of affiliate support services, including victim communications, technical assistance, and extortion pressure tactics. Storm is recruiting affiliates and access providers, promoting a tiered revenue-sharing model that increases the affiliate share as ransom values rise:

- 75 percent of ransom proceeds up to USD 500,000
- 80 percent of proceeds up to USD 750,000
- 90 percent of proceeds thereafter



Storm's T1erOne post

Source: ZeroFox Intelligence

ZeroFox assesses that the alleged AI-powered designation very likely does not indicate a fully autonomous or AI-directed capability. Storm has not provided sufficient detail to determine the extent of any AI integration, which is more likely confined to assisting or automating discrete elements of the operation. Both the AI and quantum-resistance claims remain unverified and likely contain promotional or exaggerated elements intended to differentiate the offering in a crowded ransomware-as-a-service (RaaS) market.

- As of writing, ZeroFox is unable to confirm the credibility of Storm's claims, as the actor has not provided samples, demonstrations, or technical documentation supporting the advertised capabilities.

Despite Storm's limited history on T1erOne, the elevated affiliate payouts and breadth of the operational offering are likely to make the program attractive to experienced initial access brokers (IABs) and ransomware operators, particularly those seeking higher margins than established programs provide. Conversely, the actor's lack of forum tenure and reputation very likely constrains near-term recruitment, as prospective affiliates typically weigh operator trust heavily when selecting a program.

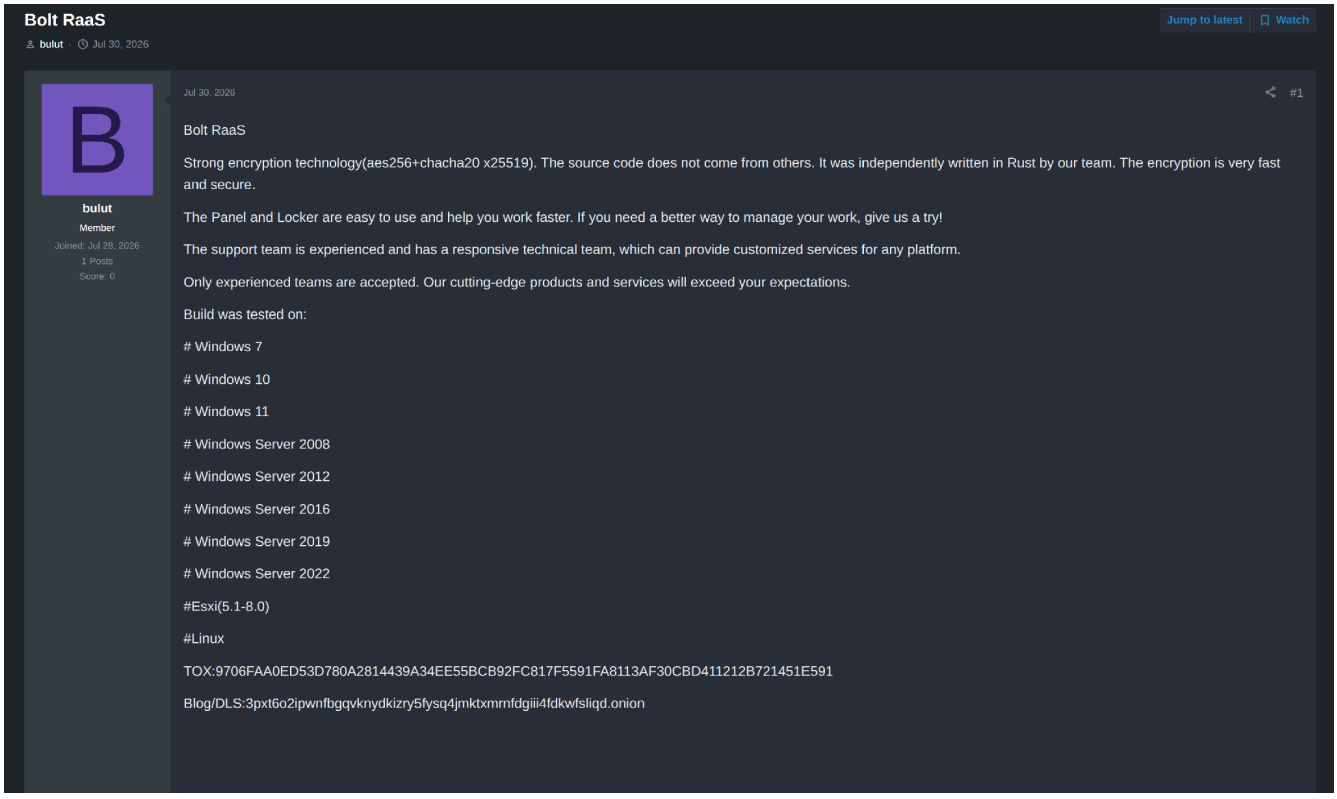
Bolt Ransomware Affiliate Program

On July 30, 2026, a threat actor using the alias "bulut" and claiming to speak on behalf of RaaS collective Bolt announced the group's partnership program on the T1erOne dark web forum—marking the first observed advertisement of Bolt on the platform. The actor promoted Bolt as an affiliate-only operation, stating that only experienced teams would be accepted.

Bulut further claims the malware employs a hybrid encryption scheme that combines sophisticated codes for key exchange, emphasizing encryption speed and reliability. Interested affiliates are instructed to establish contact via TOX. Several aspects of the advertisement are noteworthy.

- **Affiliate recruitment**: Restricting participation to "experienced teams" suggests the operators are very likely targeting established intrusion crews capable of conducting full-enterprise compromises.
- **Cross-platform capability**: Claimed support for Windows, Linux, and ESXi indicates the ransomware is likely designed to impact heterogeneous enterprise environments, including virtualization infrastructure commonly targeted during ransomware attacks.
- **Professionalized operations**: References to an affiliate panel, technical support, and customized services reflect the continued maturation of the RaaS ecosystem, whereby operators compete by offering operational tooling and support.

- **Modern implementation**: Development in Rust aligns with an ongoing trend among ransomware developers to adopt memory-safe languages that can facilitate cross-platform development and complicate reverse engineering.



bulut's post on T1erOne
Source: ZeroFox Intelligence

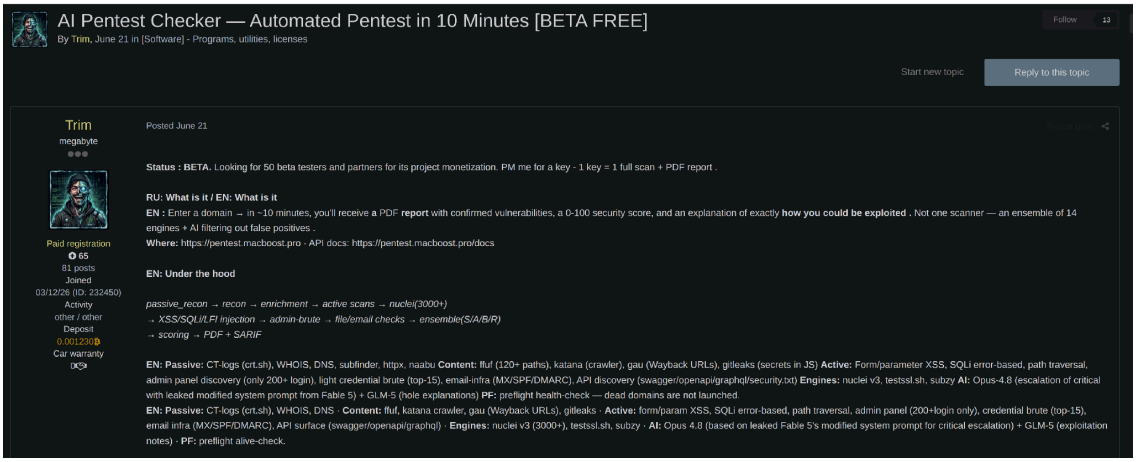
Bolt's appearance as a partnership program on T1erOne very likely expands the group's recruitment efforts and represents the first observed promotion of the RaaS on that forum, almost certainly increasing its visibility among experienced ransomware affiliates.

While the claims regarding encryption, platform support, and operational capabilities cannot be independently verified from the advertisement alone, the post indicates that Bolt is actively seeking affiliates and attempting to establish a presence within the cybercriminal ecosystem. Continued monitoring for subsequent affiliate activity, victim disclosures, and technical samples will be important to assess the group's operational maturity and threat level.

Threat Actor "Trim" Seeks Pentesters and Partners for Beta Reconnaissance Platform

On June 21, 2026, well-regarded threat actor "Trim" advertised on dark web forum Exploit a beta version of a security assessment platform providing automated domain reconnaissance, vulnerability scanning, API discovery, and report generation against a target domain. The actor is actively recruiting up to 50 beta testers and monetization partners.

- Trim claims the service delivers comprehensive results via PDF and JSON/SARIF formats approximately 10 to 15 minutes after a scan. Access to the platform is managed through single-use keys, with one key authorizing a single complete domain scan.
- The platform allegedly brings together well-known, open-source security tools into a centralized workflow. The tools include Nuclei, Katana, ffuf, testssl.sh, subfinder, httpx, naabu, gau, gitleaks, and subzy. It also features an AI layer designed to filter false positives, prioritize findings, assign a zero to 100 security score, and generate contextual exploitation narratives.
- Additionally, the service allegedly exposes an API for integration into automated workflows and claims to support the continuous discovery of newly registered domains via certificate transparency and WHOIS monitoring.



Threat actor seeks pentesters for AI-assisted vulnerability scanner
Source: ZeroFox Intelligence

Trim's intent to recruit monetization partners very likely indicates an intention to turn the security assessment platform into a cybercrime-as-a-service (CaaS) operation. While the platform does not claim to introduce novel exploitation techniques or previously unknown vulnerabilities, it likely lowers the operational effort required to conduct reconnaissance and vulnerability assessments against targets at scale as compared to manual reconnaissance.

- Trim's security assessment platform's alleged ability to provide contextual exploitation narratives sets it apart from commercially available vulnerability assessment pipelines, likely enabling less-skilled threat actors to efficiently identify and attempt to exploit potentially vulnerable internet-facing assets.

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.