ZEROFOX INTELLIGENCE

Brief

The Underground Economist: Volume 6, Issue 14

B-2026-07-02b

Classification: TLP:CLEAR

Criticality: LOW

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

July 2, 2026

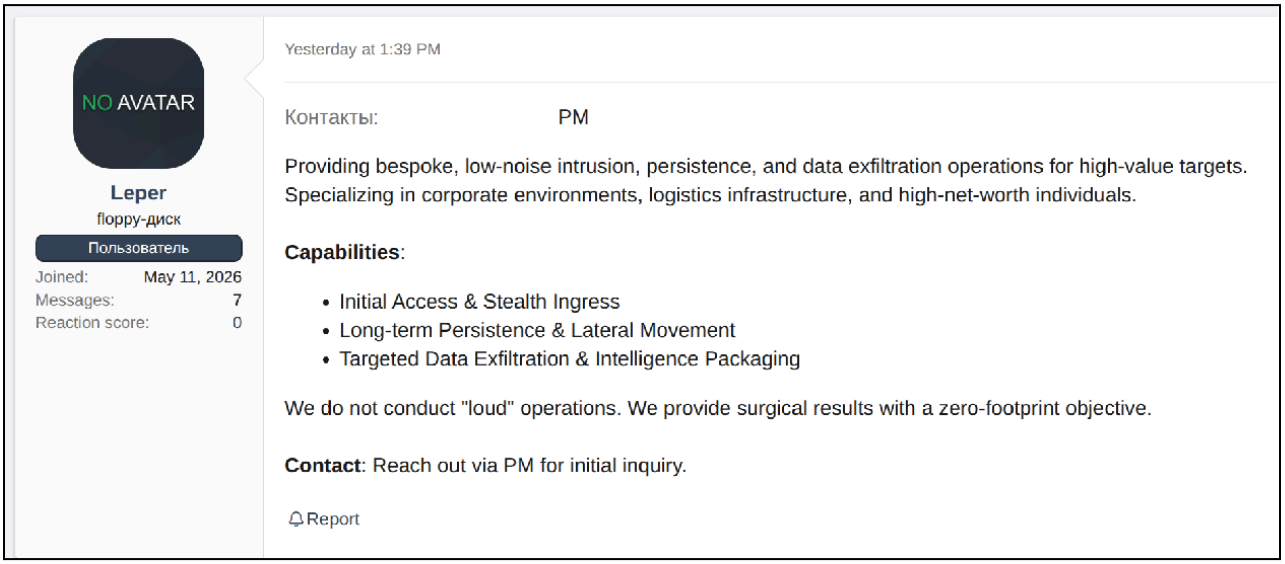
ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot 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 July 2, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | The Underground Economist: Volume 6, Issue 14

| Threat Actor Offering Bespoke Services on Dark Web

On June 30, 2026, untested threat actor "Leper" posted on the dark web forum XSS advertising bespoke services for silent intrusions, persistence, and data exfiltration operations targeting high-value organizations and individuals. The actor claimed to be part of a group specializing in corporate environments, logistics infrastructure, and high-net-worth individuals. Leper advertised the following capabilities:

- Initial access and stealth ingress
- Long-term persistence and lateral movement
- Targeted data exfiltration and intelligence packaging



Leper's XSS post
Source: ZeroFox Intelligence

The actor emphasized that the group conducts "silent" and "surgical" operations designed to not leave traces behind. As of writing, ZeroFox is unable to verify these claims due to the absence of supporting evidence and the actor's lack of an established positive reputation on the forum. However, based on the nature of the advertised services, the group does not appear to fit the profile of a typical Initial Access Broker (IAB). Instead, the offering suggests a focus on highly targeted intrusion operations, likely involving organizations and individuals with significant cryptocurrency holdings.

StealC Version 2 Source Code for Sale

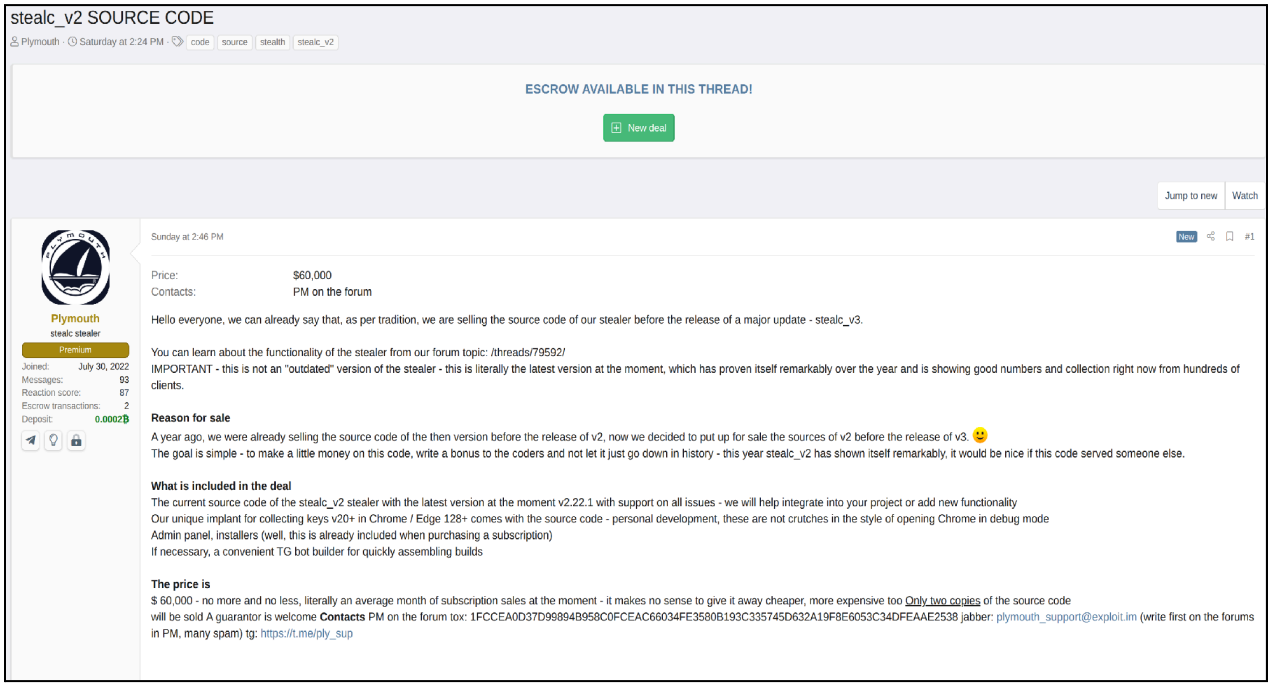
On June 27, 2026, prominent threat actor "Plymouth" announced on the XSS forum that they were selling two copies of the source code for StealC version 2, each priced at USD 60,000.

- Plymouth is the alleged owner of the StealC infostealer project.
- Selling source code of an infostealer before releasing a new version is a common practice among threat actors.
- ZeroFox assesses that StealC version 3 is likely to be released soon as a major update.

Plymouth emphasized the source code for sale is not an outdated version but rather a fully functional and up-to-date infostealer that has already been responsible for millions of infections over the past year.

- StealC is one of the five most active infostealer malware families currently, alongside Vidar, Rhadamanthys, Lumma, and Acreed.

The threat actor claims the primary reason for selling the version 2 source code is to generate additional revenue while ensuring the continued operation of the already successful malware by transferring ownership to other operators. However, there is a roughly even chance the sale is an effort to raise additional funds for the completion of the version 3 upgrade.



Plymouth's post on XSS
Source: ZeroFox Intelligence

The offer includes an allegedly proprietary implant designed to extract cryptographic keys from Chromium-based browsers, including Chrome and Edge (versions 128 and later). Plymouth claims the implant is an internally developed capability and emphasizes it does not rely on publicly known techniques such as launching browsers in debug mode. The offering also includes an administrative panel, deployment installers bundled

with the subscription, and an optional Telegram-based builder intended to streamline the creation and customization of malware builds.

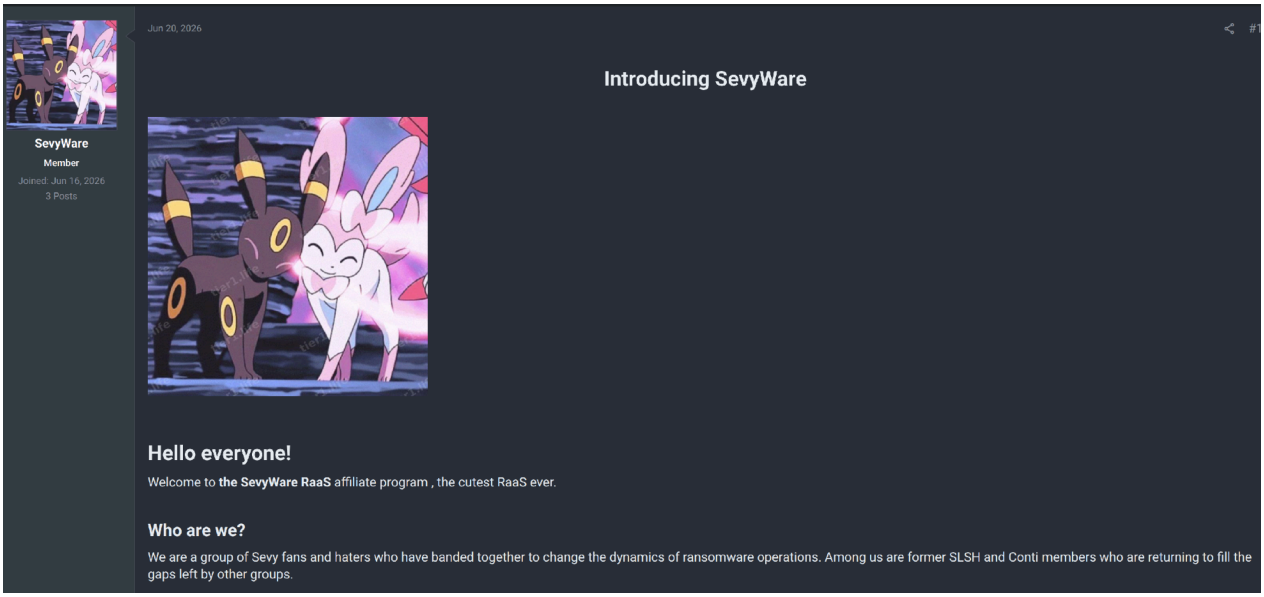
- In an update to the post, Plymouth claimed that one of the two copies of the source code had already been sold.

ZeroFox assesses that threat actors will very likely continue to use StealC version 2 in their attacks in the near term. There is also a roughly even chance that version 2 will continue to be used after the release of version 3. However, use of StealC version 3 will almost certainly eclipse that of version 2 by the end of 2026 and will likely be a popular option for threat actors upon its release.

Threat Actor Launches Violence-Backed RaaS Program

On June 20, 2026, untested threat actor "SevyWare" announced the launch of a ransomware-as-a-service (RaaS) affiliate program called SevyWare on the dark web forum T1erOne, claiming the operation involves former members of Scattered Lapsus$ Hunters (SLSH) and Conti. The operation reportedly seeks to recruit affiliates with IAB capabilities and insider access, offers violence-as-a-service (VaaS), and claims to follow a payment model that offers 90 percent of ransom proceeds to its affiliates.

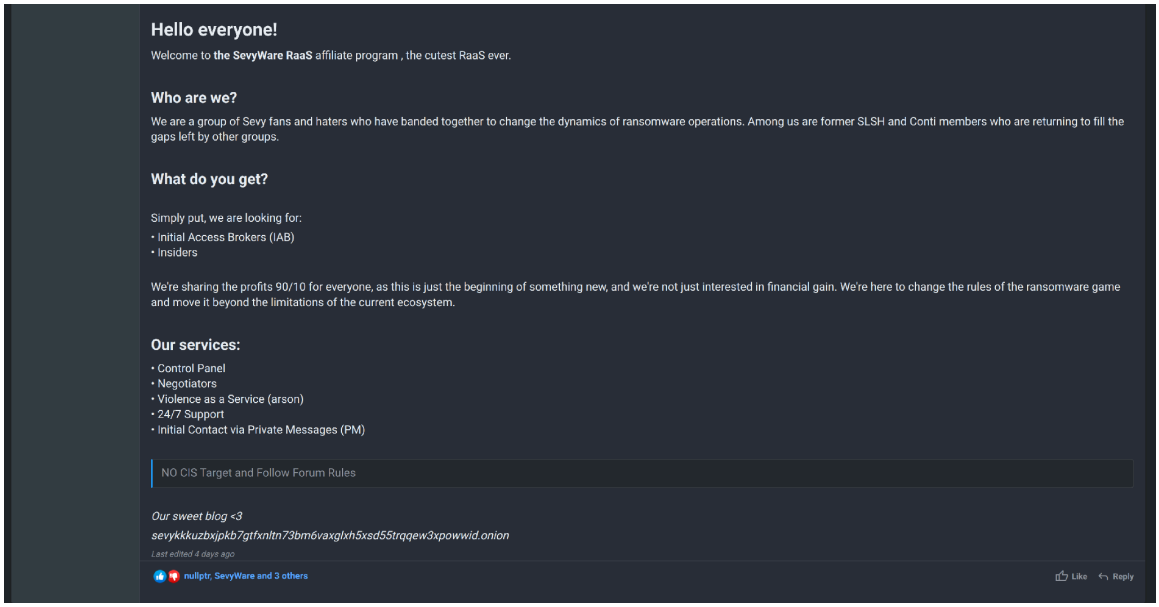
- The payment model is likely to draw the attention of financially motivated actors.
- As of writing, ZeroFox could not independently verify SevyWare's claimed affiliations, operational capabilities, or advertised services.
- Although the group has established a dedicated dark web leak site, ZeroFox did not observe any victims listed on the portal at the time of writing.



SevyWare's post on T1erOne
Source: ZeroFox Intelligence

SevyWare joined T1erOne on June 16, 2026, and has posted three times to date on the forum. ZeroFox has observed significant negative commentary from forum members regarding the actor's post about the RaaS program, with several commenters questioning both the legitimacy of the operation and the credibility of its advertised services.

- Forum member "Anubis" criticized SevyWare's proposal, arguing that promoting physical violence could increase law enforcement scrutiny and negatively impact the broader ransomware ecosystem.
- Another commenter, "Aels", opposed the advertised physical attacks on targeted entities, stating that destroying a victim's assets eliminates the funds needed to pay a ransom.



Features of SevyWare RaaS listed on T1erOne
Source: ZeroFox Intelligence

The RaaS allegedly includes features such as an administrative control panel, negotiation services, 24/7 operational support, and private-message-based onboarding. The stated VaaS specifically mentions arson. However, the actor presented no evidence demonstrating the capability to conduct or facilitate physical attacks.

- Physical intimidation is becoming increasingly common in ransomware campaigns, with approximately 40 percent of global incidents in 2025 involving threats of physical harm against employees of targeted organizations.[1]
- In May 2026, the Federal Bureau of Investigation (FBI) released an advisory about Silent Ransom Group (SRG) conducting physical security breaches against victim infrastructure, in addition to utilizing routine social engineering techniques.[2]

If the claims about the RaaS's features are true, the alleged combination of cyberattacks and physical coercion is likely to enable the group to accelerate and escalate its attacks. However, at this stage, ZeroFox is unable to verify SevyWare's capabilities due to limited availability of information about its tactics, techniques, and procedures (TTPs).

[1] hXXps://www.bbc[.]com/news/articles/cr71d8vyjv0o
[2] hXXps://www.ic3[.]gov/CSA/2026/260526.pdf

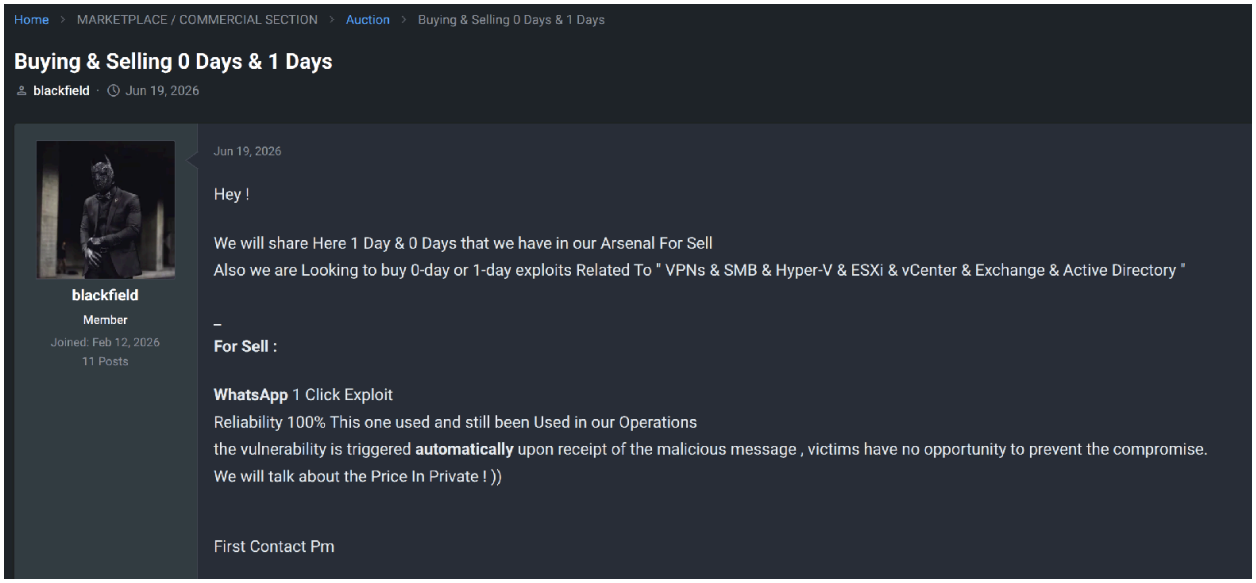
Despite an observed trend of increasing use of physical intimidation in ransomware attacks, SevyWare's claim about offering such a service remains largely unsubstantiated and has been met with skepticism from members of the T1erOne forum. Hence, there is a roughly even chance that the VaaS offering is not legitimate. Further, the absence of listed victims on the leak site and the nascent age of SevyWare's account on the forum suggest that the post is likely a recruitment and awareness campaign intended to establish presence on the forum and attract affiliates.

Threat Actor Seeks Enterprise Zero-Days and Advertises WhatsApp Exploit

On June 19, 2026, moderately credible threat actor "blackfield" advertised the sale of alleged zero-day and one-day exploits on T1erOne, including a WhatsApp one-click exploit. Additionally, the actor sought to purchase zero-day and one-day exploits targeting widely used enterprise infrastructure. Blackfield has not disclosed any prices in their post or made it clear whether they are making a sale-only post, a trade offer, or both.

- Blackfield joined T1erOne on February 12, 2026.
- ZeroFox notes that this activity on T1erOne is blackfield's first observed appearance since the disruption of the dark web forum Russian Anonymous Marketplace (RAMP), where an actor using the same handle—likely the same individual—was active.

The actor claims that the WhatsApp one-click exploit is "100% reliable," actively used in operations, and automatically compromises targets upon their receipt of a malicious message. The other vulnerabilities the actor is seeking are associated with Virtual Private Networks (VPNs), Server Message Block (SMB), Hyper-V, ESXi, vCenter, Exchange, and Active Directory (AD). ZeroFox was unable to verify the technical details of the claimed WhatsApp vulnerability and its capabilities.



blackfield's post seeking and advertising exploits on T1erOne

Source: ZeroFox Intelligence

Since blackfield is actively buying and selling exploits, the actor is likely seeking to expand and diversify their capabilities for future malicious cyber operations. The technologies the actor is seeking to exploit (VPNs, Exchange, AD, Hyper-V, ESXi, and vCenter) facilitate initial access, privilege escalation, lateral movement, and compromise of virtualized infrastructure, indicating an interest in capabilities that support end-to-end network intrusions.

- It is likely that blackfield is advertising the alleged WhatsApp exploit alongside their request for specific zero-days and one-days to increase the visibility and credibility of the post, thereby encouraging other forum users to offer for purchase or trade the exploits the actor is seeking.

Blackfield's alleged WhatsApp exploit is likely to attract some attention within the cybercriminal community due to WhatsApp's widespread adoption. If the claimed one-click exploit is genuine, it is likely to present a significant risk to high-value individuals (including corporate personnel and executives) by enabling unauthorized access to devices, data theft, or surveillance or facilitating further compromise of targeted environments. However, as of writing, ZeroFox is unable to verify blackfield's claims or the exploit's legitimacy and capabilities.

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 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.