ZEROFOX INTELLIGENCE

Brief

The Underground Economist: Volume 6, Issue 15

B-2026-07-16b

Classification: TLP:CLEAR

Criticality: LOW

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

July 16, 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 16, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

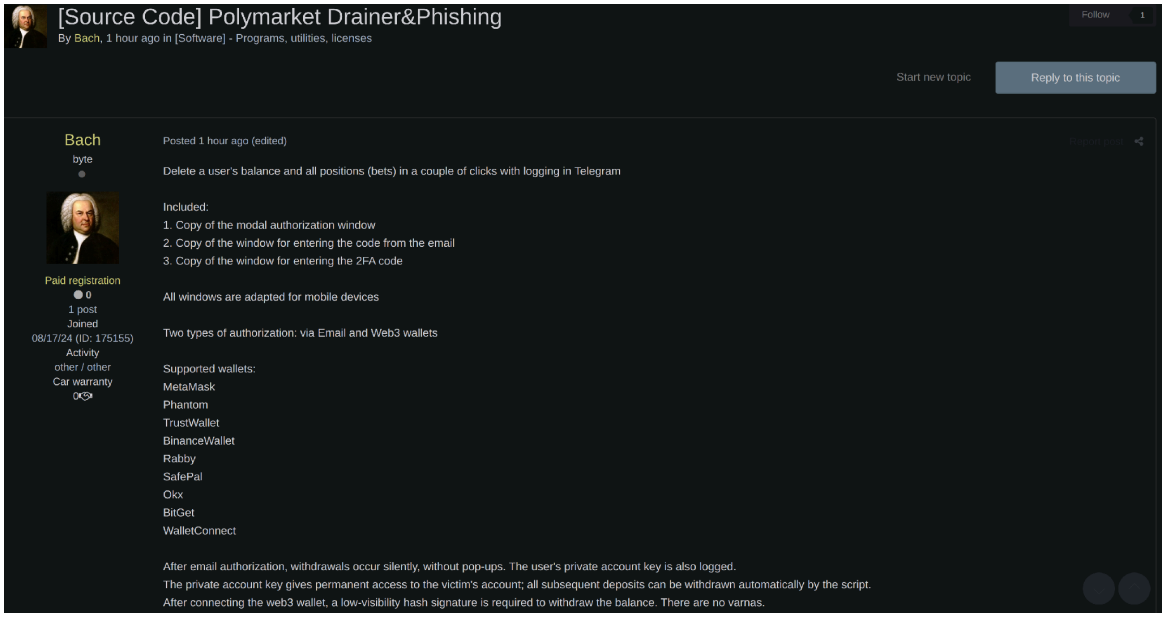
| Brief | The Underground Economist: Volume 6, Issue 15

| Phishing and Drainer Kit Targeting Polymarket for Sale

On July 15, 2026, untested threat actor "Bach" advertised the source code for a sophisticated drainer and phishing kit targeting the cryptocurrency-based prediction platform Polymarket on the dark web forum Exploit. The actor claimed the kit can drain users' account balances and liquidate all bets and positions in just a few clicks while sending activity logs to Telegram. Bach listed the source code for sale for USD 10,000.

The kit allegedly supports email-based and Web3 authentication for the following cryptocurrency wallets:

- MetaMask
- Phantom
- Trust Wallet
- Binance Wallet
- Rabby Wallet
- SafePal
- OKX Wallet
- Bitget Wallet
- WalletConnect



Bach's original post on Exploit
Source: ZeroFox Intelligence

According to the advertisement, the kit captures users' account credentials, enabling persistent unauthorized access and the automated theft of future deposits. Bach further claimed that withdrawals can be executed with minimal user visibility after a wallet is connected by leveraging a low-profile transaction-signing process designed to reduce the likelihood of detection or user intervention.

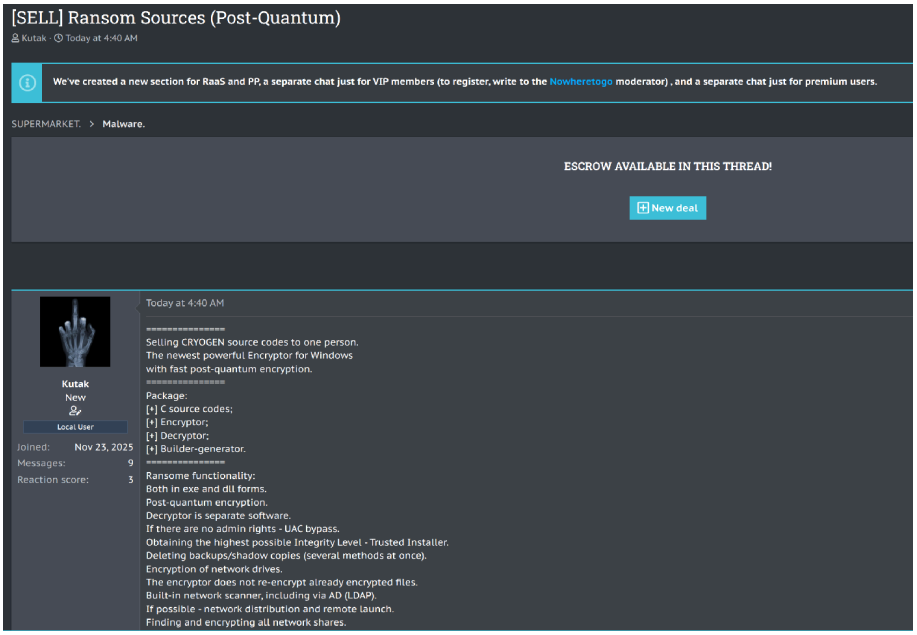
ZeroFox assesses that phishing and drainer kits targeting Polymarket are almost certain to become more prevalent and sophisticated over time, as the platform continues to attract millions of users and gain broader adoption.

CRYOGEN Ransomware Source Code for Sale

On July 15, 2026, moderately credible, Russian-language threat actor "Kutak" advertised the sale of source code for CRYOGEN ransomware on the dark web forum ReHub. According to the actor, CRYOGEN is a modern Windows ransomware framework designed to target both workstations and servers using a fast, post-quantum cryptographic algorithm intended to complicate decryption efforts.

Kutak is allegedly offering a complete ransomware development package, including the source code, encryptor, decryptor, and a builder-generator for creating customized payloads. Based on the advertisement, CRYOGEN supports privilege escalation, Active Directory discovery, network share encryption, configurable propagation, deletion of backups and shadow copies, configurable file and directory exclusions, and hardware-bound decryption.

- The ransomware also employs configurable partial ("zebra") encryption using National Institute of Standards and Technology (NIST)-standardized cryptographic algorithms while preserving file metadata and avoiding the re-encryption of previously encrypted files.
- Instead of dropping ransom notes into every directory, the malware reportedly delivers ransom notifications through multiple Windows interfaces.



Kutak's original post on ReHub
Source: ZeroFox Intelligence

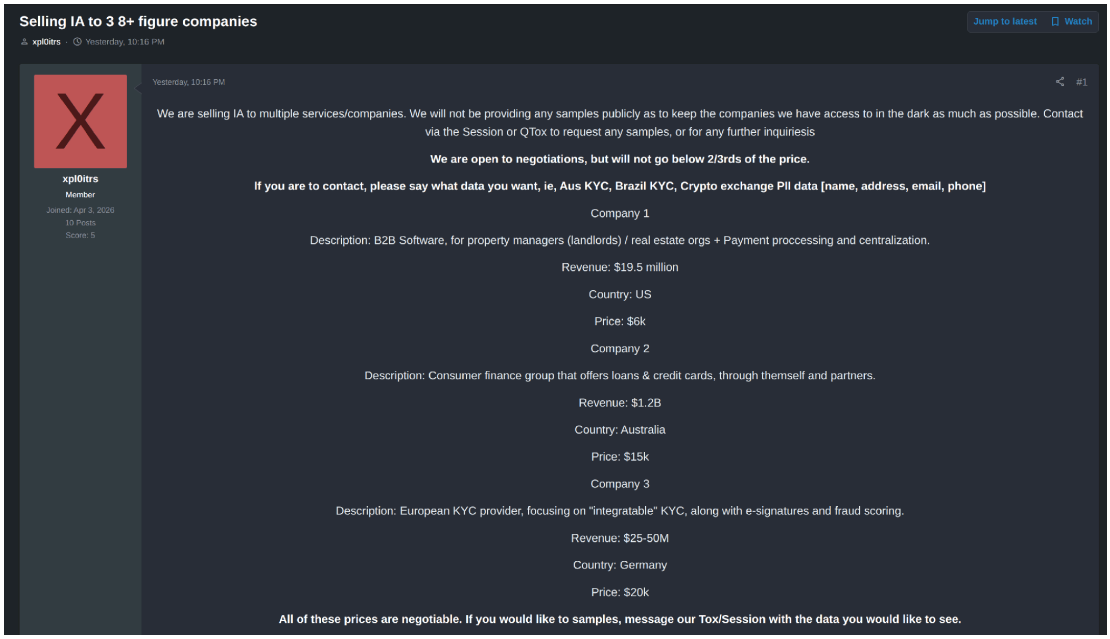
Unlike traditional ransomware-as-a-service (RaaS) offerings, the seller claimed the source code will be transferred exclusively to a single buyer for USD 50,000 and will not be operated under an affiliate model, positioning the sale as a one-time transfer of ownership. The sale allegedly includes:

- The complete C project
- A Microsoft Visual C++ (MSVC) build environment
- Initial deployment assistance
- Limited maintenance

The availability of a mature, enterprise-focused ransomware framework with exclusive ownership will likely increase the occurrence of future targeted attacks by a well-resourced threat actor. Although ZeroFox cannot independently verify the seller's claims regarding the ransomware's capabilities, the advertised functionality aligns with features commonly observed in advanced ransomware families targeting corporate Windows environments and very likely represents a risk of sophisticated ransomware attacks in the near term.

Initial Access to Multiple Companies Advertised on Dark Web

On July 14, 2026, prominent threat actor "xpl0itrs" advertised initial access to multiple companies and service providers across several geographic regions on the dark web forum T1erOne. The actor stated that no samples would be disclosed publicly, likely in an effort to keep the accesses secure and vet prospective buyers before sharing further details.



xpl0itrs' T1erOne post
Source: ZeroFox Intelligence

In the post, xpl0itrs claimed to hold access to three organizations: a U.S.-based business-to-business (B2B) software company with an estimated annual revenue of USD 19.5 million, an Australian consumer finance group offering loans and credit cards with an estimated annual revenue of USD 1.2 billion, and a European Know Your Customer (KYC) and fraud score provider with an estimated annual revenue between USD 25 million and USD 50 million.

- This advertisement comes less than a month after xpl0itrs announced access to multiple organizations valued in the tens of billions of dollars, stating their intention to leverage the compromises for maximum financial gain.
- The actor has drawn sustained attention over the past three months following a string of high-profile incidents; they have been linked to alleged compromises of Dynatrace, BMW Group, and Sportradar AG, as well as the exposure of approximately 57 million Chinese electronic medical and insurance-related records.

ZeroFox assesses that xpl0itrs is unlikely to monetize these three companies directly. The actor will likely achieve greater financial return by reselling the initial access to other

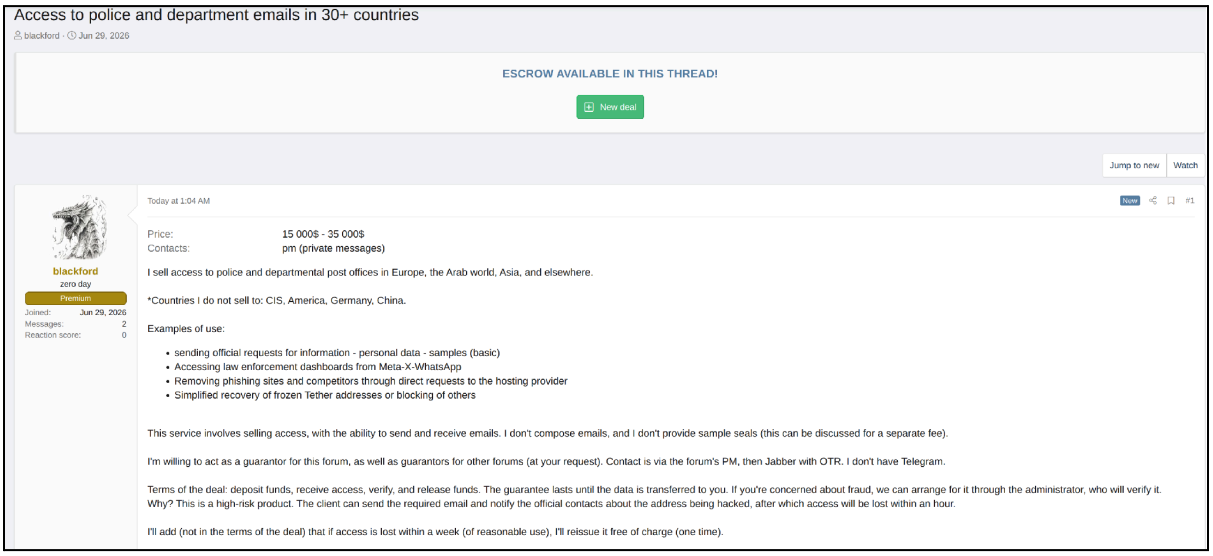
threat actors rather than conducting their own extortion campaign—consistent with the threat actor's established pattern of brokering rather than operating. ZeroFox further assesses that xpl0itrs is likely retaining access to larger, more high-value organizations for future operations and using smaller sales such as this one to sustain cash flow and reputation on T1erOne in the interim.

Threat Actor Advertises Access to Police and Government Email Accounts

On June 29, 2026, untested threat actor "blackford" advertised the sale of access to the email accounts of police and other government departments from more than 30 countries in Europe, the Middle East, and Asia on the dark web forum XSS. The actor quoted prices between USD 15,000 and USD 35,000, depending on the number of email accounts.

- Additionally, blackford stated that they do not sell access to users from the Commonwealth of Independent States (CIS), “America,” Germany, and China. The specification likely reflects an effort to avoid detection by law enforcement or indicates proximity to the actor's own residence. However, ZeroFox assesses that the actor would likely be unable to filter out buyers from these regions if they utilize a virtual private network (VPN) to conceal their locations.
- The actor claimed the access can be used to send official information requests (including for personal data and documentation); register with or access law enforcement portals operated by Meta, X, and WhatsApp; submit takedown requests to hosting providers targeting rival criminal infrastructure; and facilitate the freezing or recovery of Tether (USDT) wallets.

The actor claimed that buyers would receive the ability to send and receive emails using the compromised accounts. However, they stated that email drafting services are not included in the offering and that they would provide sample messages or customized communications only through separate negotiations and for an additional fee.



blackford's post on XSS

Source: ZeroFox Intelligence

ZeroFox assesses that the description of the access suggests the data, if legitimate, was likely obtained through infostealer logs or an adversary-in-the-middle phishing attack. Such logs typically capture credentials and session cookies, enabling attackers to bypass multi-factor authentication (MFA). The offer to "reissue" access likely indicates an active log feed or phishing infrastructure.

- Despite the plausibility of methods, the claims are unlikely to be legitimate, given that the actor neither has any prior posting history on XSS nor has provided any free samples.
- Furthermore, ZeroFox assesses the asking price is disproportionately high for a database of unspecified volume and countries. Paying a steep price for freezing or taking down rival infrastructure would likely be a costly endeavor for threat actors.
- This type of data is likely most useful for phishing, social engineering, and impersonation activities. ZeroFox assesses the actor's claim that the accesses can be used to enable the unfreezing of crypto wallets is unlikely, absent further independent verification.

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 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.