ZEROFOX INTELLIGENCE

Profile

Krybit

P-2026-04-28a

Classification: TLP:AMBER

Criticality: Medium

Intelligence Requirements: Threat Actor, Ransomware, Dark Web

April 28, 2026

Profile | Krybit

Created on: April 27, 2026
Intelligence Cut-off: 7:00 AM (EST) on April 27, 2026

Key Findings

- Krybit is a ransomware and digital extortion (R&DE) collective active since at least April 3, 2026, that publishes victim information on its dark-web hosted blog; the collective has claimed at least 19 victims so far.
- Krybit is very likely financially motivated; neither its dark web leak site nor its public statements on dark web forums, social media, or covert communication channels indicate any political stance, ideological messaging, or affiliation with a specific cause.
- Krybit employs a double extortion model, as indicated by the file encryption experienced by known victims, as well as the ransom note left behind in confirmed attacks.
- On April 13, 2026, rival ransomware collective 0APT exploited a vulnerability in Krybit's backend database, gaining access to Krybit's victim data set, among other data. Subsequently, on April 15, 2026, Krybit revealed its own counterattack against 0APT, defacing 0APT's leak site and publicly releasing its full source code and operational logs. This response likely indicates that, beyond its core financial objectives, Krybit is willing to allocate resources to retaliatory actions to safeguard its reputation.
- ZeroFox assess Krybit is a low-to-medium sophistication, immature ransomware-as-a-service (RaaS) provider that warrants continued monitoring, given its expanding platform capabilities and infrastructure.

First Observed	April 3, 2026
Origin	Country Unknown
Alias	N/A
Motivation	Financial Gain
Targeted Industries	- Transportation - Professional Services - Education - Manufacturing - Food/Agriculture - Energy
Targeted Nations	- United States - Germany - Mexico - Japan - Austria - Botswana - China - Brazil - Spain - South Africa - New Zealand - Romania - Thailand
Tools	Unknown; but likely unsophisticated based on victim security stack
	Note: This list should not be treated as exhaustive.

Krybit overview

Source: ZeroFox Intelligence

History

Krybit is an R&DE collective active since at least April 3, 2026, that publishes victim information on its dark-web hosted blog. Since claiming its first victim, the collective has allegedly conducted at least 19 attacks—an average of more than one attack per day.

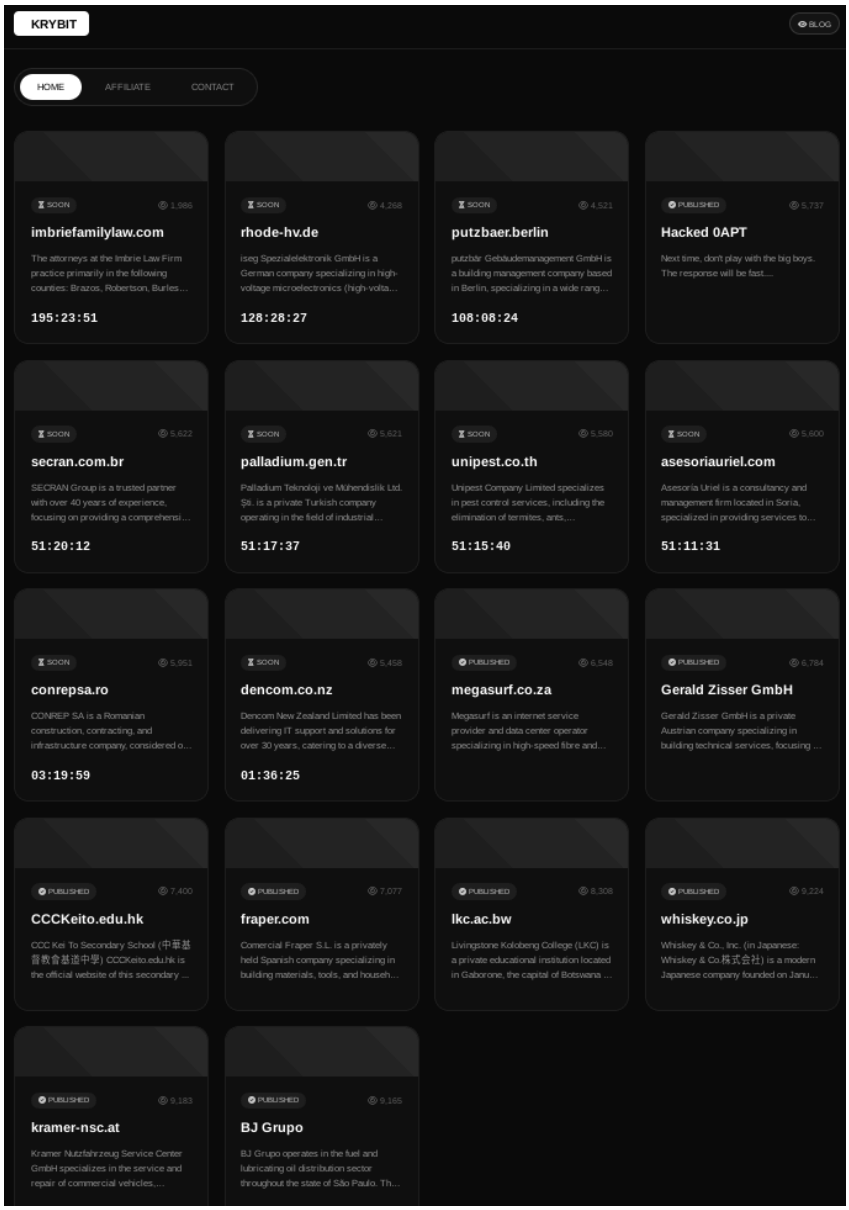
- Krybit published its first victim on its leak site on April 3, 2026. This initial victim was followed by four additional targets on the same day and a further 15 in the weeks since.
- The group established a Tor-based data leak site, alongside a negotiation portal that includes a custom-built chat interface. The implementation of features such as Cross-Site Request Forgery (CSRF) protection and anti-spam rate limiting suggests deliberate, pre-planned developmental capabilities.

Motivations and Victim Profile

Krybit is very likely financially motivated; neither its dark web leak site nor its public statements on dark web forums, social media, or covert communication channels such as Telegram indicate any political stance, ideological messaging, or affiliation with a specific cause. Instead, Krybit's victim selection indicates opportunistic targeting.

- In its short time of activity, Krybit has targeted several industries and regions, with no established pattern typical of most RaaS collectives. This seemingly random attack profile very likely suggests an opportunistic, access-driven approach to targeting.
- Krybit's targeted sector distribution is weighted slightly to consumer and professional services; education, technology, energy, and manufacturing account for the remainder of industries.
- Krybit's geographic spread covers the United States, Germany, Mexico, Japan, Austria, Botswana, China, Brazil, Spain, South Africa, New Zealand, Romania, and Thailand. While this victim profile is seemingly random, it notably does not include any targets in Russia. This indicates Krybit is likely a Russian-language collective based somewhere in the Commonwealth of Independent States (CIS), as its

targeting profile is consistent with collectives that seek to avoid Russian law enforcement scrutiny.



Victims listed on Krybit's leak site

Source: ZeroFox Intelligence

Tactics, Techniques, and Procedures (TTPs)

Krybit employs a double extortion model, as indicated by the file encryption experienced by known victims, as well as the ransom note left behind in confirmed attacks. The double extortion approach involves both encrypting the victim's files and exfiltrating sensitive data from compromised systems. Victims are provided with instructions on how to initiate contact with the group to negotiate ransom payment.

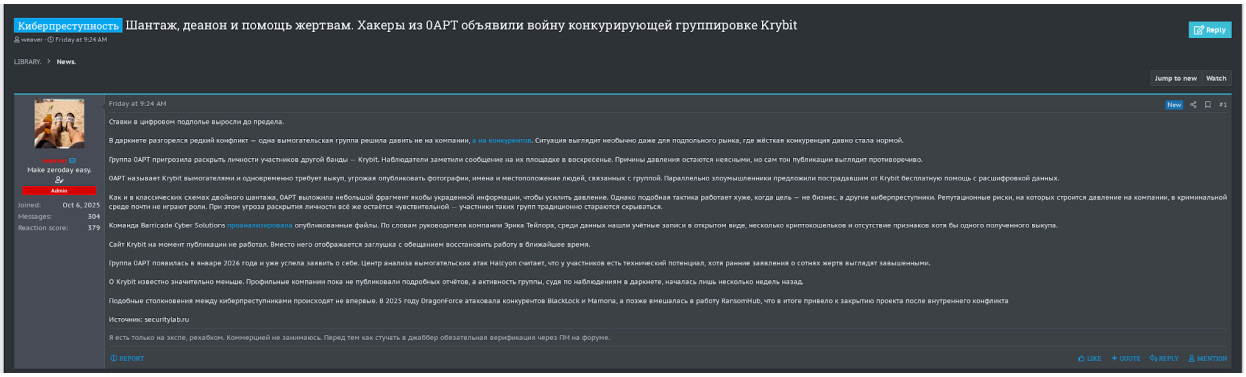
- Initial access is likely gained via public-facing web applications, such as WordPress and reCAPTCHA. Krybit operators likely exploit misconfigured web panels and database interfaces, which are likely supplemented by credentials sourced from initial access brokers.
- Krybit's victims all share a similar technology stack (including the use of WordPress, reCAPTCHA, and PHP), Windows and Linux hosting, and Microsoft 365 and Exchange management.
- No confirmed victims thus far have deployed a complex or hardened cybersecurity technology stack.

ZeroFox considers Krybit an immature, low-to-medium sophistication collective. In its short time on the RaaS scene, Krybit has conducted a relatively large number of attacks; however, its technology stack and random victim profile indicate a developing capability rather than a fully mature threat actor. Given the speed of the group's deployment and development thus far, there is a roughly even chance Krybit will become a more mature and dangerous threat over the next year.

Rivalry with 0APT

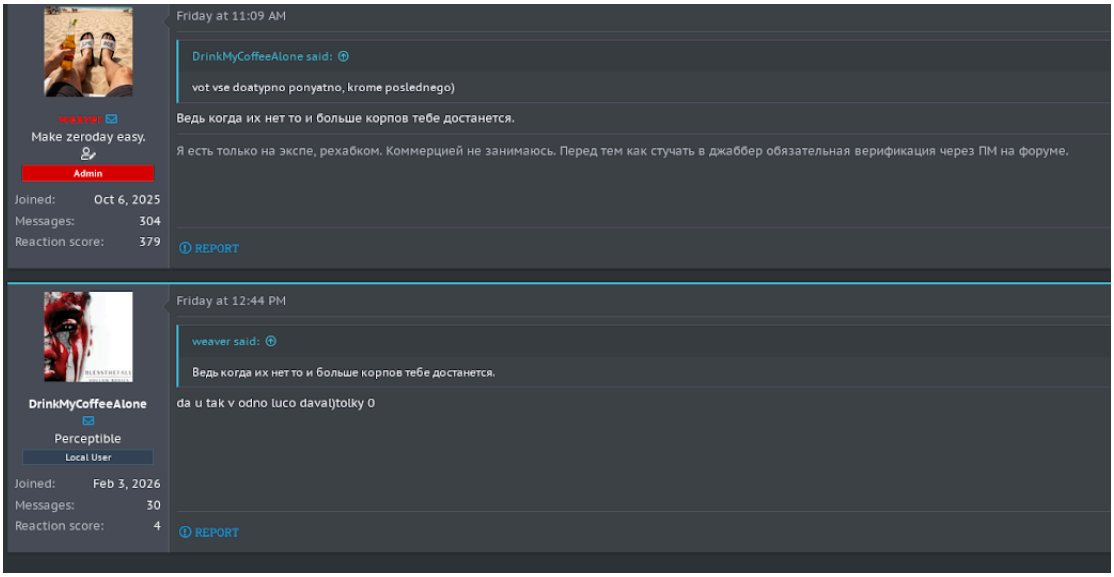
On April 13, 2026, rival ransomware collective 0APT exploited a vulnerability in Krybit's backend database, gaining access to Krybit's victim data set, among other data. The leaked data revealed significant operational security deficiencies on the part of Krybit (including plaintext password storage), as well as victim negotiation records showing zero payments across at least 13 victims.

On April 17, 2026, a post on the Russian-language cybercrime forum ReHub detailed 0APT's attack against Krybit. The post was made by a ReHub administrator known by the alias "weaver", who summarized available open-source information detailing the rivalry between 0APT and Krybit.



Original ReHub post by weaver

Source: ZeroFox Intelligence



Observation by weaver that competitors benefit from Krybit removal

Source: ZeroFox Intelligence

According to weaver, 0APT listed Krybit as a victim on its own dark web leak site, threatened to reveal the identities of Krybit operatives, and offered free decryption services to Krybit's victims. Forum responses have been limited but point to a likely belief

among threat actors that opportunistic cybercriminals will seek to inherit Krybit's victim pipeline.

Subsequently, on April 15, 2026, Krybit revealed its own counterattack against 0APT, defacing 0APT's leak site and publicly releasing its full source code and operational logs. The released material revealed that 0APT had been operating its infrastructure on Android-hosted servers, likely substantially damaging its credibility on criminal forums. Krybit publicly posted: "Next time, don't play with the big boys. The response will be fast."

- This response likely indicates that, beyond its core financial objectives, Krybit is willing to allocate resources to retaliatory actions to safeguard its reputation.

Krybit is a new, but active, RaaS group with multi-platform encryption and an aggressive posture. Its rapid deployment of attacks against a wide variety of victims across multiple regions and sectors demonstrates a very likely financially motivated group attempting to make money as fast as possible. Further, its quick response and counteroffensive against 0APT likely suggest a group willing to devote resources to protect its reputation in the cybercrime underground.

ZeroFox assesses Krybit is a low-to-medium sophistication, immature RaaS provider that operates a fairly standard business model with an outdated technology and security stack. Operational security failures, such as plaintext password storage, very likely indicate a lack of technological development that would have to be overcome if Krybit were to become a more dangerous threat.

However, while Krybit warrants continued monitoring, given its expanding platform capabilities and infrastructure, the group has yet to be established as a mature or reliable operation at this stage.

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%