[KRYBIT] - Ransomware Victim: Hacked 0APT - RedPacket Security

By April 14, 2026

Published: 2026-04-14 · Archived: 2026-04-17 02:04:49 UTC

NOTE: No files or stolen information are exfiltrated, downloaded, taken, hosted, seen, reposted, or disclosed by RedPacket Security. Any legal issues relating to the content should be directed at the attackers, not RedPacket Security. This blog is an editorial notice informing that a company has fallen victim to a ransomware attack. RedPacket Security is not affiliated with any ransomware threat actors or groups and will not host infringing content. The information on this page is automated and redacted whilst being scraped directly from the KRYBIT Onion Dark Web Tor Blog page.

Ransomware group:

KRYBIT

Victim name:

HACKED 0APT

AI Generated Summary of the Ransomware Leak Page

The leak page published for the technology company identified as Hacked 0APT is attributed to the threat actor group Krybit. The post is dated 2026-04-14 20:21:55.235455 and identifies Hacked 0APT as the victim in this incident. The post does not specify a precise compromise date; instead, it presents the publication date as the reference point for when the exposure or data status was publicly disclosed. The content suggests a hostile post aimed at the victim, with a terse message indicating that “Next time, don’t play with the big boys. The response will be fast….” While the exact nature of the impact (whether data was encrypted, leaked, or otherwise exfiltrated) is not explicitly stated in the available text, the post documents intent to publicly pressure the victim and signals that a confrontation or post-exploitation claim is being made.

The page contains no visual material such as screenshots or images, and there are no downloadable files associated with the post. A claim URL is noted as present within the leak page, though no direct link is included here. Redacted content in the public-facing excerpt does not reveal specific data types or ransom figures. The observed framing is consistent with a ransomware-leak style post where the attackers threaten fast responses in response to the victim’s actions, but there is no explicit statement of a monetary demand or data categories within the provided text. The focus remains on the victim’s identity (Hacked 0APT) and the threat actor’s message rather than on disclosed data specifics.

Support Our Work

A considerable amount of time and effort goes into maintaining this website, creating backend automation and creating new features and content for you to make actionable intelligence decisions. Everyone that supports the site helps enable new functionality.

If you like the site, please support us on Patreon or Buy Me A Coffee using the buttons below.

AI APIs OSINT driven New features

Buy Me A Coffee Patreon

Post navigation
