

[SHADOWBYT3\$] - Ransomware Victim: UMSA - RedPacket Security

By September 10, 2026

Published: 2026-02-25 · Archived: 2026-09-13 02:00:20 UTC

 [Read with OpenAI](#)

 image

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 SHADOWBYT3\$ Onion Dark Web Tor Blog page.

Ransomware group:

SHADOWBYT3\$

Victim name:

UMSA

AI Generated Summary of the Ransomware Leak Page

The leak page associated with the victim UMSA, attributed to the threat group ShadowByt3\$, appears as a data-exfiltration post published on 2026-02-17 at 17:00:00. The available metadata indicates a reference to a file labeled “UMSA_LEAK.7z,” suggesting that the attackers claim to have exfiltrated data from the organization and are presenting a compressed archive as part of the leak. The post does not provide a clear statement of the industry, operational impact, or a specified ransom demand within the available fields. The absence of an explicit compromise date beyond the post date means the published timestamp serves as the primary temporal marker for this event in the leak listing.

Regarding the content and presentation of the page, there is no evidence of included screenshots or other images within the provided data (the record shows zero images and zero downloads). The post references an archive file name but does not disclose additional visible artifacts or graphics in the metadata. In keeping with standard ransomware reporting, the incident is described here as a data-leak event rather than a confirmed encryption-only incident, though the exact scope and nature of affected data remain unspecified in the available details. PII or contact information is not present in the summary, and the victim name “UMSA” is preserved as issued. The absence of visible images or links means there are no additional visual proofs to reference in this summary.

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

Source: <https://www.redpacketsecurity.com/shadowbyt3-ransomware-victim-umsa/>