

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:46:01 UTC

Description([Varonis](#)) The Darkside ransomware attack campaigns stood out for their use of stealthy techniques, especially in the early stages. The group performed careful reconnaissance and took steps to ensure that their attack tools and techniques would evade detection on monitored devices and endpoints.

While their initial entry vectors vary, their techniques are more standardized once inside, and their endgame is coldly efficient.

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=f1c9260c-3f22-42ce-a6fc-eed1a89e5c64>