

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:52:13 UTC

Description([Check Point](#)) Once OSX/Dok infection is complete, the attackers gain complete access to all victim communication, including communication encrypted by SSL. This is done by redirecting victim traffic through a malicious proxy server.

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=7816abd3-afe2-413c-a0f8-5c080d92ed82>