

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:43:27 UTC

Description Clop is a ransomware which uses the .clp extension after having encrypted the victim's files. Another unique characteristic belonging with Clop is in the string: 'Dont Worry C|0P' included into the ransom notes. It is a variant of [CryptoMix](#) ransomware, but it additionally attempts to disable Windows Defender and to remove the Microsoft Security Essentials in order to avoid user space detection.

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=8792eefb-d852-4a24-ad09-46614ef7a815>