LevelBlue - Open Threat Exchange

By dekaRituraj

Archived: 2026-04-06 01:04:44 UTC

FileHash-SHA1: 1 | **FileHash-SHA256:** 10 | **Domain:** 1 | **Hostname:** 2

In late June 2018, Unit 42 revealed a previously unknown cyber espionage group we dubbed Rancor, which conducted targeted attacks in Southeast Asia throughout 2017 and 2018. In recent attacks, the group has persistently targeted at least one government organization in Cambodia from December 2018 through January 2019. While researching these attacks, we discovered an undocumented, custom malware family – which we've named Dudell. In addition, we discovered the group using Derusbi, which is a malware family believed to be unique to a small subset of Chinese cyber espionage groups.
