LevelBlue - Open Threat Exchange

By AlienVault

- Created 5 years ago by AlienVault
- Public
- TLP: White

FileHash-MD5: 5 | **FileHash-SHA1:** 5 | **FileHash-SHA256:** 10

Threat Actors make use of packers when distributing their malware as they remain an effective way to evade detection and to make them more difficult to analyze. In this blogpost, Blueliv shows how to unpack TA505 packed samples using the Qiling Framework emulator version 1.2, which will allow us to do so, without needing to study and replicate all the implementation details of the unpacking algorithm.
