

The compromised host is running Linux so we have a number of persistence mechanisms available to us. The first option which, is arguably the most straightforward is to add a public key that we control to the `authorized_keys` file at `/root/.ssh/`. Using `docker-compose` also allows us to specify automatic restarts which increases the backdoor's resilience.