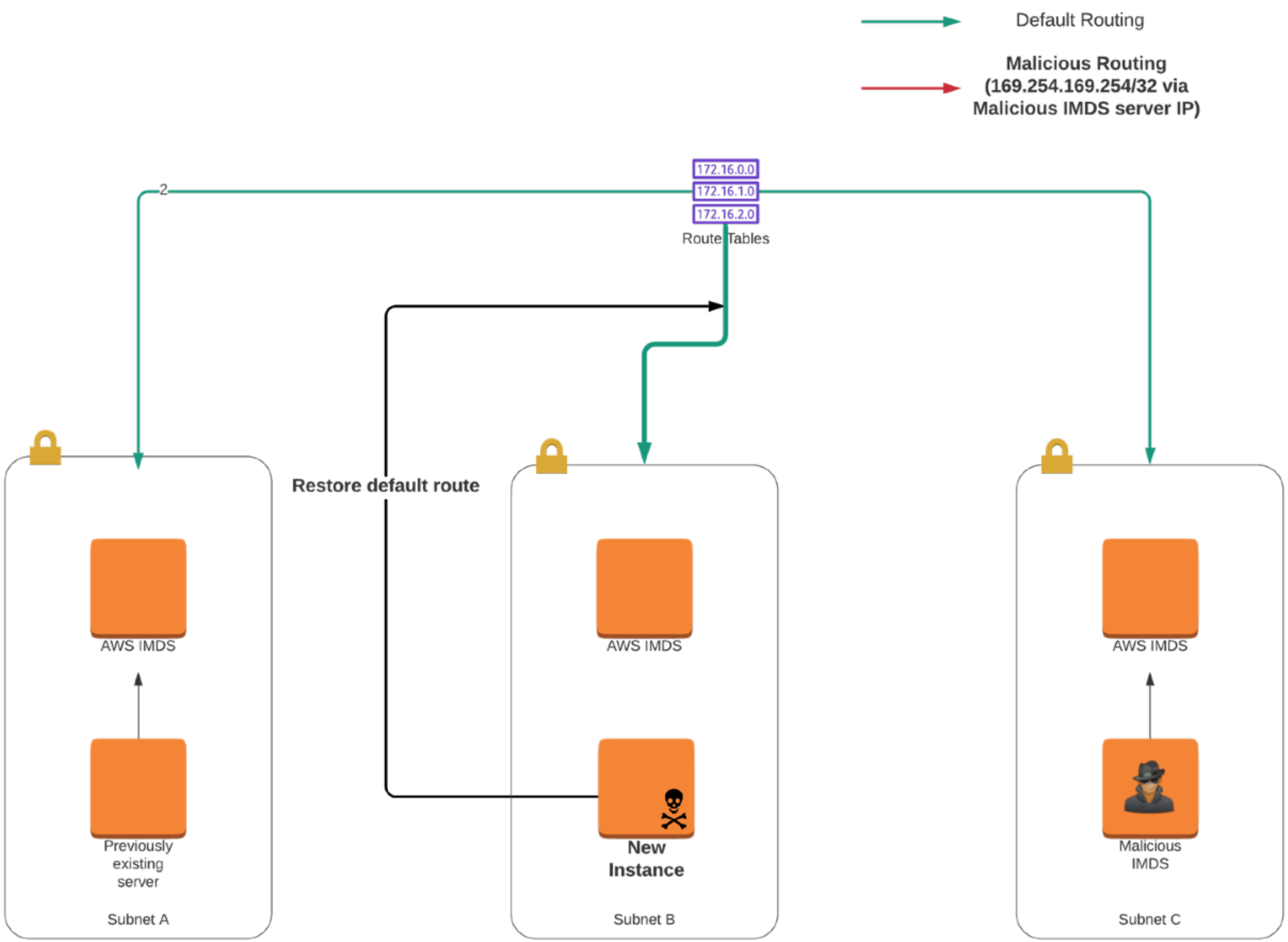
AWS IMDS Persistence/Priv escalation

Ryan Gerstenkorn | November 29, 2020



Notes

The now comprimised new instance does the following.

1. Restore default route

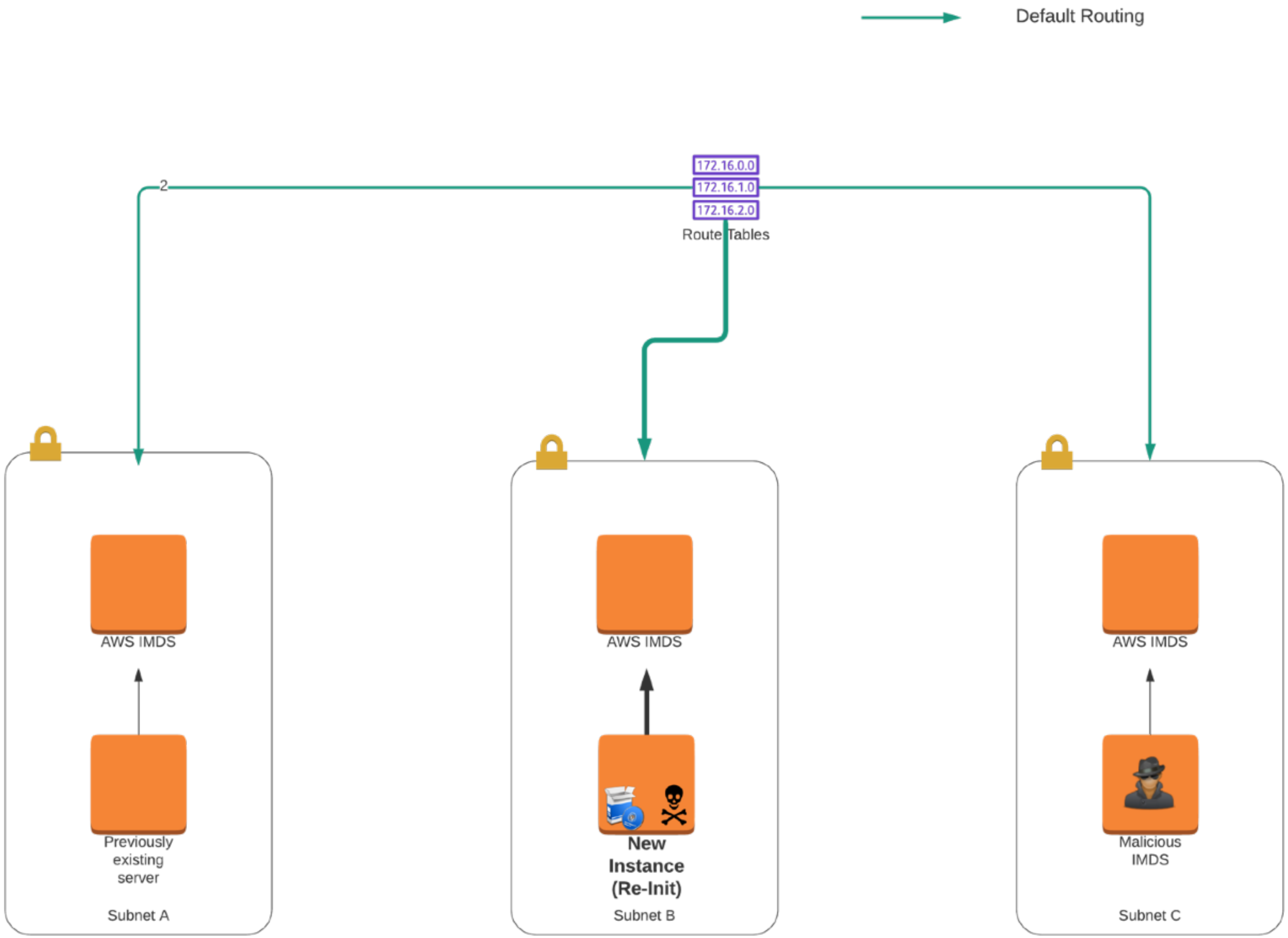
2. Clear cloud-init data

3. Reboot

Hardcoded credentials served via the user data from the malicious IMDS server can be used to restore the default route.

AWS IMDS Persistence/Priv escalation

Ryan Gerstenkorn | November 29, 2020



Notes

On reboot the new rooted instance will rebootstrap with the default user data and work as expected from the end user's view.