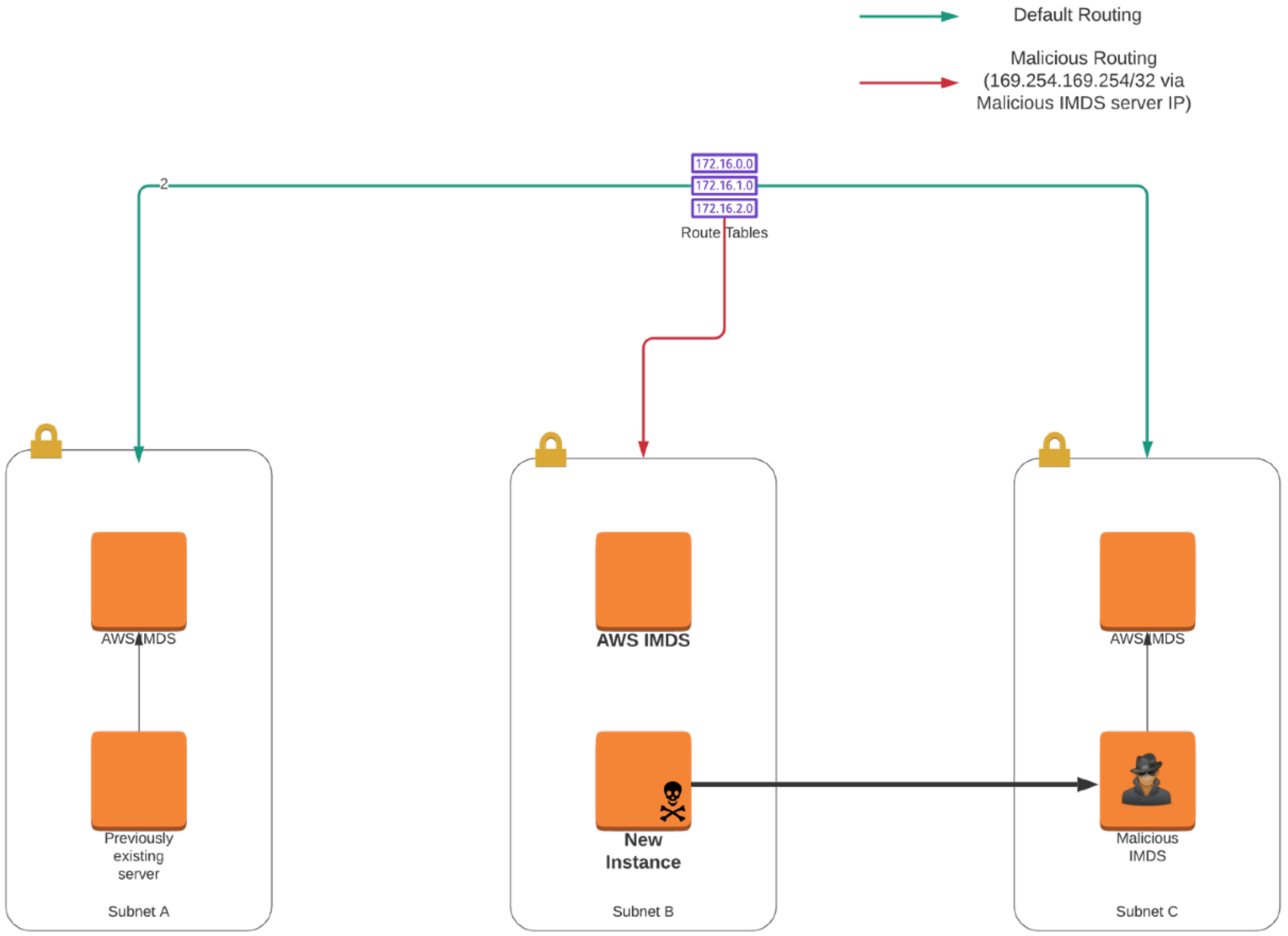
AWS IMDS Persistence/Priv escalation

Ryan Gerstenkorn | November 29, 2020



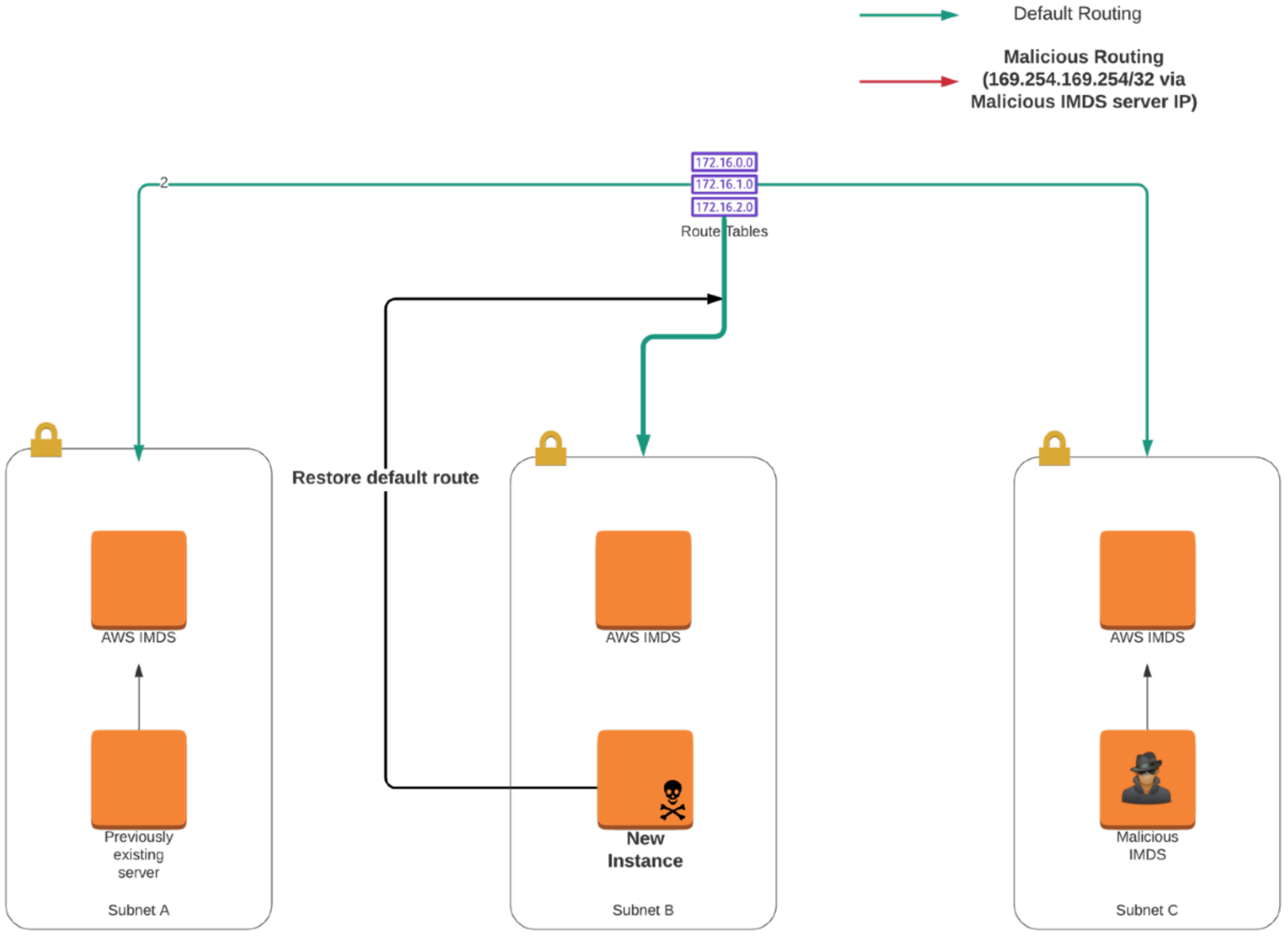
Notes

The new instance connect's to the malicious IMDS server in subnet C and and then executes the returned user data as root.

It's possible that other already operational instances in subnet B will experience issues during this time.

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.