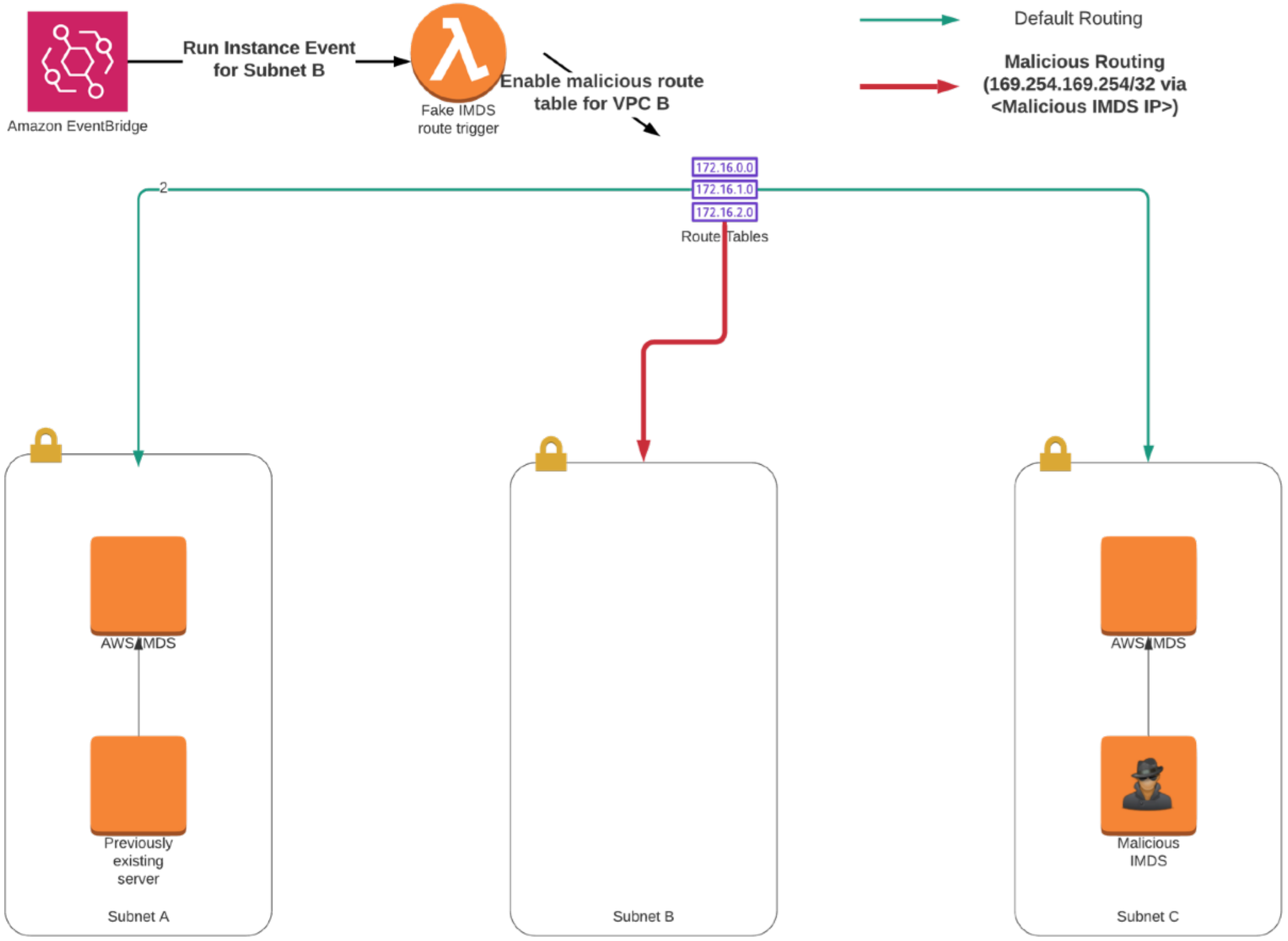
AWS IMDS Persistence/Priv escalation

Ryan Gerstenkorn | November 29, 2020



Notes

1. RunInstance API is called.

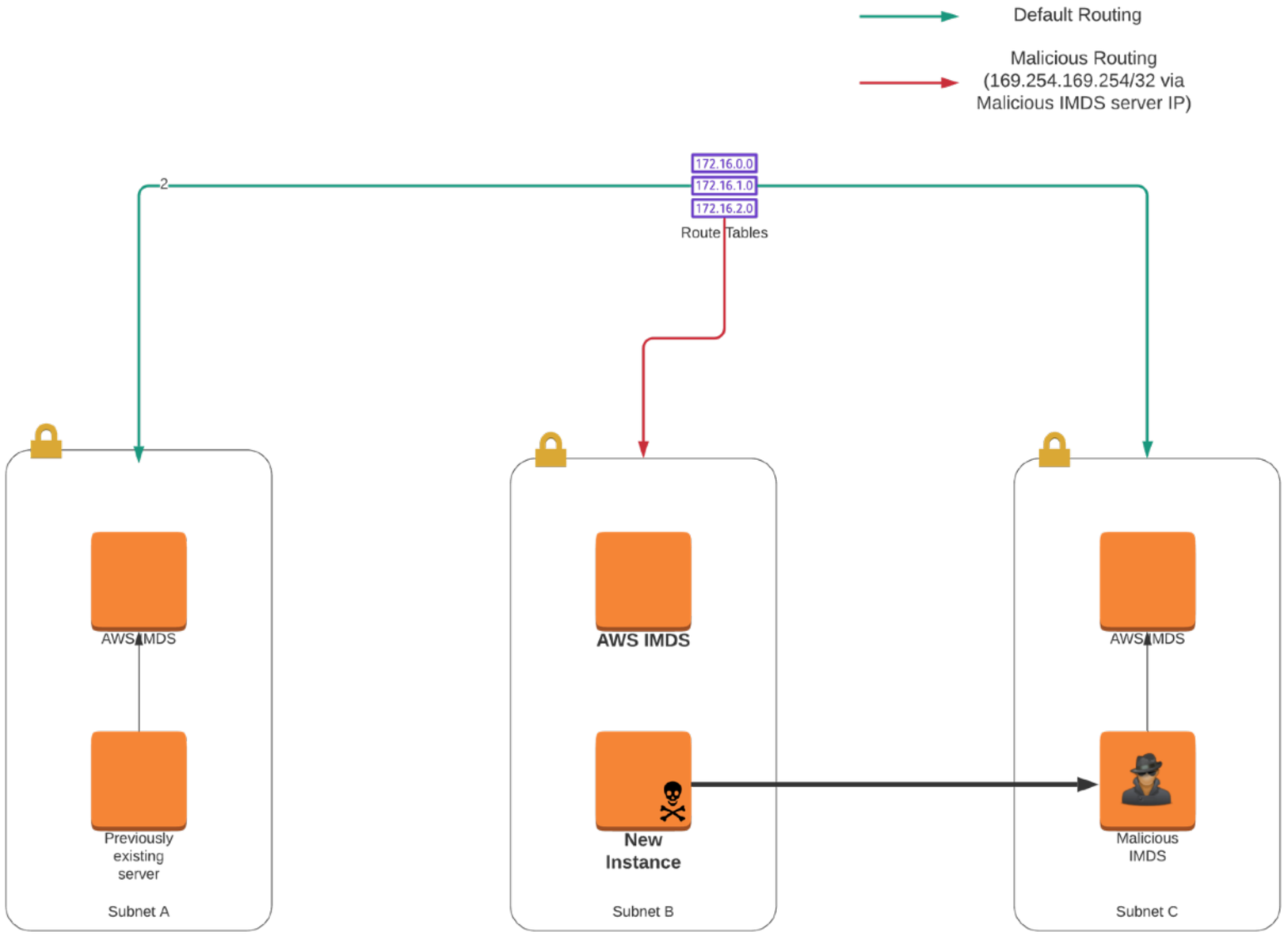
2. Event Bridge trigger's a lambda tthe fake IMDS route trigger lambda.

3. 169.254.169.254/32 via <Malicious IMDS IP> is added to the route table in subnet B.

Event bridge/route updating is fast enough to complete before the new instance is started.

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.