# Cobalt Strike can set its beacon payload to reach out to the C2 server on an arbitrary and random interval and Machete sends stolen data to the C2 server every 10 minutes. Blending malicious traffic within normal activity is one of the final parts of a red team's attack and it is very thoroughly documented. Can you distinguish the tactic's name and technique ID? You surely know the platform to do the job. Example: CSCTF{T1557.004-Credential_Access}

THE FLAG : CSCTF{T1041-Exfiltration}
~Z4uqe