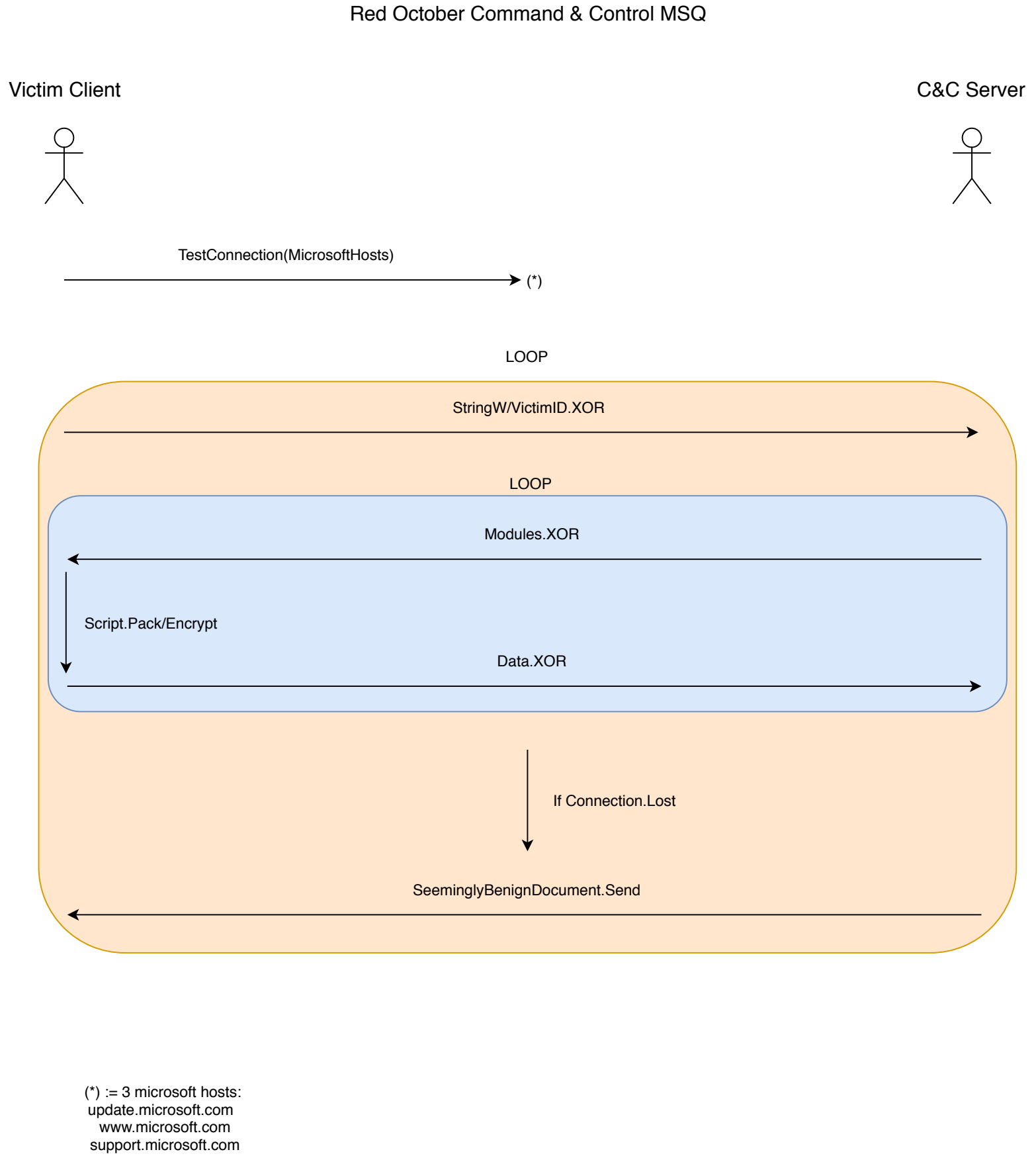
Red October Command & Control MSQ
Victim Client
C&C Server
TestConnection(MicrosoftHosts)
(*)
LOOP
StringW/VictimID.XOR
LOOP
Modules.XOR
Script.Pack/Encrypt
Data.XOR
If Connection.Lost
SeeminglyBenignDocument.Send
(*) := 3 microsoft hosts:
update.microsoft.com
www.microsoft.com
support.microsoft.com