

Forum: [Hack Forums](#)

Thread: [Reverse Proxy Concerns](#)

susp3ct - February 13, 2022, 4:31 pm

It appears I'm a bit confused behind the concept of a "Reverse Proxy";

When I see the feature "Reverse Proxy", I think about masking my ip, that is, with the IP of the infected machine.

However, when I dwell on the difference between a proxy and a reverse proxy, my perception becomes obscured.

Based on what I've read,

a proxy is a configured machine that acts as a intermediary between the client and server, obscuring the client's ip to the server, (conceptually)

and a reverse proxy obscures the server to the client. That is, it appears the proxy resolved the request itself, but it was instead resolved elsewhere.

Hence,

if this is the case, the reverse proxy feature sounds as if, it's a proxy? I assume the infected machine acts as the server to obscure our request.

How is this a reverse proxy? I must be wrong, there must be something I'm not understanding.

Can someone care to explain?

Thanks, susp3ct.

Update:

--The reasoning I've defined is that the reverse proxy is the server used by the rat, and that it sends the packet with important client details while changing other details in the favor of an attacker. This in return would imply the infected client must invoke the request, which I assume is apart of the exploit? That is, the reverse proxy feature handles this invocation? If that's the case, it seems a bit more than needs to be done, but I'm not a security professional. I assume it would be easier to hide if you're invoking requests on the client's behalf as opposed to making them a proxy server? However, I don't know! Please correct this analysis. It's annoying me.

platty - March 6, 2022, 9:55 pm

you overthink too much my man, you explained it yourself really