Premium Remote Control connects to John-PC

https://campus.barracuda.com/doc/98217023/

If a partner is occasionally connecting to a system called John-PC the below is from ISL and will explain what is happening. This is outside of Barracuda Networks and ISL Online's control.

The connection was established to the "John-PC" computer instead of the customer's actual computer. This behaviour was also noticed by some of our other clients and it's commonly related to the security software present on your customer's PC, namely Sandbox threat detection and execution. Sandbox threat detection and execution system is an isolated machine (usually a virtual PC), where suspicious content is delivered for execution/detonation. If anything malicious would have happened with the delivered executable, it would be executed on an isolated PC (sandbox), instead on an actual computer. We received some information, that your customer is using F-secure security suite. Here is the schematic of F-secure advanced threat protection (https://www.f-secure.com/documents/10192/2362688/fsecure-threatshield-technical-brochure-en.pdf):

Why you got connected to the "John-PC"?

If your customer was joining the session using the session invitation link or from the Join webpage, downloaded ISL Light Client executable contained your session code (embedded). If sandbox protection was enabled, ISL Light Client executable was first downloaded/transferred and executed on the sandbox system (PC). When such ISL Light Client with session code embedded is executed, it automatically connects the customer to the session (without typing the session code again). In order to validate that this behaviour is definitely connected to the Antivirus Sandbox, please verify the following with your customer:

1. Inquiry of security software present on their computers.
2. Obtain the System information file from their computer (msinfo32) and send it to us.

How to prevent this?

---

1. Whitelist or disable sandbox protection for ISL Light Client application (https://www.islonline.net/start/ISLLightClient)
2. Instruct customer to download ISL Light Client first, then input session code in the application instead of on the website. (https://www.islonline.net/download/ISLLightClient)
3. Applying customization with "

Further response for ISL regarding the system

ISL does not have any info where John-PC (or other instances) are located, it depends on the Sandbox system used on the remote side (where the client joined the session). Locations of Sandbox systems are usually not disclosed with security vendors. You mentioned your partner is using Kaspersky without any Sandbox, but it it not clear where your partner was connecting to. For this case, it is essential to make an inquiry about the security software present on the client/customer side, where your partner was connecting to. If he got connected to the John-PC when starting on-demand session with his customer, that means that Sandbox is active on his customer side (ISL Light Client executable was detonated on the John-PC Sandbox VM). It may very well be that customer of your partner will not be able to provide the exact information about the security software used on their side (e.g. lack of technical knowledge, sometimes those systems are part of network filtering - e.g. Sophos Sandstorm, ...) but it can be escalated on their side to make such inquiry and obtain the logs from their security software, that will identify Barracuda ISL Light Client being executed in their Sandbox PC.