Seit Dez 2025 beobachte ich massig dummen Port-Zugriff. Der Start war tcp 3389 (RDP) mit botnets. Konnte dann die nets „killen“ durch drop von erkannten botmasters. Nur einen verbliebenen bot musste ich wirklich „killen“, ging easy durch dummen access on his web interface.

Seitdem aber immer weiter, eine Überschwemmung. Ziemlich klar, dass die meisten src IPs als bots missbrauchte hosts sind. Nur selten mal ein full scan durch offenbar botmasters für den Quatsch, z.B. aus „Security-Firma“ CENSYS, von den Seychelles. Dadurch dann auch wieder dummer: Ich anwortete der full scan IP auf den Seychelles wieder mit full scan retour. Der Scan stoppte wieder gleich, doch diesmal „lustiger Blödsinn“: Per Zufall war mein src port in Scan Antwort nicht high ports, sondern tcp 23 (telnet). – Seitdem massig mehr als bots missbrauchte hosts (IPs), die nicht vorhandenes telnet versuchen.

Bis vorgestern (Jun 22) war meine Einstellung: Ich will den bot Schlafmützen nicht schaden, blocke deren IPs nicht, mache keine „active response“.
- Nun aber wird jede Spielfritzen-IP automatisch blocked, wenn es nicht nur web access etc. war. Sorry..

Momentan ~26,000 IPs fully blocked.

Tja.., warum so massiv „gegen“ j-log.eu ? Meinereiner war auch Urknall von networking, globales Net Spielen, nach uucp/uux auch via IP. Dann Inet Kinderüberraschung, somit dann viel network security. - Ja, Inet macht Kriminalität salonfähig. Konnte hacking auf vielen Servers überall in der Welt beobachten. So einen daueraktiven Blödsinn wie gegen meinen Server erlebte ich aber nie. Sollte ich dankbar sein, statt stinkig? ☺ *Die srv IP war zuvor auch Cloud von Luciaphone.*

Since Dec 2025, I’ve been seeing a massive amount of mindless port-probing activity. It started with tcp 3389 (RDP) attacks from botnets. I managed to "kill" the nets by dropping traffic from the identified botmasters. I only really had to "kill" one remaining bot—which was easy, thanks to “stupid” access on its web interface.

But since then, it’s been a relentless flood. It’s pretty clear that most of the src IPs are hosts being hijacked as bots. Only rarely do I see a full scan—likely from the botmasters themselves—such as one from the "security firm" CENSYS - or by masters on the Seychelles. That led to a bit of a silly moment: I responded to the Seychelles full-scan IP with a full scan of my own. Their scan stopped immediately, but with a funny twist: by chance, my source port for the response wasn't a high-range port, but tcp 23 (telnet). Since then, I’ve seen a huge surge in hijacked host IPs trying to connect via telnet—a service I don't even run.

Up until the day before yesterday (Jun 22), my policy was: I don't want to harm the bot-herders; I won't block their IPs or engage in "active response".
- But now, any IP acting up gets automatically blocked if it did anything beyond standard web access. Sorry...

Currently, about 26,000 IPs are fully blocked.

Well... why such a massive onslaught against j-log.eu? I was there at the dawn of networking and global online gaming—moving from uucp/uux to IP-based connections. Then came the "Internet Surprise Egg" era, bringing a heavy focus on network security. Yes, the Internet has made cybercrime commonplace. I’ve witnessed hacking attempts on servers all over the world, but I’ve never experienced anything as relentlessly persistent as the nonsense directed at my server.
Should I be grateful instead of annoyed? ☺ *The srv IP was previously also a Luciaphone cloud service.*