BPFDoor — an active Chinese global surveillance tool

By Kevin Beaumont

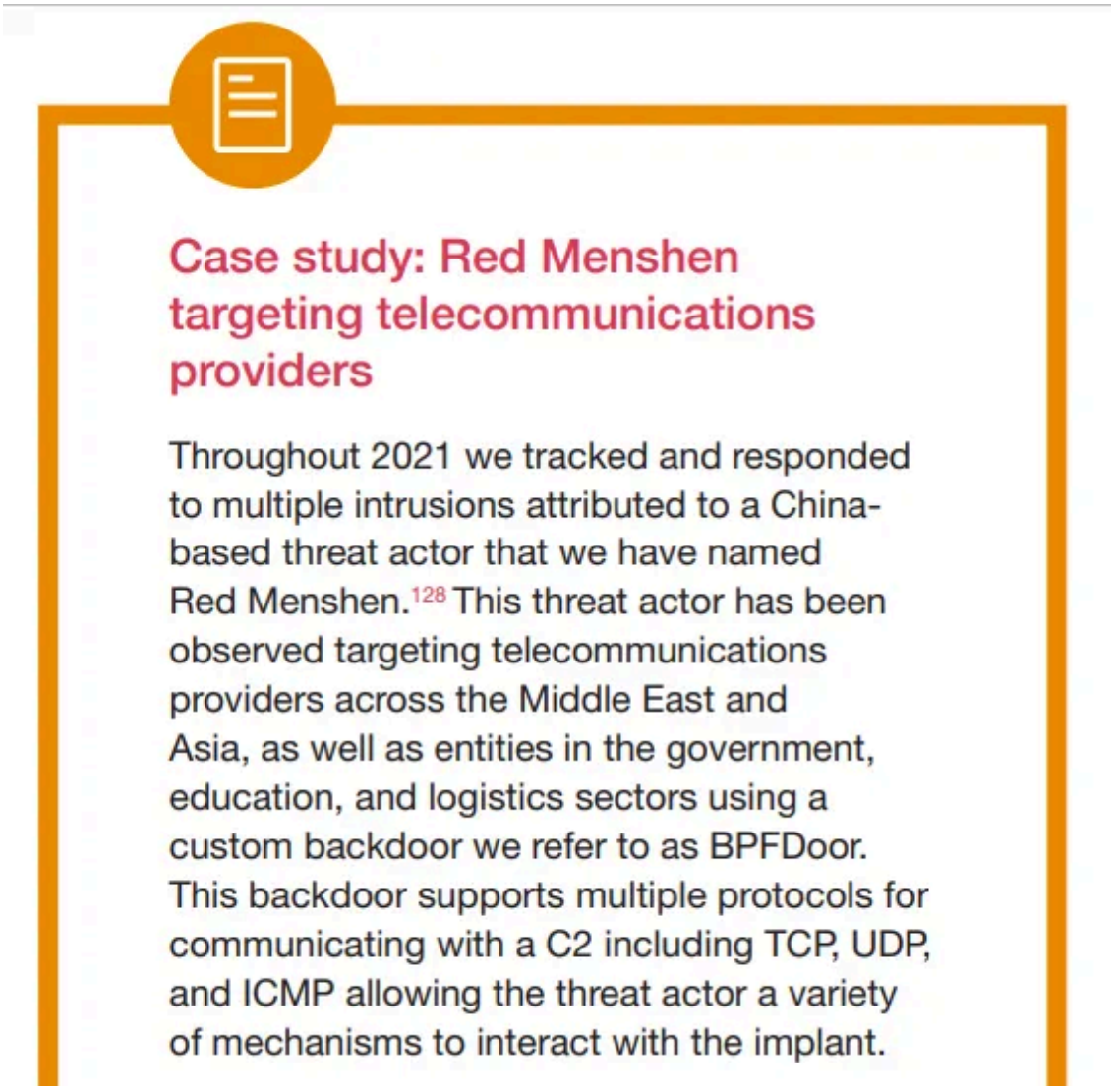
Published: 2022-05-08 · Archived: 2026-04-10 02:32:00 UTC

Member-only story

3 min read

May 7, 2022

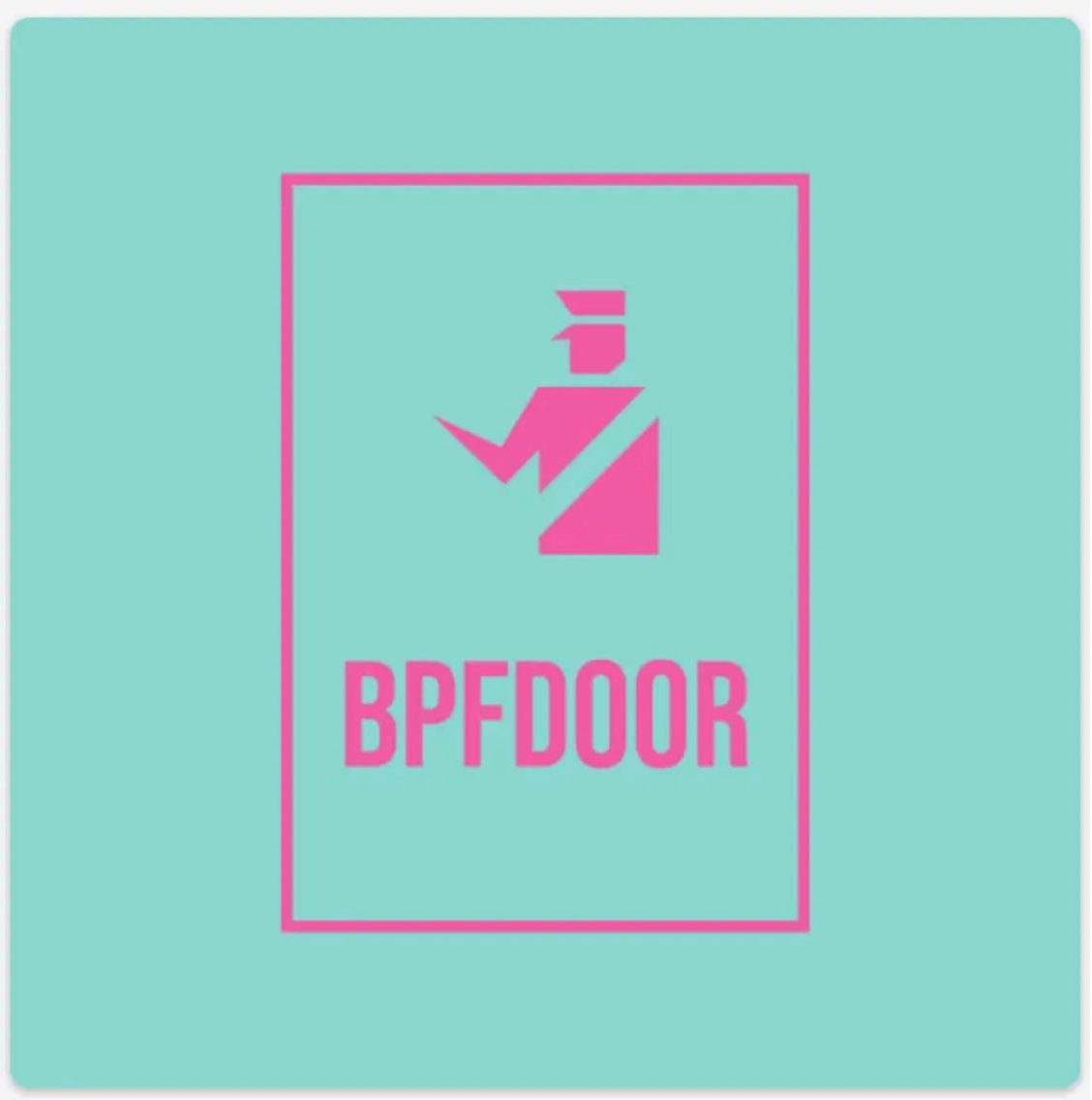
Recently, PwC Threat Intelligence documented the existence of BPFDoor, a passive network implant for Linux they attribute to Red Menshen, a Chinese threat actor group.



You can read more in PwC's great, yearly threat intelligence brief, here.

PwC plan to present their findings in June:

BPFDoor is interesting. It allows a threat actor to backdoor a system for remote code execution, without opening any new network ports or firewall rules. For example, if a webapp exists on port 443, it can listen and react on the existing port 443, and the implant can be reached over the webapp port (even with the webapp running). This is because it uses a BPF packet filter.



Operators have access to a tool which allows communication to the implants, using a password, which allows features such as remotely executing commands. This works over internal and internet…

Source: https://doublepulsar.com/bpfdoor-an-active-chinese-global-surveillance-tool-54b078f1a896