

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.



Case study: Red Menshen targeting telecommunications providers

Throughout 2021 we tracked and responded to multiple intrusions attributed to a China-based threat actor that we have named Red Menshen.¹²⁸ This threat actor has been observed targeting telecommunications providers across the Middle East and Asia, as well as entities in the government, education, and logistics sectors using a custom backdoor we refer to as BPFDoor. This backdoor supports multiple protocols for communicating with a C2 including TCP, UDP, and ICMP allowing the threat actor a variety of mechanisms to interact with the implant.

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>