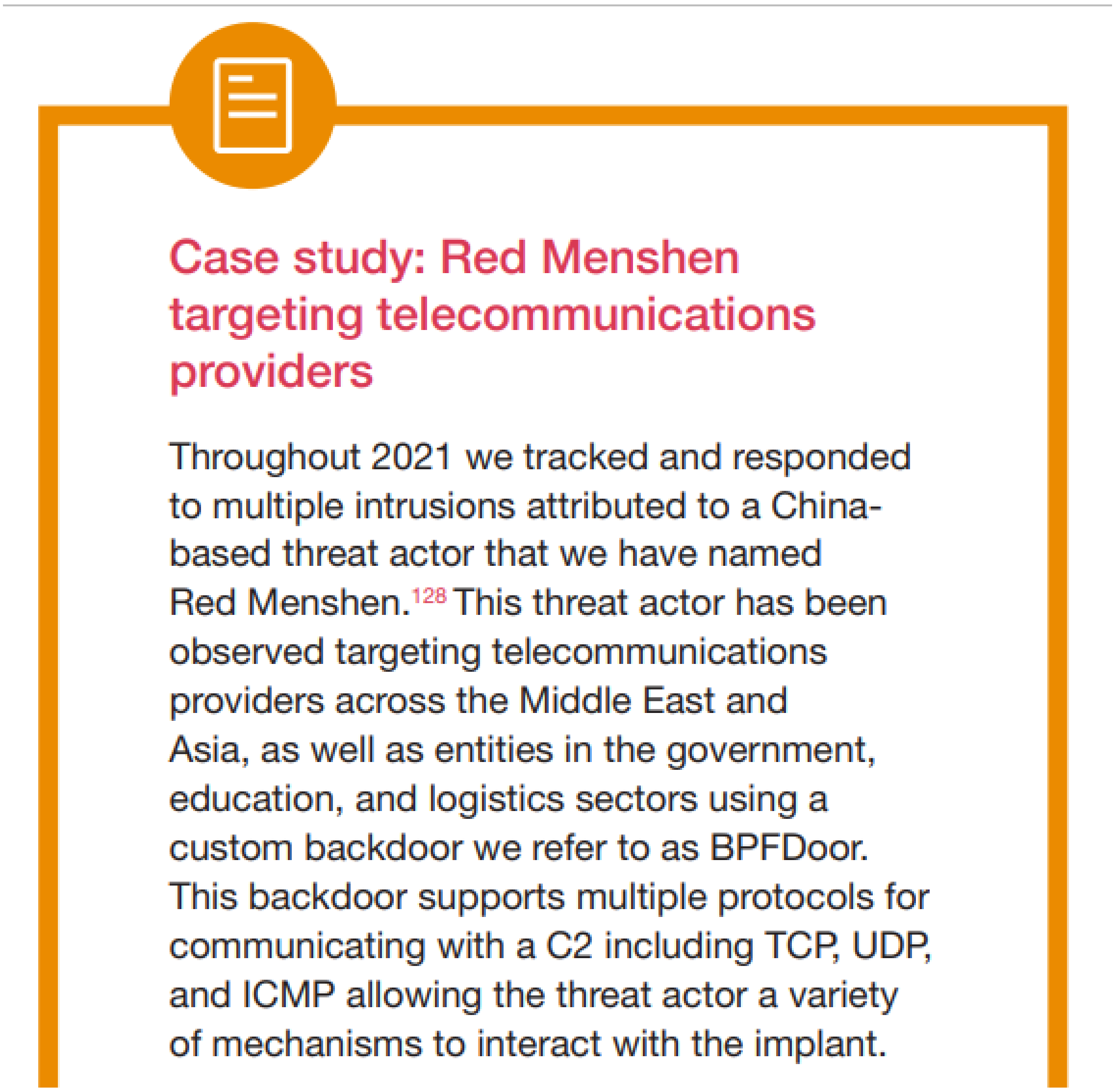
doublepulsar.com /bpfdoor-an-active-chinese-global-surveillance-tool-54b078f1a896

BPFDoor — an active Chinese global surveillance tool

Kevin Beaumont ⁝⁝ 5/7/2022

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.



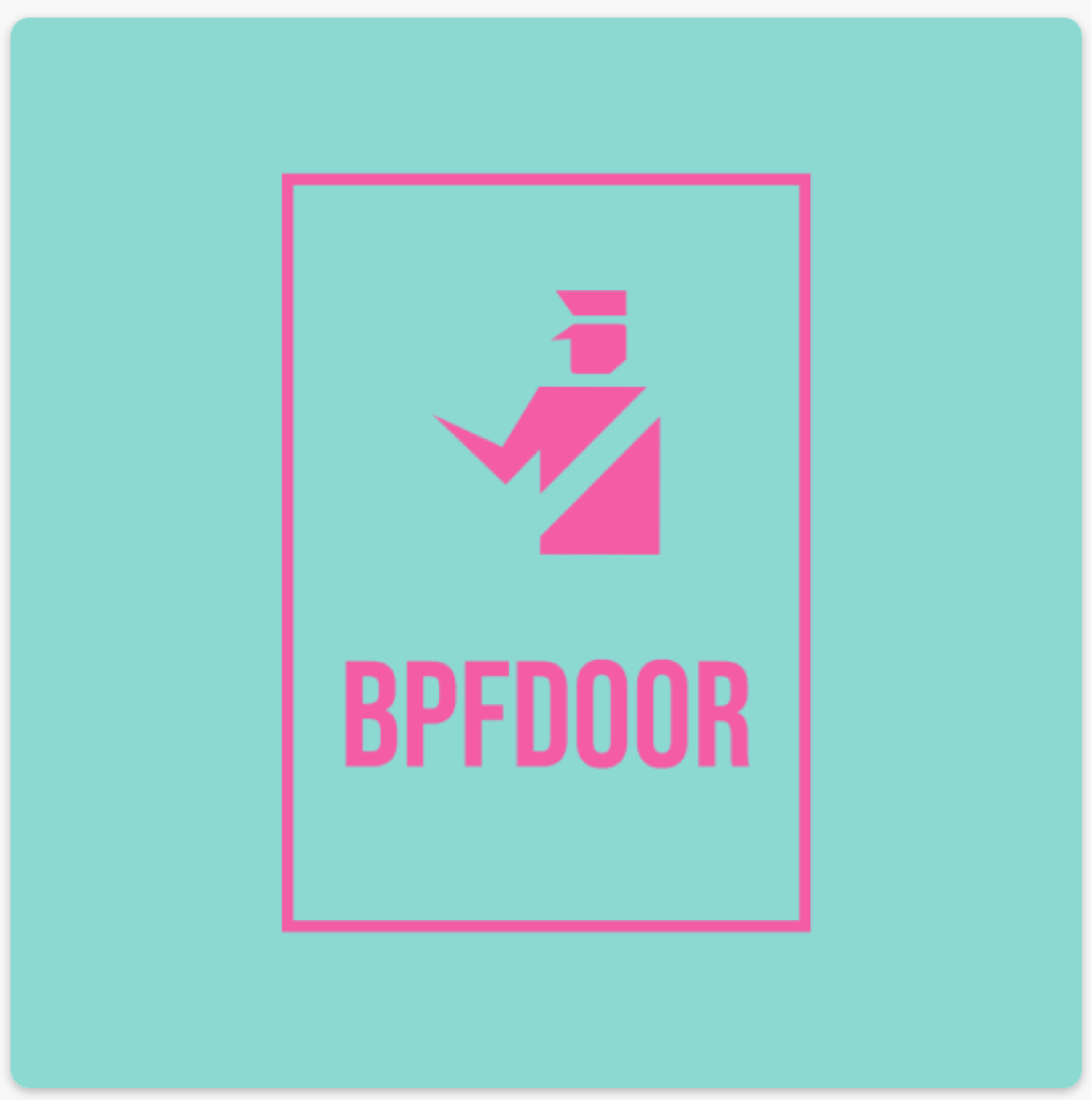
Case study: Red Menshen targeting telecommunications providers

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 networks.

Because BPFDoor doesn't open any inbound network ports, doesn't use an outbound C2, and it renames its own process in Linux (so ps aux, for example, will show a friendly name) it is highly evasive.

I swept the internet for BPFDoor throughout 2021, and discovered it is installed at organisations in across the globe— in particular the US, South Korea, Hong Kong, Turkey, India, Viet Nam and Myanmar, and is highly evasive. These organisations include government systems, postal and logistic systems, education systems and more.

Inside those organisations I believe it is likely present on thousands of systems. The implant appears to be for surveillance purposes.

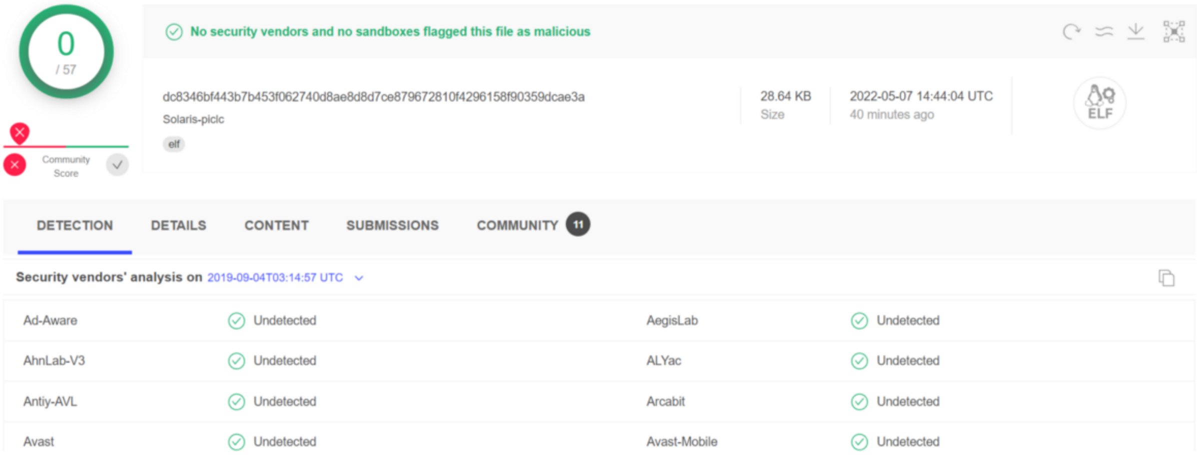
Per PwC:

> We also identified that the threat actor sends commands to BPFDoor victims via Virtual Private Servers (VPSs) hosted at a well-known provider, and that these VPSs, in turn, are administered via compromised routers based in Taiwan, which the threat actor uses as VPN tunnels. Most Red Menshen activity that we observed took place between Monday to Friday (with none observed on the weekends), with most communication taking place between 01:00 and 10:00 UTC. This pattern suggests a consistent 8 to 9-hour activity window for the threat actor, with realistic probability of it aligning to local working hours.

The implant has been in use for many years — over 5 — and has flown under the radar.

Versions exist for Linux appliances, Solaris SPARC boxes and more. For example, here's a Solaris version first uploaded to VirusTotal in 2019:

VirusTotal — File — dc8346bf443b7b453f062740d8ae8d8d7ce879672810f4296158f90359dcae3a



No security vendors and no sandboxes flagged this file as malicious

dc8346bf443b7b453f062740d8ae8d8d7ce879672810f4296158f90359dcae3a
Solaris-piclc
elf

28.64 KB
Size

2022-05-07 14:44:04 UTC
40 minutes ago

Security vendors' analysis on 2019-09-04T03:14:57 UTC

Ad-Aware	✓ Undetected	AegisLab	✓ Undetected
AhnLab-V3	✓ Undetected	ALYac	✓ Undetected
Antiy-AVL	✓ Undetected	Arcabit	✓ Undetected
Avast	✓ Undetected	Avast-Mobile	✓ Undetected

Nextron Systems THOR was detecting the activity over the past year or so, visible in VirusTotal comments:

Indicators of Compromise and Indicators of Attack

(note that each implant has a unique hash, so hunting for file hashes is a *BAD IDEA*).

VirusTotal — Collections — BPFDoor

- YARA rules:

signature-base/mal_lnx_implant_may22.yar at master · Neo23x0/signature-base (github.com)

ThreatHunting/BPFDoor-Unknown.yar at master · GossiTheDog/ThreatHunting (github.com)

- Files insuch as

Sandbox report from 2019 — includes useful commands; Automated Malware Analysis Report for m8XMnec4Vb.elf — Generated by Joe Sandbox