GitHub - 0xThiebaut/PCAPeek: A proof-of-concept re-assembler for reverse VNC traffic.

By 0xThiebaut

Archived: 2026-04-05 23:13:05 UTC

A proof-of-concept re-assembler for reverse VNC traffic such as IcedID & Qakbot's VNC Backdoors.

Do note that as PoC, PCAPeek offers no guarantees on backwards compatibility and might be modified in the future for additional protocols.

Installation

This utility depends on Npcap for PCAP parsing, which you likely already have installed if you have WireShark.

To download and build this utility using the Go programming language, simply...

```
go install github.com/0xThiebaut/PCAPeek@latest
```

Usage

To use PCAPeek, use the `--help` flag.

```
PCAPeek --help
```

```
 PCAPeek is a tool to peek into PCAPs. It doesn't do much besides acting as a proof of concept to reconstruct re



Usage:
  PCAPeek PCAP [PCAP ...] [flags]

Flags:
      --files              Output clipboard files
      --files-dir string   The output directory for the clipboard files (default "./")
      --filter string      A BPF filter to apply on the PCAPs
  -h, --help               help for PCAPeek
      --jpeg               Output JPEG frames
      --jpeg-dir string    The output directory for the JPEG frames (default "./")
      --jpeg-fps int       The number of JPEG frames to output per second (default 0, outputs all frames)
      --jpeg-quality int   The JPEG frame quality percentage (default 100)
      --mjpeg              Output MJPEG videos
      --mjpeg-dir string   The output directory for the MJPEG videos (default "./")
```

```
      --mjpeg-fps int       The number of MJPEG frames to output per second (default 10)
      --mjpeg-quality int   The MJPEG video quality percentage (default 100)
```

Thanks

Thanks to Brad Duncan (Malware-Traffic-Analysis.net) and Erik Hjelmvik (NETRESEC) for their extensive research on IcedID and its BackConnect protocol.
