

SharkFest'26 Europe

Attacks in the Network
A look at real world malicious traffic examples

Jasper Bongertz
G Data Advanced Analytics

WIRESHARK

Sponsored by:
PROFITAP DEEP NETWORK OBSERVABILITY
cPacket
TCP/IP training
endace Record. Respond.

About me

- Head of CSIRT at G Data Advanced Analytics, Germany
  - Mostly Incident Response in Ransomware Attacks on customers
- Member of the Board of Directors of the Wireshark Foundation
- Network analysis & forensics since 2003
  - NetXRay, Sniffer Pro/Distributed, Clearsight…
  - Ethereal/Wireshark since version 0.9something
- Creator of TraceWrangler
- Wireshark Certified Analyst (WCA #2) 🎉



Agenda – Live Demos

- Case 1: To SYN or not to SYN
- Case 2: The Sneaky Spy
- Case 3: The Fly Swatter
- Case 4: The Lurker
- Bonus Case: The Underminer

Thank You!

WIRESHARK

Enjoy Sharkfest!

