SEC-5 Using wireshark to gather forensic evidence on malware outbreaks

Christian Landström - Senior Consultant
CASSIDIAN Cyber Security
Outline

Not much slides – more time for demo and Q&A

• Commercial products vs. Wireshark
• DNS analysis
• Callback analysis
• Exploits in wireshark

• Q&A
House rules
Commercial products vs. Wireshark

• Not a versus
  – Have both, use both
  – Have only one of them… ;)

• Best practice:
  – SecTools / SecAppliances for automated monitoring and pre-analysis
  – Wireshark for detailed analysis and correlation
DNS Analysis

- Time consuming
- Very effective
- Recommended as permanent process
- Combined usage of GUI and CLI
- Recommended addons:
  - Good Text Editor + Spreadsheet Editor
  - “Linux” Tools like grep, cat, uniq, sort etc.
Callback Analysis

- Dependent on protocols used by malware
- TCP quite standard / UDP hard to tell
- How can you tell?
  - always depends on application knowledge

- Learn your standard protocols
- Look for anomalies, be creative
A few words on exploits

- Main focus of IDS / IPS
- Harder to spot compared to the later actions
- Usually hard to interpret
  - Obfuscated
  - Packed
  - Crypted
- Not necessarily needed
Worst case

- Malware already inside your networks
- AV does not trigger
- IPS didn’t throw events
- unknown threat
- unknown damage

→ Forensics to the max.
In-depth analysis

- Baselining every connection
- Explaining every data transfer
- Fighting through lots of false positives
- At worst: evaluate every single packet
Commercial products vs. Wireshark

• Not a versus
  – Have both, use both
  – Have only one of them… ;)
• Best practice:
  – SecTools / Sec Appliances for automated monitoring and pre-analysis
  – Wireshark for detailed analysis and correlation
Thanks for your attention!

???

Questions

???