Trussels og hændelseshåndtering

click to open

Supporting tools

- Log lab
  - VM splunk
  - Sof-elk
  - Security Onion
- Network lab (physical lab)
  - Glinet routers, switches, VPN service etc.
- VM s (Virtualbox and VMware)
  - Windows
    - Your own machine with tools
  - Linux
- Malware lab
  - Remnux
    - PCAP recording and analysis
    - Grep, tshark, TCP dump
  - Flare VM
    - Inet sim and fake dns
    - PEstudio
- Cloud sandbokses
  - App any.run
  - Joes sandbox
  - Virustotal
- Forensic lab
  - Physical machine
    - Autopsy
      - Email analysis
      - Yara rules
      - TImeline
      - Identify files and filetypes
      - detect encryption
    - Axiom
    - encase etc

Stand alone tools

- Pestudio — Static analysis for Malware files
- Autopsy — Forensics, analysis, timeline
- FTK — Imaging, memdump, mound of filesystem, AD1 container
- Cyberchef — Converter, sorter and analyzer
- Caine and paladin — Live boot software writeblockers
- Yargen — Tool for generating YARA files
- Loki — HASH and YARA recognition tool
- Volatolity + volatility workbench — Memory analysis
- Magnet ram aquire and fkt — Memory aquisition (VMware can aquire dumps as well, not guaranteed to work allways)
- Dirhash, Hashtools — File integrity calculation and checks
- Cloud service — For sharing files with encrytion
- Encryption — Veracrypt
- KAPE — Live aquisition triage tool and parser

1 Preperation

- Jump bag
- Tools
  - Caine / Paladin
  - Writeblocker equipment
  - Malware lab preparation
  - Forensic lab preparation
  - Log lab and network lab
  - hardware tools
- Prepeation for incidents
  - Know you capabilities
  - When to hire 3'rd party
- Printed procedures
  - Incident plans, telephone lists, be on call , retainer agreements etc.
- Test and exersises
  - Table top exersises
  - real world testscenarios

2 Identification

- test your tools for alarming
- start identify malware, attack, and TTP (Tools Technicques and procedures)
- Spin up labs, prepare your storage for collections data
  - Analysis for beacons, persistence, files, folders, schedueled tasks
  - Forensic imageing. Analyse malware infections or insider threats. chain of custody, image replication and analysis
- Prepare tools for integrity checks, storage, forensic analysis (triage = under 6 hours analysis)
- Gain knowledge from files, logs, artefacts, events and alarms
- Inform / report to autorities
  - Have a contact at the right partner fx Police or Military

3 Containment

- Use what you gained in identification to start contain the incident.
- Block Domains, IP´s, ports, folders, shares, Hashes, and monitor for activity. Maybe consider Yara rules
- Monitor for activity from the above blocks

Retest data for day zwero for the infection

4 Eradication

- Start to delete identified malware or infections on systems
- test with anti malware solution

5 Rollback

- New images installation on the infected systems
- Restore backups and monitor for old artefacts in the backups
  - Yara ruling and HASH values
- Long press topic to select topics in branch

6 Lesseons learned / post incident

- What went good
- What could be improved / better
- Lessosns leaned, share the knowledge and the story / timeline for others to learn.

7 Monitor phase

- An ekstra measure for doing some monitoring. In the event of a reinfection. Then we can push the panic button (NOT PART OF IR PHASES)