IT-SECURITY

ACTIONCARD -

ANALYSIS OF MALWARE

Steps for Analysing Malware

Malware analyzed

Malware analysis

Always work on the copy

- Where was the sample collected? (Time, date, machine, user / division)
- HASHvalue
- Online sandbox sample (DO NOT UPLOAD ANYTHING, UNLESS APPROVED) and references to the web
- Who carried out the analyses
- Any constraints to the analysis?

Malware lab / sandbox setup

What sandbox/s was used, and how is the network setup

- Network setup. Online / Offline
  - Default allways offline
  - Use of specific hardware, fx router with VPN capability? (Fx Gl-Inet routers)
  - Was the VM´s setup to work toghether in the same network (network capture)
- Vm environment (Vmware, Virtualbox, Proxmox, ESXI etc) and verion
- Virtual mashines used.
  - Windows with FlareVm or Remtools
  - Linux. Fx Remnux
  - Other?
- Search methods for specific scans IOC, YARA, HASH, method of seach from vendor file Signatures
- Online cloud sandboxes
  - What service and link to result
  - what services was provided
  - Any constraints. Fx sample was run for 5-60 minutes
  - What decission was made to use the cloud. was this activly decided?

Steps for Analysing Malware

Malware analyzed

Static analysis

What was performed to identify the strings

- Tools used ? fx PEstudio, Detect It Easy (DIE)
- Fingerprints / HASHes
- Antivirus scanning
- String extraction
- File format
- Packer analysis
- Disassembly
- Tools used and versions of the tool

Dynamic analysis

It can be very individual how this are carried out. The important part here is that its predefined what actions are chosen, accordingly with the analysis.

- What Operating system was used for this anslysis?
  - How was this configured?
  - Network setup
  - Virtual or hardware (some malware do not funtion as expected in virtual environments)
  - Freshly installed lab or use of legacy labs (that looks inhabitated from a user, with docs, mediafiles, links and logs etc)
- Runtime behaviour
  - What tools did we use for tecteion. Fx Process hacker, process exlorer, regshot etc.
  - what processes and files was spawned and where?
  - Network activity. Contact to C2 servers or domains / IP´s
- Persistence
  - schedueled tasks
  - Service installation
  - Hidden sectors
  - contact to Command and Control trafic (C2)

Steps for Analysing Malware

Malware analyzed

Reverse engineering analysis

Based on earlier results and decissions. A reverse engineering of the file can be carried out

- Purpose of the analysis? fx insider, leagalcase, nation state actors, espionage etc.
- Tools used ? fx IDA, IDA pro, Ghidra
- Timeconstraints / definitions
- Specific purpose of the anslyzed malware / software
  - intentions
  - Vulnrabilities
- Functions
  - Call executions
  - Return executions
- Memory
  - calls
  - allocation of processes and space
  - Identify possible tampering with memory
- Language used
  - Maybe comments left
- Obfucsation
  - evasive measures
  - Just In Time actions (JIT)
- Encryption / decryption