anti-virus

detecting a malicious file

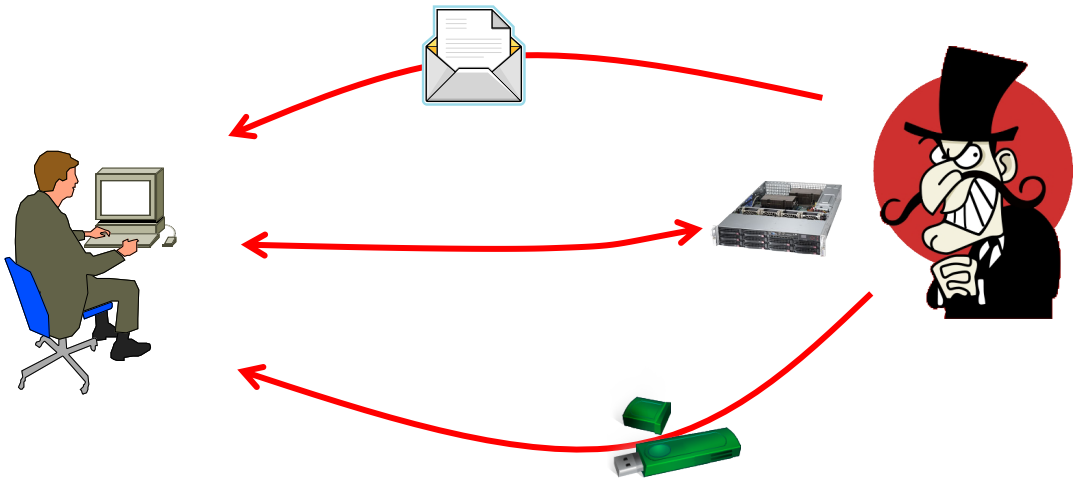
malware, detection, hiding, removing

malware

- is the generic term for computer virus, worms, spyware and other malicious software
- skilled attacker can make it, joy attacker can use it.
  - even there are malware build tools with GUI ☹

infection

- attackers try to make your devices infected in many ways
  - security holes, e-mail, web
  - USB memory, file servers



causes

- vulnerability
  - 0-day security hole without patch
  - old security holes are still used to infect
- auto-execution for removal media
  - USB memory, CD loading
- users’ careless open
  - sometimes happen to execute malwares

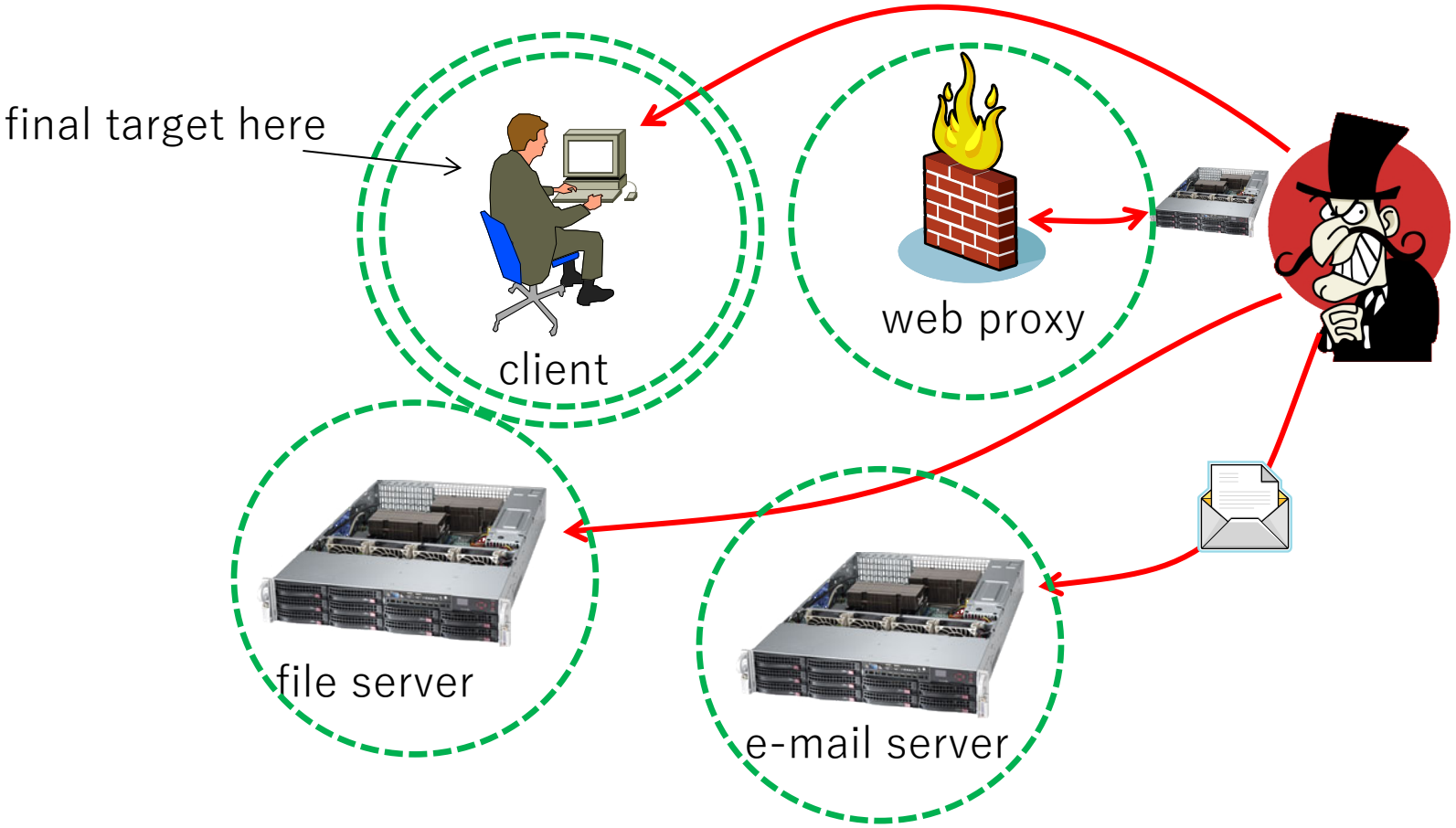
detection

- signature-based detection
  - blacklist of malwares
  - check a file with the signatures
  - update needed to detect newer malware
- heuristics detection
  - behavior, characteristic code

when?

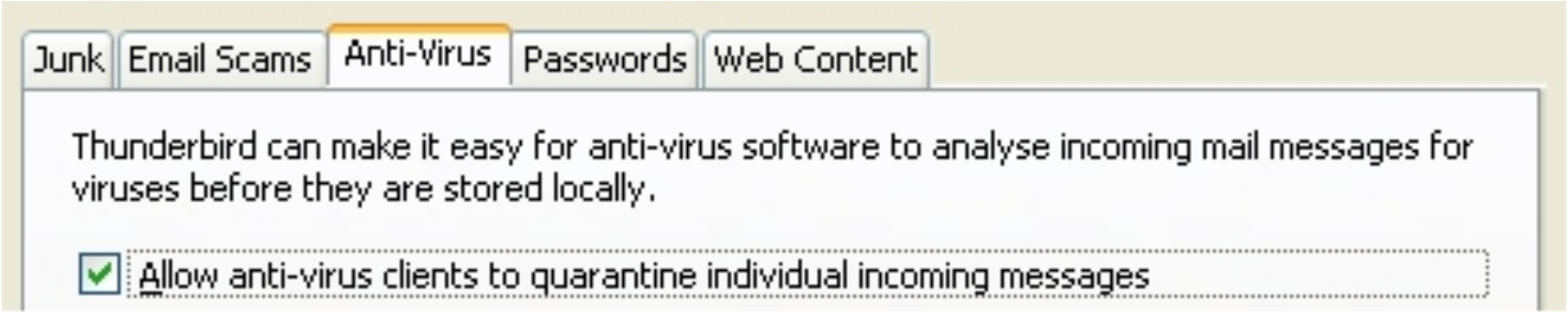
- where write operations take place
  - new file, file modification
- new media is inserted
  - USB memory, CD
- periodic or manually
  - scan all or important files

where?


final target here
client
web proxy
file server
e-mail server

staging for detection

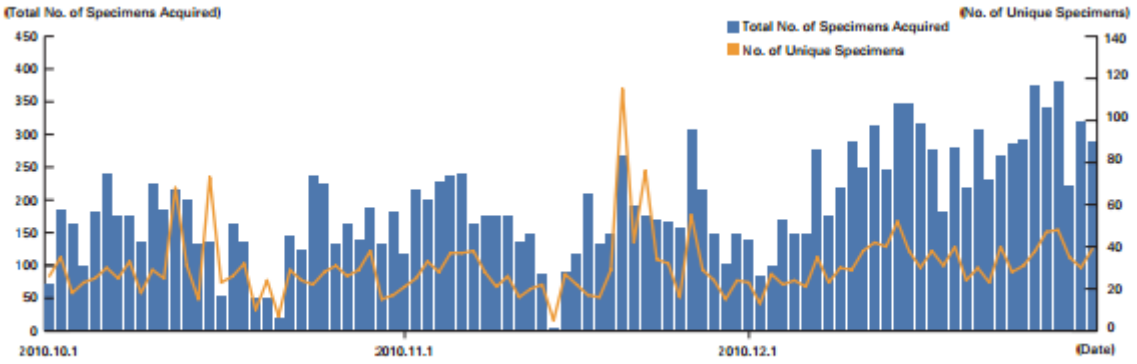
- Thunderbird example



- otherwise, entire INBOX file would be considered as ‘suspicious’ once attached malware is stored into your inbox file

hiding

- attackers modify malwares
  - not to be detected by anti-virus
  - they can check this locally

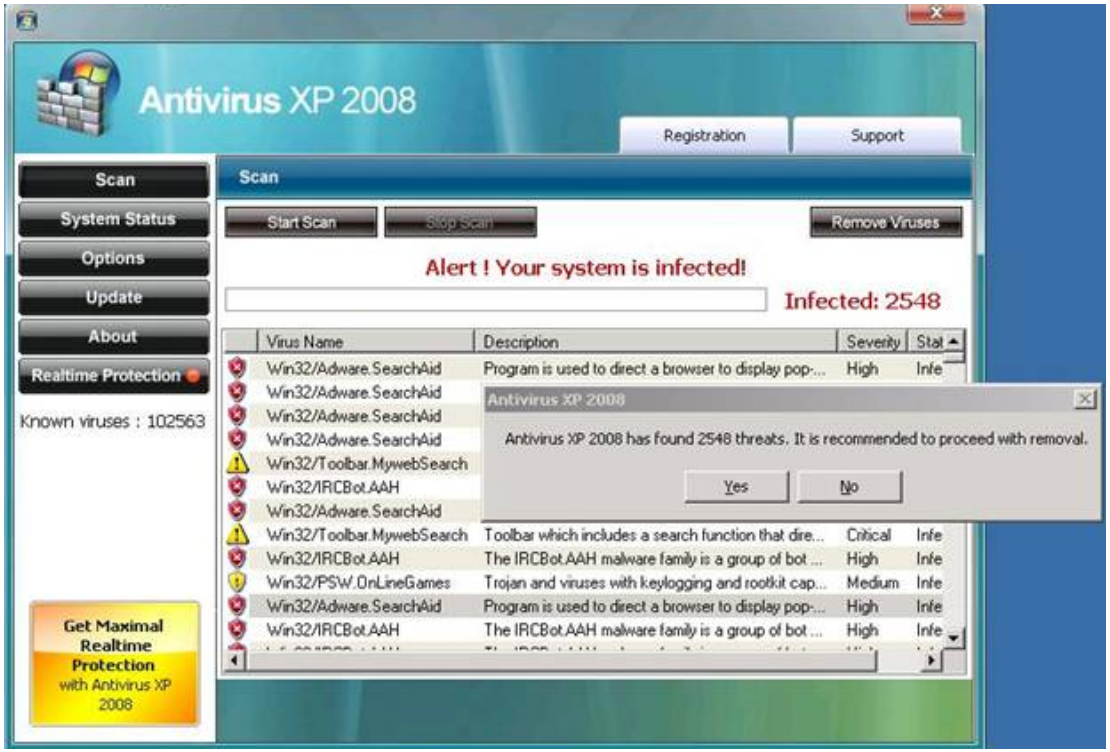


Trends in the Number of Malware Specimens Acquired (Total Number, Number of Unique Specimens)

  - up-to-date signature needed

fake security software

- do nothing, or is just a malware
  - also known as ‘scareware’



summary

- update system
  - less security holes
- update anti-virus signature
  - to detect newer malware
- use caution for received/downloaded file
  - documents or software