Securing a client

Matsuzaki ‘maz’ Yoshinobu

<maz@iij.ad.jp>

Hardening a host

Hardening a host

- Differs per operating system
  - Windows: users can not be trusted to make security related decisions in almost all cases
  - OS X : make things work magically for users. Try to handle security issues in the background
  - Linux: varies by distribution:
    - Ubuntu: try like OS X to make things just work.
    - RedHat: include very useful tools but turned off by default
  - BSD: users will figure it out
- Changes with time

General consideration

- Define a personal usage profile and policy.
  - What hardware do you use?
  - What software tasks do you do on your computer?
  - Do the first two change when you travel?
  - What habits from the above two do you need to change to be more secure?
  - Decide if you *really* need VPN access to your network while travelling.

General practices

- Install only the services and software you actually need.
  - Uninstall or disable all software and services you do not use or need.
  - Periodically actively scan your machine for vulnerabilities.
  - Have as few user accounts on your systems as possible
- Protect your administrative account. Have a strong password, do not permit remote password based logins and do not log in as an administrator unless you need to do an administrative task.

Hardware

- Rule 1: all bets are off with physical access to your devices.
- Consider removing hardware you never use – say bluetooth.
- Disable in BIOS or EFI or your operating system the hardware or features you can not remove physically.
    - wake on lan
    - Bluetooth discoverability
    - USB ports?
- BIOS passwords not that useful
- BIOS level encryp8on/locking of hard disks may not be portable

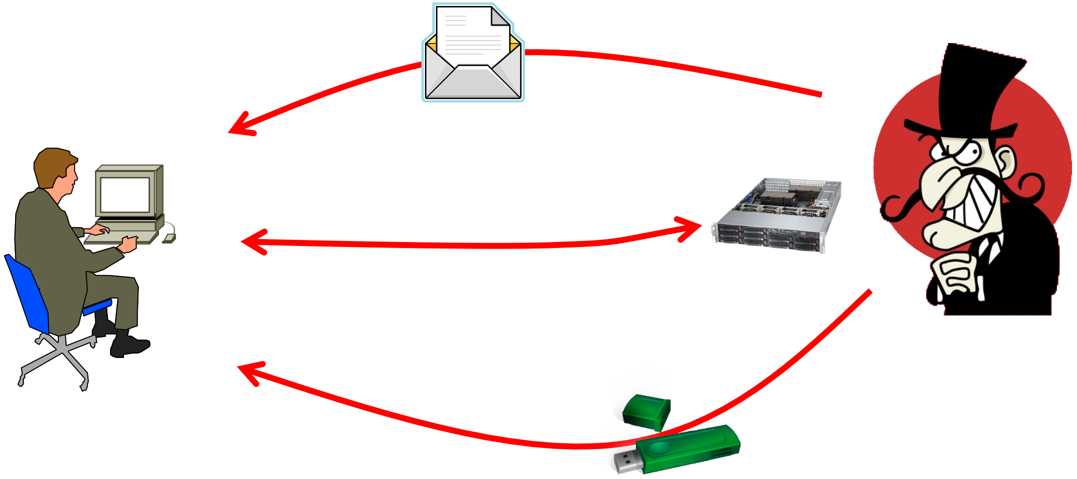
Anti virus

Malware

- The generic term for computer virus, worms, spyware and other malicious software
- Skilled attacker can make it, fun 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 holes
  - old security holes are still used to infect
- Auto-execution for removal media
  - USB memory, CD loading
- Users’ careless open
  - infected files
  - sometimes happen to execute malwares

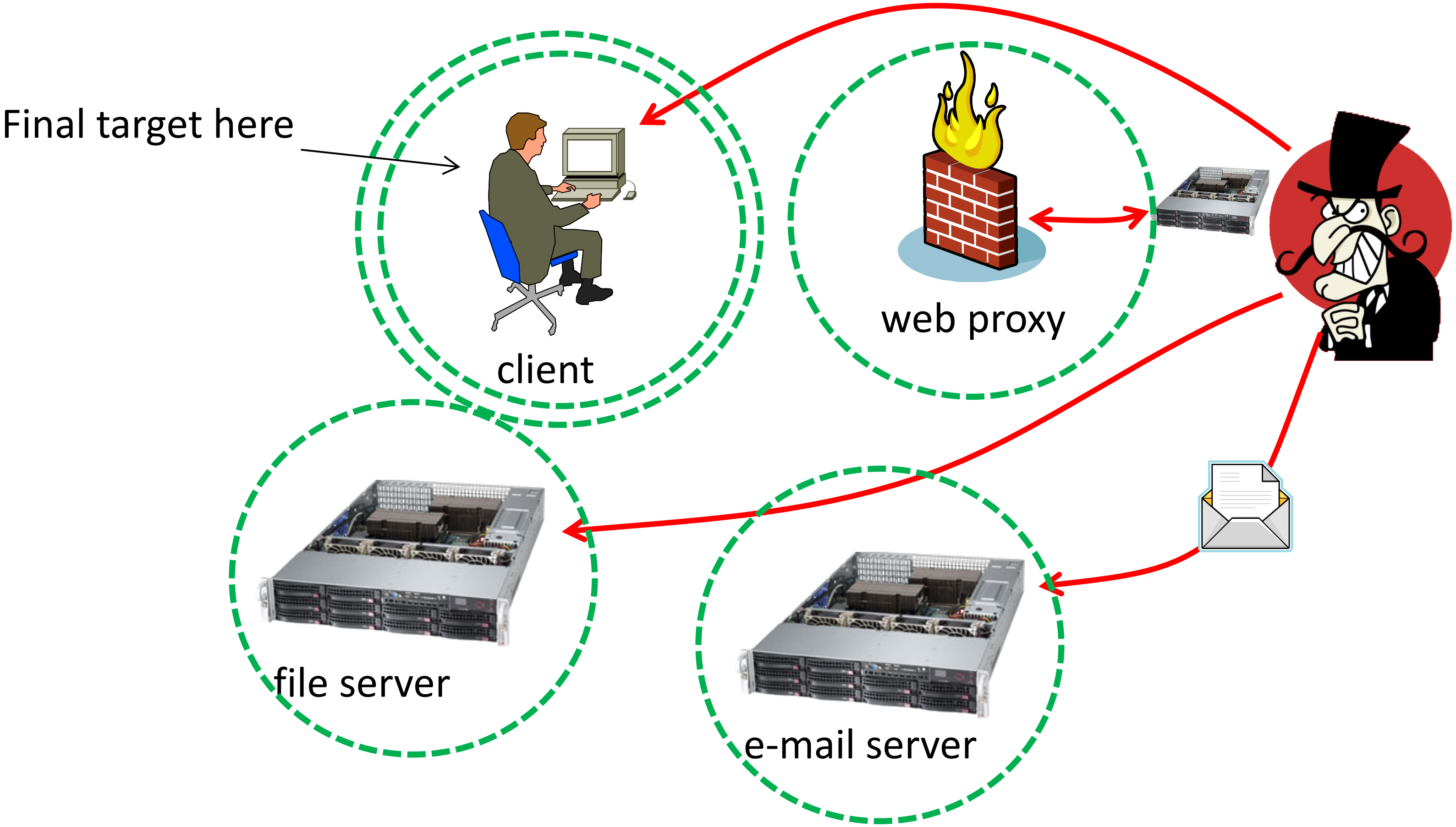
Detection

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

When?

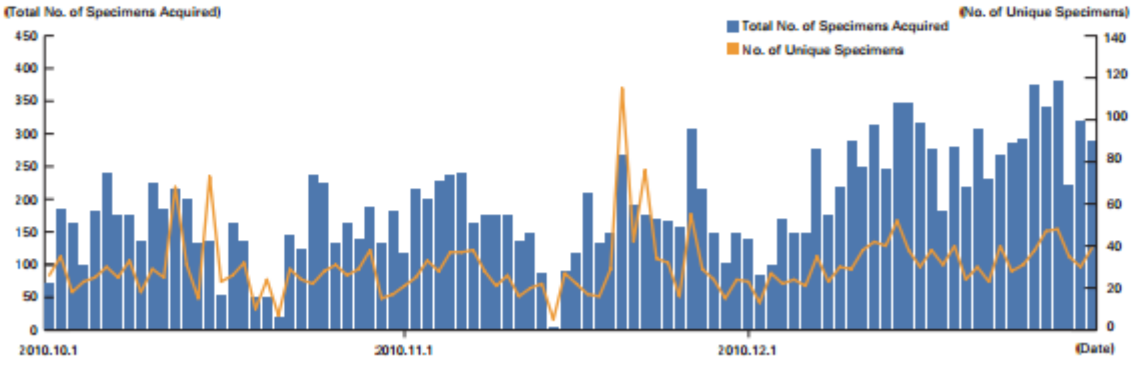
- Write operations take place
  - creating a new file, modifying an existing file
- New media is inserted
  - USB memory, CD
- Periodic or manually
  - scan all or important files

Where?


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

Hiding

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

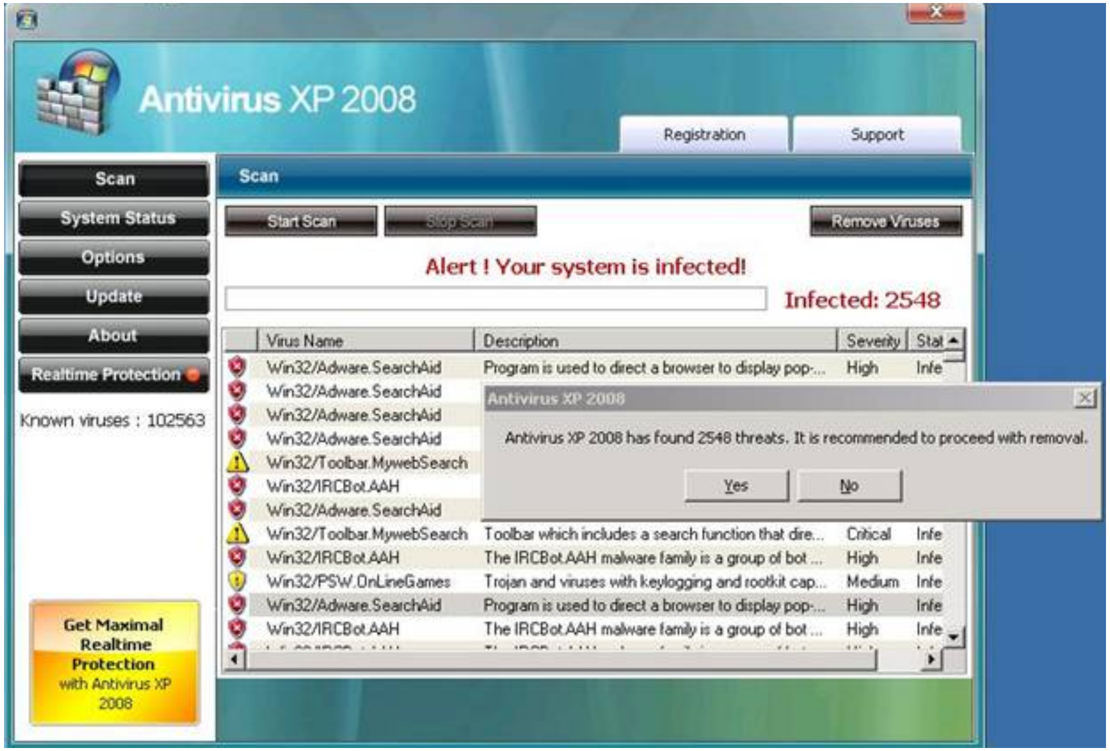


Trends in the Number of Malware Specimens Acquired (Total Number, Number of Unique Specimens)

- Updating your signature DB is needed

Fake security software

- Do nothing, or is just a malware
  - also known as 'scareware'



Alert ! Your system is infected!

Infected: 2548

Known viruses : 102563

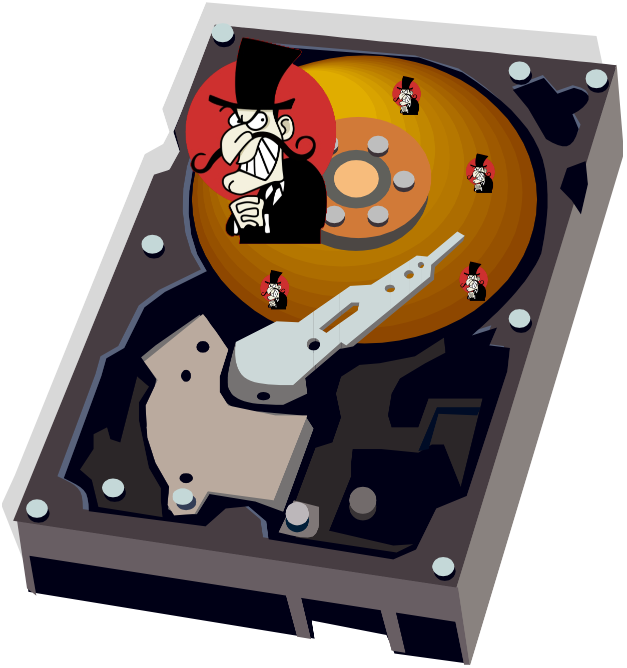
Antivirus XP 2008

Antivirus XP 2008 has found 2548 threats. It is recommended to proceed with removal.

Virus Name	Description	Severity	Stat
Win32/Adware.SearchAid	Program is used to direct a browser to display pop-...	High	Infe
Win32/Adware.SearchAid			
Win32/Adware.SearchAid			
Win32/Adware.SearchAid			
Win32/Toolbar.MywebSearch			
Win32/IRCBot.AAH			
Win32/Adware.SearchAid			
Win32/Toolbar.MywebSearch	Toolbar which includes a search function that dire...	Critical	Infe
Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot ...	High	Infe
Win32/PSW.OnLineGames	Trojan and viruses with keylogging and rootkit cap...	Medium	Infe
Win32/Adware.SearchAid	Program is used to direct a browser to display pop-...	High	Infe
Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot ...	High	Infe

Compromised system

- Any file on the system is already suspicious
  - You may be able to remove a malware
  - there could be another one that you can not detect



Wipe

- Don’t use files in the compromised system
  - programs
  - documents
  - images
- Clean up the storages that was connected to the system
  - HDD
  - SSD
  - flash memory

How can we rescue information from suspicious data files

- Convert it into another format
  - png -> jpg, jpg -> png
  - doc -> txt
  - excel -> csv
  - pdf -> png/jpg

- Infected code can not survive such a drastic modification

Wipe to give away

- Data is still there even if it’s formatted
  - experts can read the data by using special tools
  - an electric microscope can read more
  - leakage of secret data
- You need to make sure the data is erased

  -
    ```
    # dd if=/dev/urandom of=/dev/<disk> bs=16M
    ```

Recover

- ‘clean install’ from a scratch
  - format the disk, use a proper OS image
- Apply latest OS patches to be up-to-date
  - it could be vulnerable before patched
  - do update in a secure network
- Install needed applications
  - check upgrades, of course

Recover (cont.)

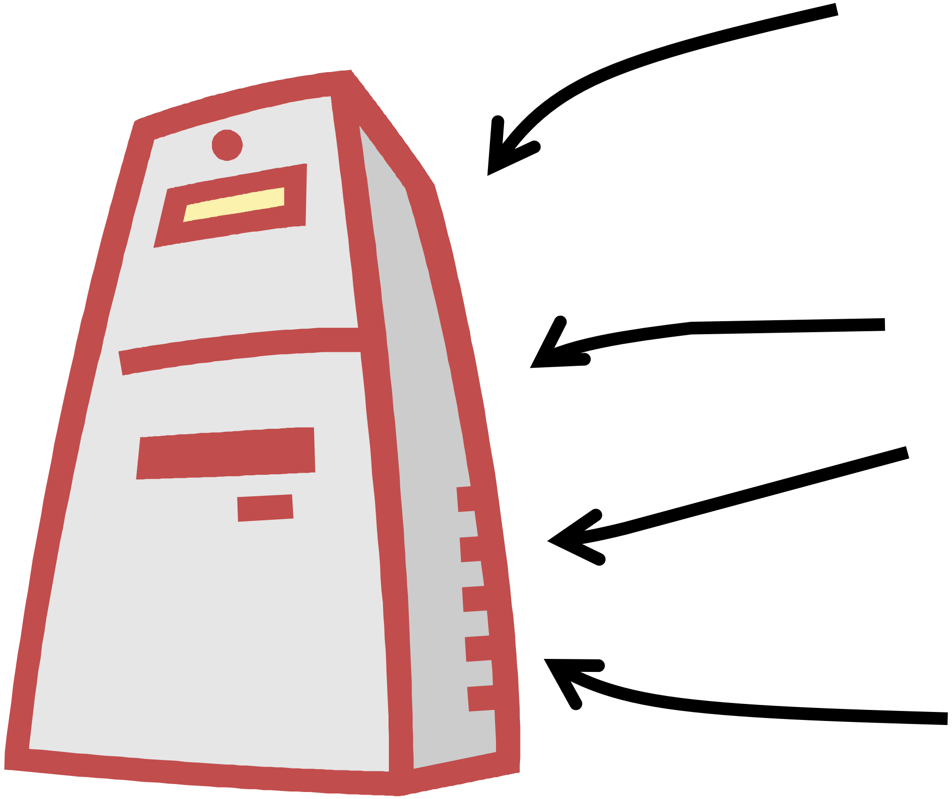
- Disable unnecessary services
  - The same as hardening procedure
- Check configurations
  - If any weakness
- Change all password on the system
  - Any password might be stolen

Replacing might be your choice

- Securing the compromised system as is
  - for further investigation
  - malware that stays in the memory only
- Just replace the compromised system
  - spare hardware

Backups

- Encryption
- Automation
- Generations



Encryption

- Assume theft and lost
- Your backups must have at minimum the same encryption level as the source data

Automation

- We are lazy!
  - Easy to forget

- Automated backup will help you
  - Most systems have scheduled backup

Generations

- You should have a ‘good’ version of backup there
  - if a system is compromised, malware might be also backup in the archive, you won’t want to restore that though
  - if something goes wrong by change, you may restore the previous version
- Find a ‘good’ version from your archives

Off-site archives

- 2011 Tohoku earthquake and tsunami
  - flushed buildings, data centers
  - 4 local governments lost whole data on the family registration system
- They have off-site backups ☺
  - took about 1 month to recover though
  - wanted to make sure nothing is missed