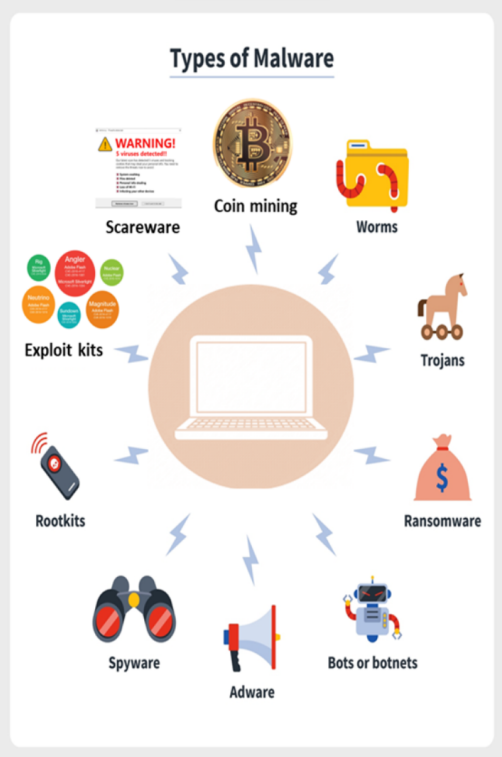
Unit 3

Malware

1. **Coin miners**
   - generates crypto coins and requires significant computing resources
   - XMRig mining Monero cryptocurrency.
2. **Scareware**
   - tricks users into believing their computer is infected with a virus.
3. **Exploit Kits**
   - a set of malware intended to exploit known vulnerabilities
   - Browsers, Adobe Flash Player, Oracle Java
   - Magnitude, Redline, Neutrino, Angler, Rig

1. **Rootkits**
   - remote access of device to hackers
   - bootloaders, firmware, kernel mode

1. **Spyware/keylogger**
   - monitor user activities or collect info
   - darkhotel, fireball, snake
2. **Adware**
   - Advertising software that serve fake advertisements
3. **Wipers**
   - Delete data from computers
   - oon, NotPetya



8. **Virus**
   - require a host program to trigger the infection.
   - The virus writes into a host program/file/boot/usb to infect or propagate.
   - Upon execution of infected program/file/… there is propagation/damage.
9. **Worms**
   - spreads through a network by replicating itself
   - Stuxnet, Trickbot
10. **Trojans**
    - a Trojan horse is any malware that misleads users of its true intent.
    - The term is derived from the Ancient Greek story that led to the fall of the city of Troy

10. **Ransomware**
    - denies access to your data till ransom is paid
    - Ryuk, Conti, REvil, Petya, WannaCry

8

10. **Bots/Botnets**

Attack kit is a toolbox.

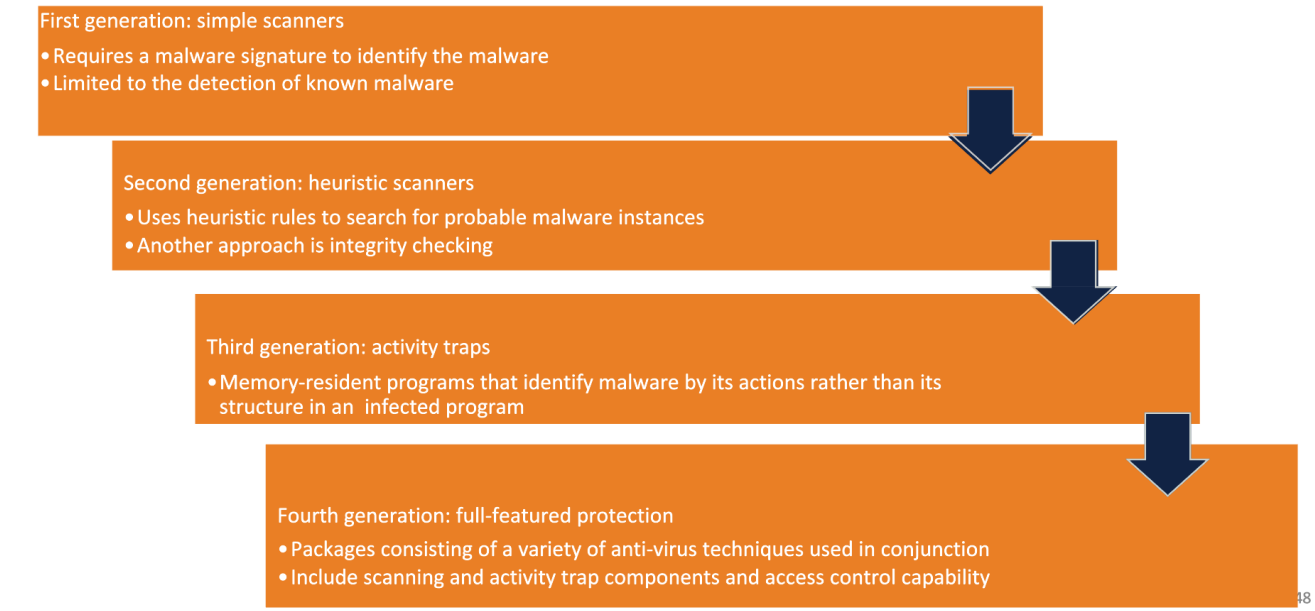
APT: Advanced persistent threat

Worm

morris worm is the first significant one. Email. tries to crack local password file.

Clickjacking is where we make the victim type or click on a thing they dont see or dont intend to.

Generations of Anti-Virus Software



antivirus generations.

conflicker worm used a windows buffer overflow exploit. it removed auto update and messed with the dns of anti virus websites.

STUXNET was not designed for windows, for SCADA -> factory software. this hit a nuclear reactor. It spread using windows tho. 3 things a printer vul, remote code and disk media shell vul.

WannaCry

Threat modelling

way to find security issues. • Think about security issues early • Understand your requirements better • Don’t write bugs into the code

trust boundary is where entities with different privilages interact.