6

MALWARE

- Sono vari i **meccanismi di propagazione**:
  - Programma che viene inserito di nascosto in un sistema al fine di corrompere la CIA o di infastidire la vittima
    - **Payload**
      - Sono vari i **meccanismi di propagazione**:
        - **Corruzione di sistema**
          - **Distruzione dei dati** → **Chernobyl**
          - **Danni nel mondo reale** → **Chernobyl**
          - **Bomba logica**
        - **Bot**
        - **Furto di informazioni**
          - **Keylogger**
          - **Spyware**
          - **Phishing** → **Spear-phishing**
        - **Occultamento**
          - **Backdoor** → È un punto di entrata segreto in un programma che consente l'accesso senza passare dalle procedure di sicurezza
          - **Rootkit** → È un insieme di programmi per mantenere un accesso nascosto al sistema con privilegi di root
            - Un esempio prevede la modifica del comportamento delle syscall in modalità kernel
              - Modifica degli indirizzi a cui puntano le syscall, per farle puntare al codice malevolo
              - Modifica del codice a cui puntano le syscall
              - Reindirizzamento del sistema ad altra tabella di gestione delle syscall
  - **Infezione di contenuti esistenti**
    - **Virus**
      - Sono composti da tre parti e durante la loro vita attraversano quattro fasi:
        - **Vettore di infezione**
        - **Trigger (bomba logica)**
        - **Payload**
        - **Fase dormiente**
        - **Fase di propagazione**
        - **Fase di attivazione**
        - **Fase di esecuzione**
      - Frammenti di software parassita che infettano programmi, al fine di modificarli e propagarsi
        - Esistono vari tipi di virus in base a:
          - Target
            - **Settore di boot**
            - **File**
            - **Virus macro**
              - Si attaccano ad un documento in modo da modificare il funzionamento in fase di esecuzione
            - **Multipartito**
          - Strategia di occultamento
            - **Virus criptato** → una porzione è cifrata
            - **Virus invisibile** → creato e manutenuto per essere invisibile ad antivirus
            - **Virus polimorfici** → le copie prodotte sono diverse ma con stessa funzione
            - **Virus metamorfici** → le copie prodotte sono diverse anche nella funzione
  - **Ingegneria sociale**
    - **Spam**
    - **Trojan**
      - Continuano a svolgere la funzione del programma di hosting ma eseguono anche la funzione dannosa
      - Continuano a svolgere la funzione del programma di hosting ma modificando il comportamento
      - Eseguono solo la funzione dannosa
  - **Sfruttamento delle vulnerabilità software**
    - **Worm**
      - Programma che cerca attivamente sistemi da attaccare e da usare come trampolino per ulteriori infezioni
      - Esistono vari tipi di virus in base a:
        - Posta elettronica o servizi di messagistica istantanea (come allegato)
        - Condivisione di file su supporti rimovibili
        - Esecuzione remota
        - Accesso remoto
        - Trasferimento di file remoti
      - La prima funzione nella fase di propagazione è la **scansione** di sistemi di attaccare (o **fingerprinting**)
        - **Casuale**
        - **Hit List**
        - **Topologico**
        - **Subnet locale**
    - **Mobile Code** → Programma che può essere usato senza modifiche su un insieme eterogeneo di piattaforme
    - **Drive by download** → Sfrutta le vulnerabilità dei browser in modo che l'utente quando visita un sito malevolo scarica il worm → **Watering-hole**: Variante in cui il target è limitato
    - **Malvertising** → Annunci pubblicitari
    - **Clickjacking** → Introduzione di layer per indurre l'utente a premere su un collegamento semi invisibile verso sito malevolo o di indurre l'utente a digitare informazioni in frame controllati dall'attaccante
- **Contromisure**
  - La migliore è la prevenzione (policy, consapevolezza, mitigazione delle vulnerabilità e mitigazione delle minacce)
    - Se ciò fallisce:
      - **Rilevamento**
      - **Identificazione**
      - **Rimozione**
  - **Antivirus**
    - Hanno vissuto 4 epoche
      - **1: scanner semplici**
      - **2: scanner euristici**
      - **3: scanner di attività**
      - **4: protezione completa**
  - **Sandbox e macchine virtuali**
  - **Firewall**