Difesa da intrusioni e virus

Prof. Francesco Bergadano

Dipartimento di Informatica

Università di Torino

Attacchi alla Sicurezza dei Calcolatori

- Utilizzo non autorizzato di risorse *(intrusioni, fallimento di controlli di accesso)*
- Inserimento/modifica di software non autorizzato *(virus, cavalli di troia)*

Virus, worm, cavalli di Troia

Programmi dannosi

- Virus
  - si duplicano, eseguiti da un utente autorizzato
- Worm
  - si duplicano, si spostano autonomamente
- Cavalli di troia
  - non si duplicano, eseguiti da utente autorizzato

Virus

- Si riproduce in altri eseguibili presenti sul sistema
- Provoca un danno
  - non immediato, per evitare che l'utente se ne accorga subito e impedisca una ulteriore propagazione
- Esegue il programma originario
  - per fare in modo che l'utente non ne rilevi la presenza

Metodi di propagazione

- Eseguibili spostati dall'utente
- Macro di applicativi noti (es. Word)
- Loveletter (inganno per estensione file)
  - Il virus loveletter (noto anche come 'I love you') si presenta in alcune varianti e induce l'utente a salvare un allegato mail e a eseguirlo con un doppio click. L'allegato non ha tuttavia l'aspetto di un eseguibile, ma può apparire come lettera o immagine.

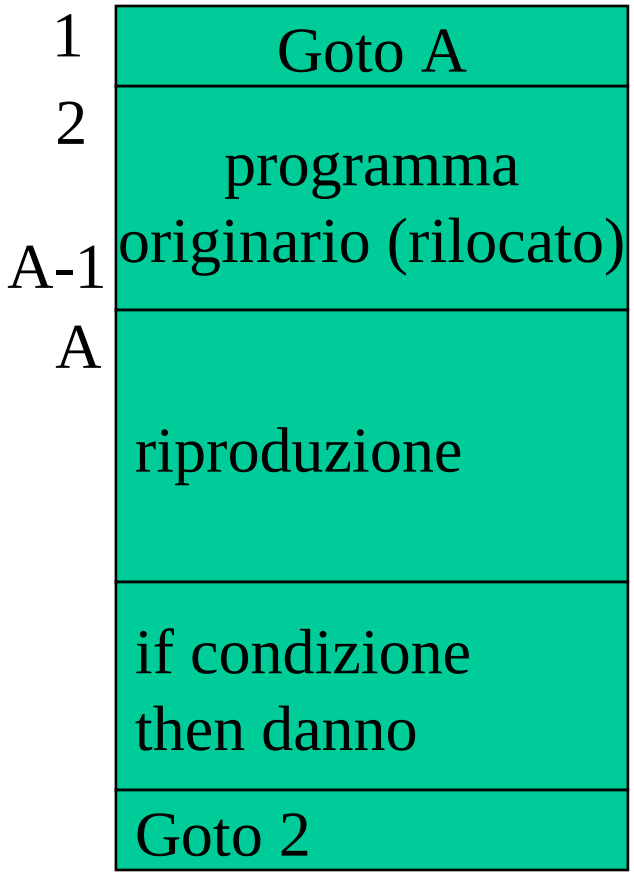
Metodi di propagazione

- Esecuzione automatica (outlook)
- Combinazione con Worm (nimda)

Difese

- Antivirus
  - installare sempre un antivirus su PC
- Autenticare i file
- Educare gli utenti
  - non eseguire programmi ricevuti via mail
  - non scaricare programmi da rete in modo incontrollato
- Sistema backup

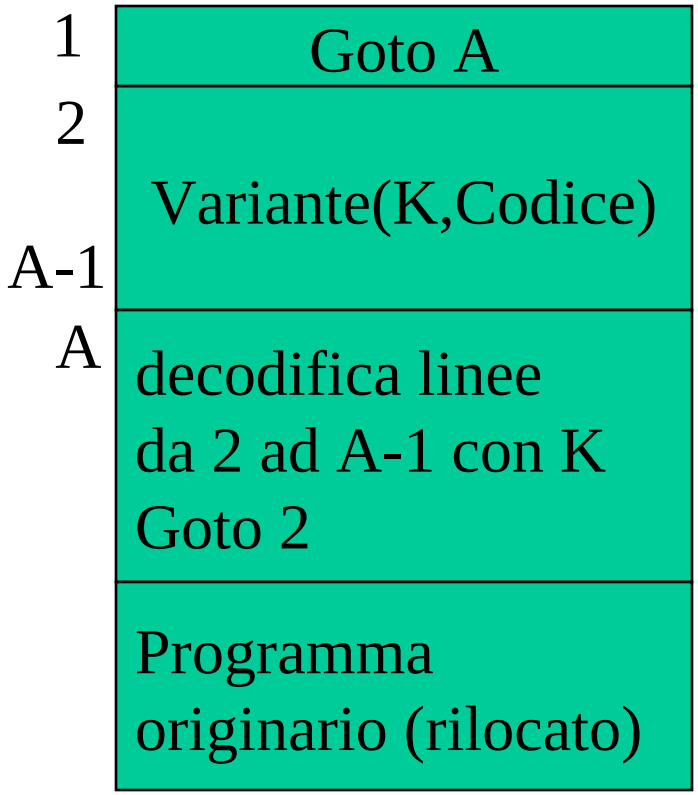
Virus (prima generazione)



Antivirus

- Si basano sul rilevamento di una traccia del virus (signature) in programmi eseguibili presenti nel sistema.
- Sono in grado di rimuovere il virus dopo averlo individuato.
- Devono essere sempre aggiornati, per poter rilevare nuovi virus.

Virus ‘polimorfi’



Worm

- Esempio storico importante:
  - Internet Worm di Morris (1988)
- Si propaga molto velocemente via rete
- Sfrutta debolezze note di un sistema (per Unix: finger, sendmail), che gli permettono di eseguire un breve programma.
- Nuovo episodio: Code Red / Nimda (2001)

Cavalli di Troia

- Rischio sempre presente
- Non si duplicano

Difesa -> configurazione shell, non eseguire programmi in modo incontrollato (Curry - Unix security)

Ransomware

- Software «ricatto»
- Nelle ultime versioni (es. Cryptolocker), basato sulla cifratura a chiave pubblica dei file della vittima