Conosciamo il Nemico - Malware & Overflow

Michele Corrias

Lombardia Plus 2019 Cyber Security - GALDUS

11/01/2020

Index

1 Introduzione

2 Malware

Software

Applicazioni

Categorie

1. applicazioni software → tutto principalmente scritto in C (`Linux`, `Microsoft Windows`, `Microsoft Office`, `OpenOffice` ...)
2. applicazioni web → `PHP`, `Javascript` ...
3. codice maligno → applicazione creata per fare male, sfrutta vulnerabilità presente nel sistema

Software

Applicazioni

Attacchi

1. attacchi alle applicazioni software: inietto all'interno di codice in esecuzione altro codice eseguibile
   - *buffer overflow*
   - *format bug* o *format string*
   - *race condition*
2. sicurezza nelle applicazioni web
   - *SQL injection*
   - *XSS* e *CSRF*

Software

Applicazioni

Categorie

1. applicazioni software → tutto principalmente scritto in C (`Linux`, `Microsoft Windows`, `Microsoft Office`, `OpenOffice` ...)
2. applicazioni web → `PHP`, `Javascript` ...
3. codice maligno → applicazione creata per fare male, sfrutta vulnerabilità presente nel sistema

Software

Applicazioni

Attacchi

1. attacchi alle applicazioni software: inietto all'interno di codice in esecuzione altro codice eseguibile
   - *buffer overflow*
   - *format bug* o *format string*
   - *race condition*
2. sicurezza nelle applicazioni web
   - *SQL injection*
   - *XSS* e *CSRF*

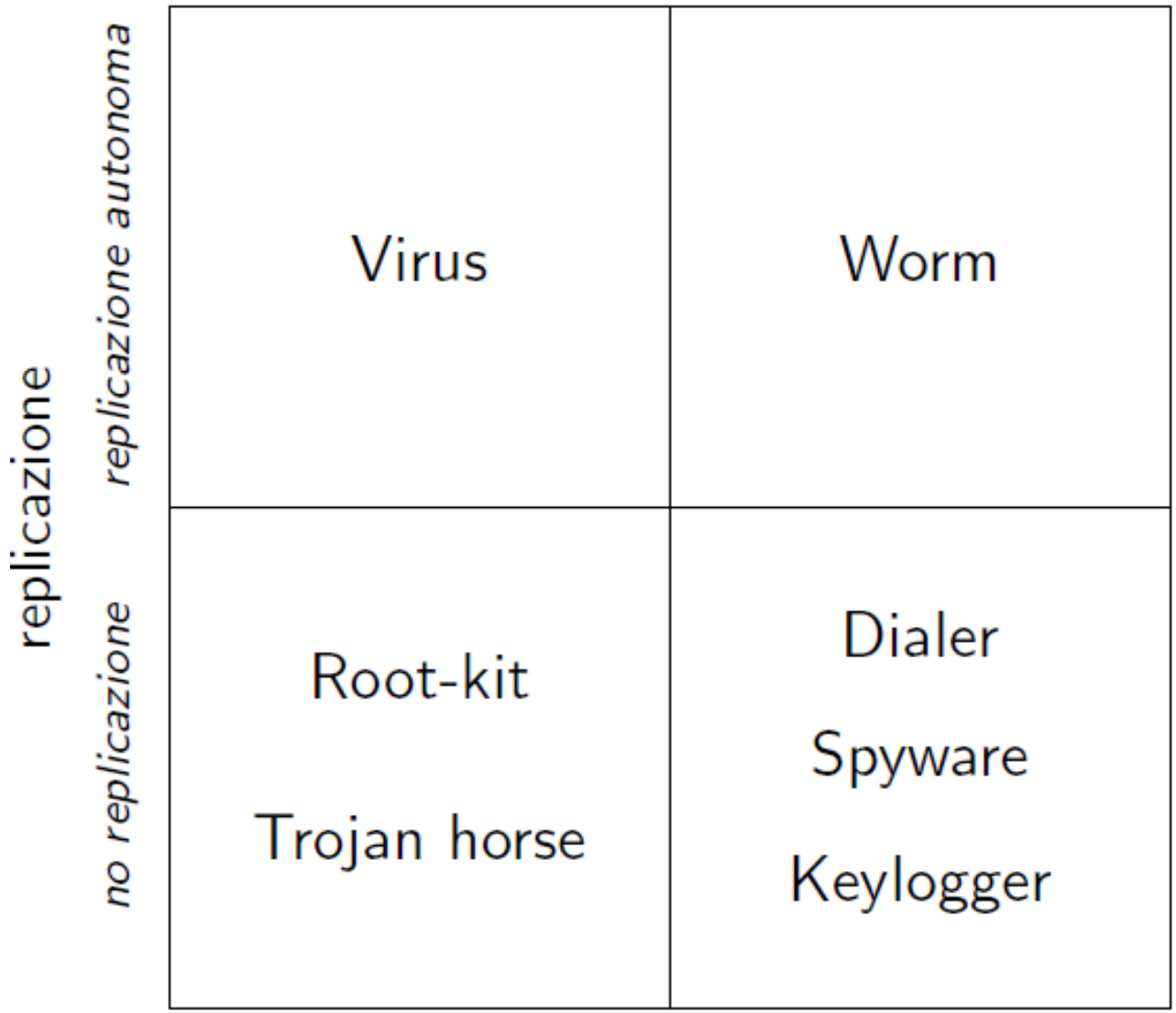
Malware

Definizione

Sequenza di codice progettata per danneggiare intenzionalmente un sistema, i dati che contiene o comunque alterare il suo normale funzionamento, all'insaputa dell'utente

Malware

Tipologie di Malware

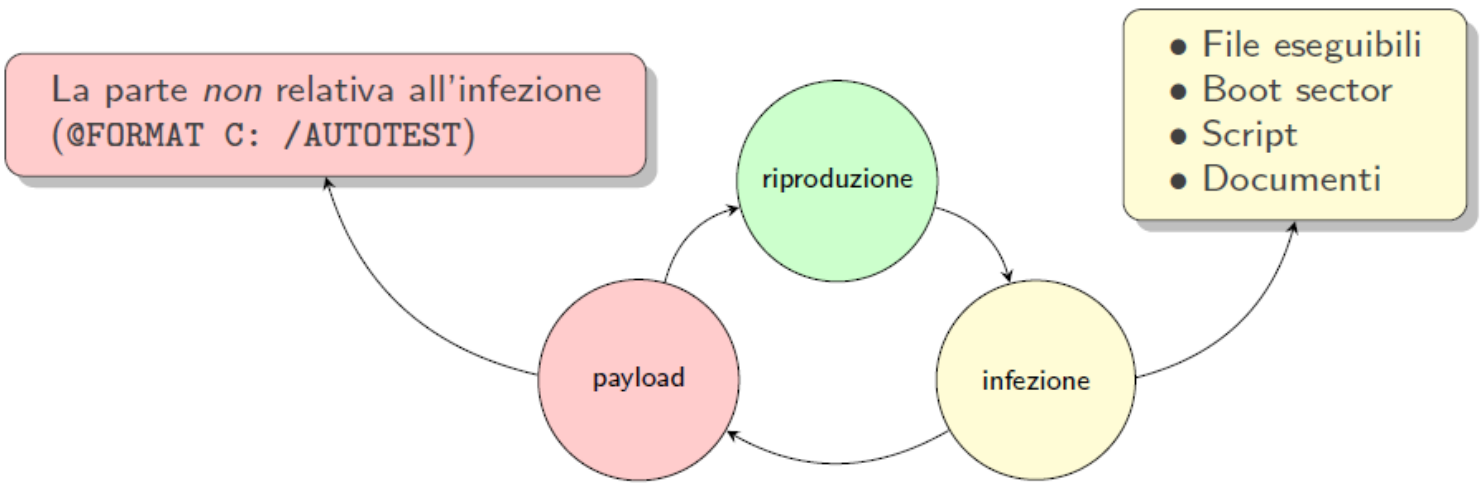


Malware

Virus

Caratteristiche

- replicazione autonoma
- necessitano di un ospite in cui inserirsi
- riproduzione attraverso la *diffusione dell'ospite*, cioè del file infetto



Malware

Virus

File Infection

Tecniche di infezione:

- companion
- sovrascrittura
- inserimento in testa/coda/*cavity*
- *entry point obfuscation* (*EPO*)

Malware

Virus

Companion Virus

- sfruttare la precedenza dei `.com` sui `.exe`
  (es.: `notepad.com` e `notepad.exe`)
- sfruttare l'ordine con cui un eseguibile viene cercato nel *path*
  (es.: `$PATH=/usr/local/bin:/usr/bin:/bin:...`)
- meno efficace quando si usa la GUI

Malware

Virus

Sovrascrittura

- parte del codice dell'ospite è sostituito con quello del virus
- l'ospite non funzionerà più correttamente ($\rightarrow$ rimozione impossibile)

Malware

Virus

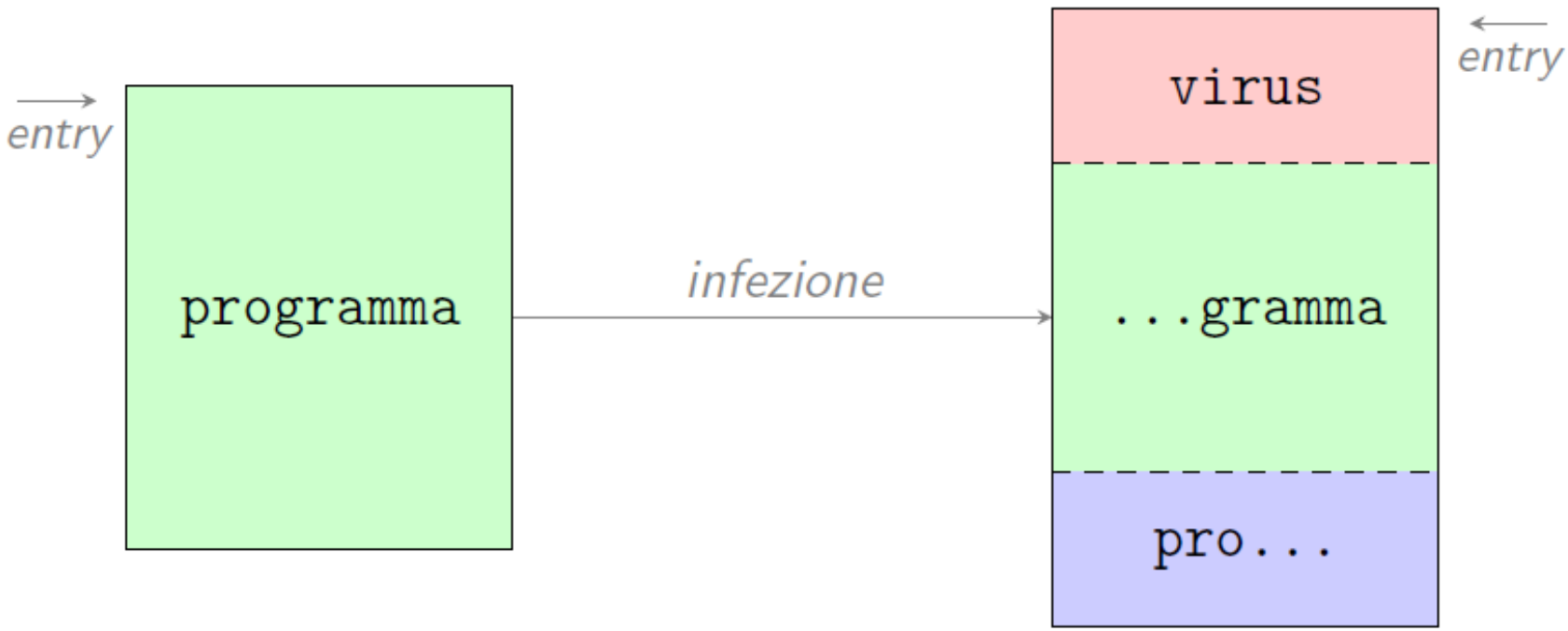


Figura 1: Parasitic virus: inserimento in testa

Malware

Virus

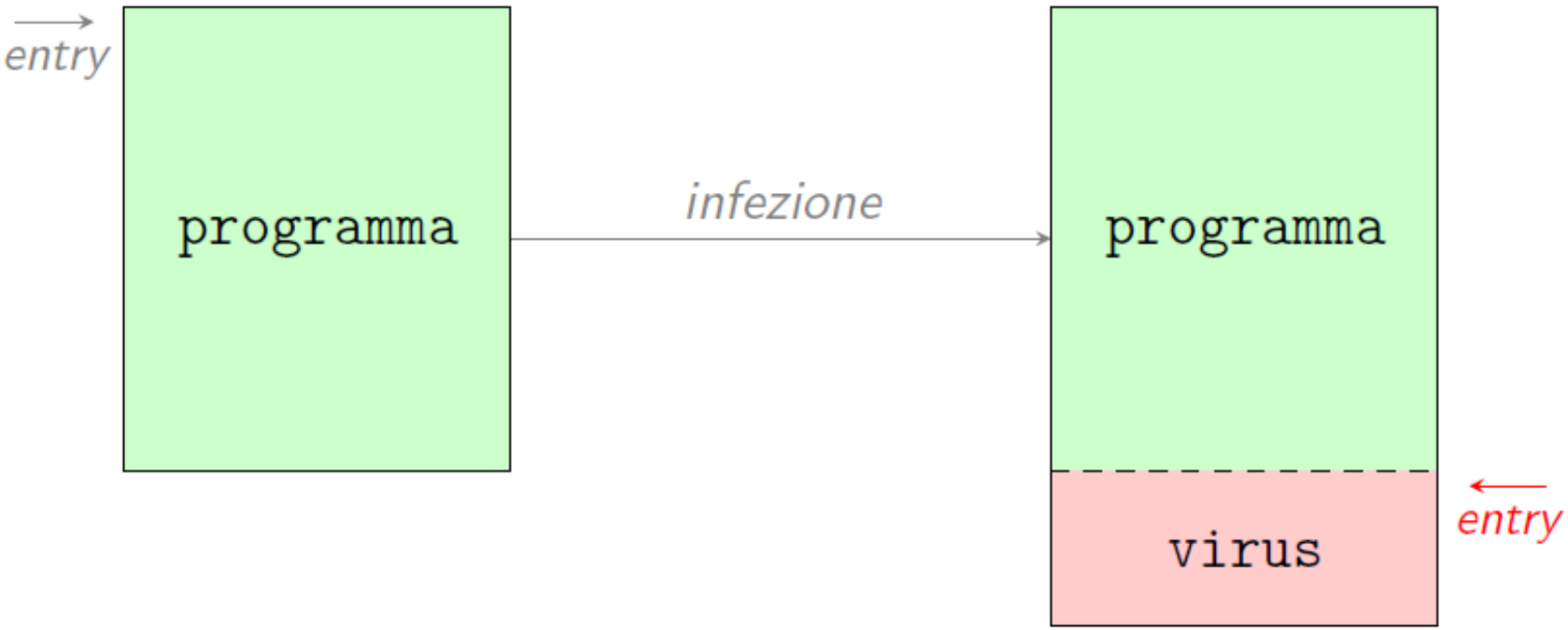


Figura 2: Parasitic virus: inserimento in coda

Malware

Virus

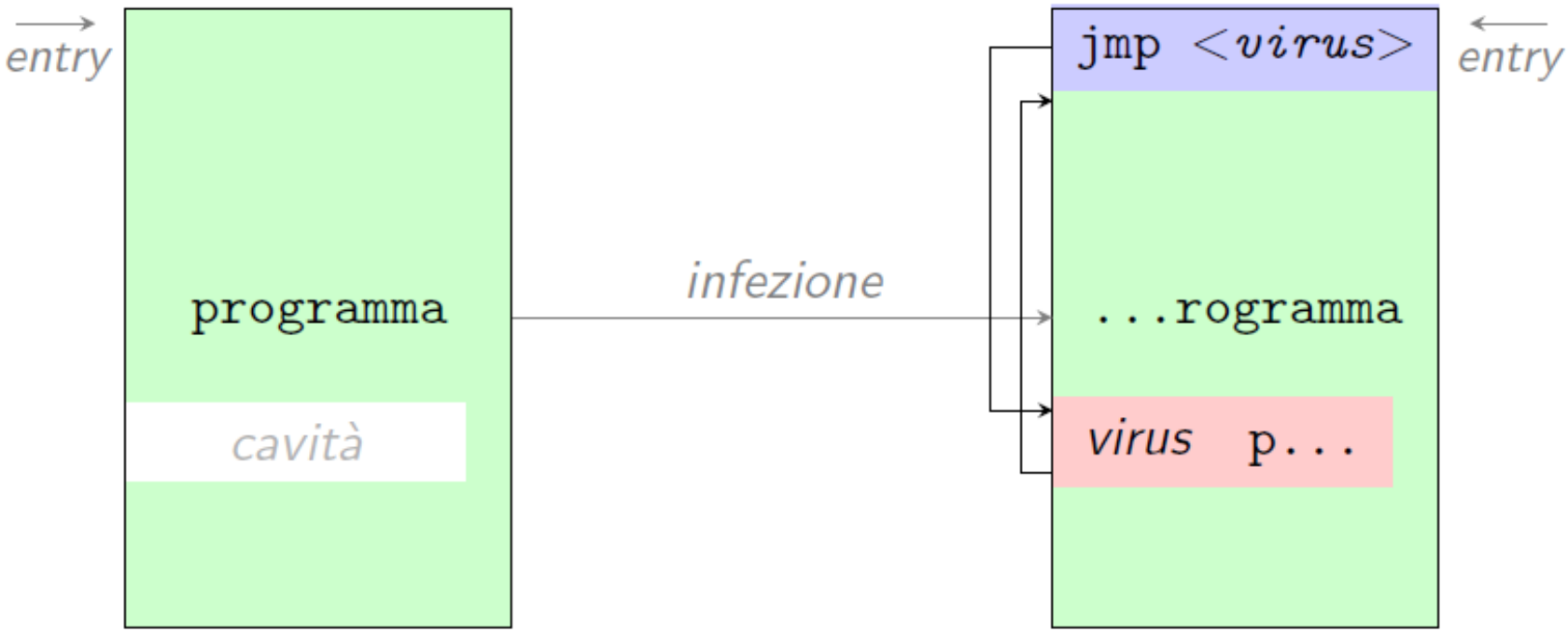


Figura 3: Cavity virus

Malware

Virus

Entry Point Obfuscation

- EPO
- modifiche all'*entry point* originale di un programma sono facilmente identificabili:
  - ```
    :~$ readelf -h /bin/ls
    ELF Header:
    Class: ELF64
    ...
    Entry point address: 0x4046d4
    ```
- il virus ritarda il passaggio del controllo al suo codice
- il virus può ottenere il controllo in modo casuale in in qualsiasi punto (tramite la sovrascrittura di una chiamata a funzione o la modifica della *import table*)
- metodo *anti-heuristic*: difficile da individuare, disinfettare e rimuovere
    ```

Malware

Virus

Code Integration

- *disassembling* del codice eseguibile del file vittima
- *inserimento* nel codice vittima
- *re-assembling*
- `W95.ZMist` o `ZOmbie.Mistfall`

Malware

Virus

Device infection

Infezione di dispositivi removibili: USB pen drive ...

- file `autorun.inf`
  - `[autorun]`
    `open=Knight.exe open`
    `icon=Knight.exe,0`
    `shellexecute=Knight.exe open`
    `shell=auto`
    `action=Disk Knight(Protection Against Mobile Disk Viruses)`
    `shell\auto=&Auto`
    `shell\auto\command=Knight.exe open`
    `shell\open=&Open`
    `shell\open\command=Knight.exe open`
    `shell\explore=E&xplore`
    `shell\explore\command=Knight.exe open`
    `shell\find=S&earch...`
    `shell\find\command=Knight.exe open`
    `...`

Malware

Virus

MBR Infection

Master Boot Record = porzione dell'hard disk che contiene il codice responsabile dell'avvio del sistema operativo

- un virus può modificarlo per venire eseguito prima del sistema operativo stesso
- difficile da individuare
- tecnica vecchia (1986-: `(c)Brain`, `Stoned`, `Michelangelo`, `Junkie`, `Tequila` ...)
- tornata poi di moda (2007: `Rustock bootkit`, 2008: `Trojan.Mebroot`, 2010: `TDL 1-4` ...)