malware

software malevolo
virus, trojans, worm, rootkits & Co.

malware

- Qualsiasi software che si comporta in modo illecito o malevolo nei confronti dell'utente
- presenti fin dai tempi dell'univac (1974)
  - ampia diffusione con i personal computer
- moltissime tipologie e varianti
  - classificazione molto complessa
  - più che una classificazione del software si classificano le tipologie di “comportamento”
    - virus, trojan, worm, ecc.
    - es. un malware può essere contemporaneamente trojan e virus

virus

- un virus è codice eseguibile in grado di infettare (copiarsi all'interno di) altro codice eseguibile
  - esempi di codice eseguibile nativo: i programmi di sistema, le applicazioni, il boot sector, il kernel del S.O., librerie dinamiche
  - esempi di codice eseguibile non nativo: gli script in VB contenuti dentro documenti MS Office, i file postscript (parente stretto dei pdf), java, perl, ecc.
- cioè è in grado di riprodursi e diffondersi automaticamente all'interno di un sistema
  - all'interno dei confini imposti dal sistema operativo
    - mediante il “controllo di accesso”
  - sono più diffusi nei sistemi Windows dove il confinamento è tradizionalmente meno stretto

virus

- alcuni sono dei semplici scherzi, altri danneggiano irreparabilmente il sistema
- usavano mezzi “sociali” per la diffusione
  - una volta erano i floppy disk (larga diffusione con l'MS-DOS)
  - ora è sopratutto l'email e lo spam (sottoforma di trojan), ma anche il web (vulnerabilità dei browser).

tipologie di virus

- possono essere...
  - residenti nella macchina
    - in esecuzione come dei demoni
  - stealth
    - attvamente si adoperano per non far vedere che ci sono
    - vedi rootkit per le tecniche adottate
  - possono attaccare
    - file eseguibili
    - boot sector
    - il kernel
    - i processi
  - polimorfi o mutanti
    - cambiano il loro codice

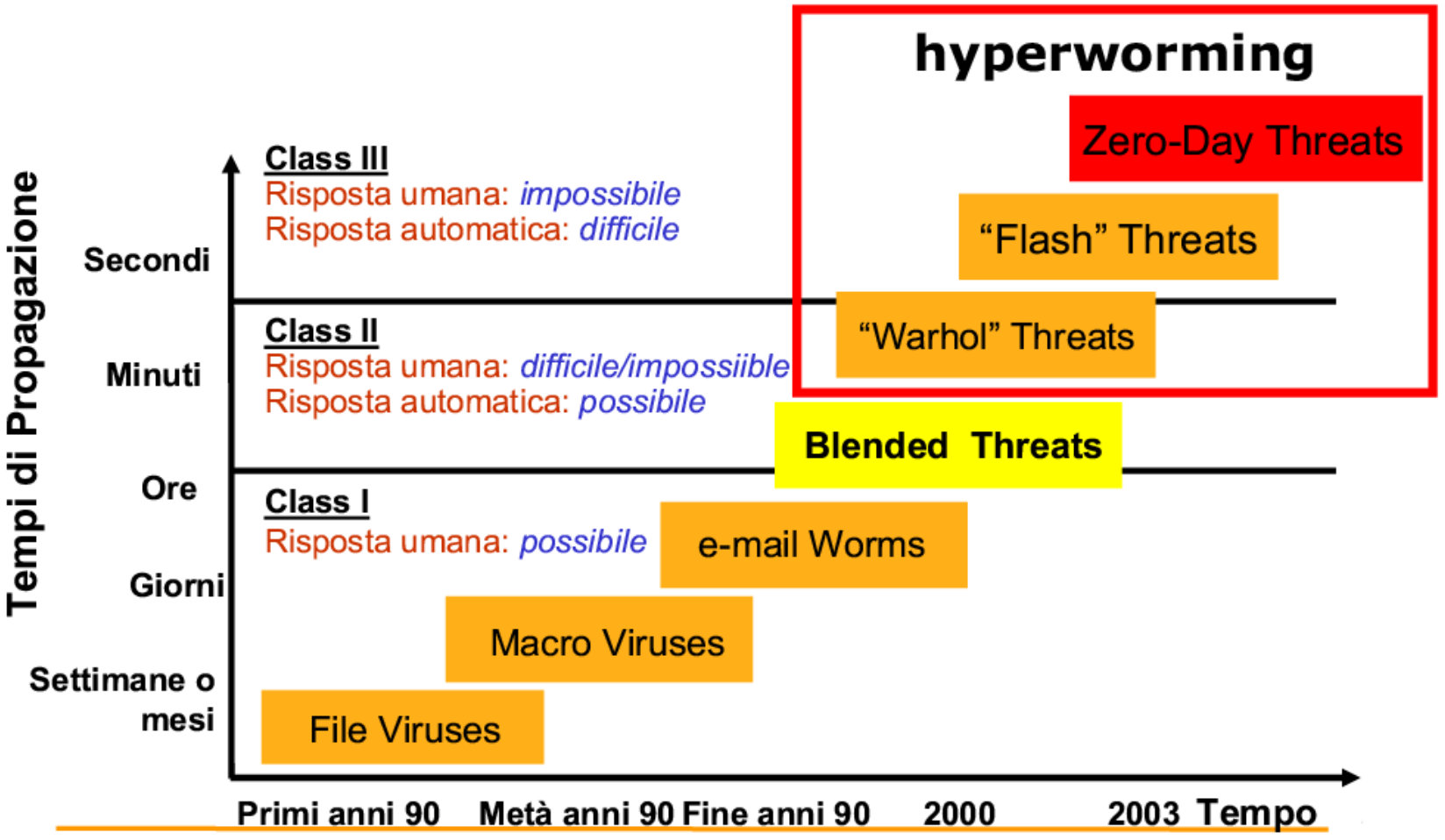
trojan horse

- un eseguibile che si spaccia per innocuo ma esegue attività malevole
  - la diffusione è tipicamente via email
- il codice malevolo contenuto è detto payload

worm

- sono una evoluzione dei virus
- si diffondono attraverso la rete sfruttando tecniche di discovery e vulnerabilità note
  - es. buffer overflow di servizi standard
- il sistema vulnerabile viene attaccato e quindi infettato
- la velocità di diffusione è enorme, solitamente infettano tutti i sistemi vulnerabili nell'arco di 15 minuti

tempo di propagazione: evoluzione



fonte www.cnipa.gov.it (govCERT.it)

zombies e botnet

- alcuni malware rimangono in attesa che il sistema sia utilizzato da un hacker (installano una backdoor)
  - tipicamente trojan, virus o worm
- una rete di zombies comandabili coerentemente è detta botnet
- spesso gli zombies sono comandati mediante Internet Relay Chat (IRC botnet)
- usi
  - 50-80% dello spam viene da zombies
    - risparmio di banda, indirizzi diversi confondono gli antispam
  - Distribute DoS (attacchi famosi a Yahoo, eBay, ecc)
  - click frauds (siti con annunci “pay per click”)
  - hosting di siti di phishing
- fonte: http://en.wikipedia.org/wiki/Zombie_computer

antivirus

- suite software che...
  - verificano che non vi sia traccia di virus negli eseguibili del sistema (approccio reattivo)
  - verificano che non vi sia traccia di virus negli eseguibili che state per eseguire (approccio proattivo)
  - sono in grado di rimuovere virus scoperti
  - contengono un DB di firme di virus noti
  - sono in grado di aggiornare (update) il DB automaticamente via rete
- possono essere pensati come delle soluzioni integrate di intrusion detection and prevention per uso personale

antivirus

- inizialmente gli antivirus erano basati sul riconoscimento di sequenze
- virus mutanti rendono molto più difficile l'intercettazione
  - ora ci sono anche tecniche di tipo euristico (esempio verificare la automodifica o l'accesso a file eseguibili o al bootsector)

rootkit

- suite software che permette ad un hacker penetrato in un sistema di modificarlo in modo che...
  - il sistema sia sotto il controllo del‘hacker
  - sia molto difficile accorgersi dell'intrusione
- sono utili al hacker dopo che l'intrusione è già avvenuta
- la modifica del sistema è automatica e non richiede conoscenze approfondite
  - purché il sistema sia conforme alle specifiche del rootkit
- www.rootkit.com (per sistemi windows)

rootkit: tipologie

- rootkit tradizionali
  - installano backdor e sniffer
  - modificano eseguibili di sistema in modo che la presenza delle backdor e dello sniffer non sia scoperta
  - gli eseguibili modificati sotto unix sono spesso ps, ls, who, login, ecc.
  - puliscono i log
- nuova generazione di rootkit kernel based
  - modifica il kernel “al volo” dirottando delle system call (tipicamente la open_file)
    - installazione di moduli del kernel (sotto Linux)
    - modifica dell'immagine del kernel

script kiddies

- “ragazzini” che utilizzano strumenti di attacco sviluppati da altri per introdursi in sistemi altrui
- 80% del traffico maligno su Internet è generato da script kiddies
- gli attacchi degli script kiddies sono innocui per sistemi correttamente configurati e gestiti
  - in cui sono state applicate le ultime security patch
- gli strumenti degli script kiddies sono
  - trojan
  - zombies
  - exploit già pronti (script)
  - rootkit

SpyWare

- Software che raccolgono informazioni su ciò che l'utente fa o ha installato sul pc e la trasmette ad altri
  - che applicazion ho installato? che siti visito? che password ho nella mia cache? che carte di credito sto usando?
- si nascondono in applicazioni free di uso comune (approccio trojan)
- è legale distribuirli se la licenza d'uso dichiara l'attività di monitoraggio.
  - quasi mai la licenza d'uso è letta con attenzione

AdWare

- (1) A form of spyware that collects information about the user in order to display advertisements in the Web browser based on the information it collects from the user's browsing patterns
- (2) Software that is given to the user with advertisements already embedded in the application.
- fonte www.pcwebopedia.com

social engineering

social engineering

- l'insieme di tecniche "sociali" che hanno l'obiettivo di manipolare le persone inducendole a…
  - divulgare informazioni confidenziali
  - fare cose contro la politica di sicurezza

persone manipolabili

- call center
- amici
- utenti
- amministratori di sistema

- cfr. Kevin Mitnick

hoax

- email che raggirano l'utente convincendolo a fare cose a suo svantaggio

hoax: esempio

```
Subject: BAD virus - act quickly!!
Date: Tue, 29 May 2001 21:57:22 -0400

Subject: Please Act Urgently
VIRUS COULD BE IN YOUR COMPUTER
It will become activate on June 1st and will delete all files and folders
   on
the hard drive.
No Anti-Virus software can detect it because it doesn't become a VIRUS
until 1/6/2001.
It travels through the e-mail and migrate to your computer.
To find it please follow the following directions:
Go To "START" button
Go to "Find" or "Search"
Go to files and folders
Make sure to search in drive C
Type in; SULFNBK.EXE
Begin Search
If it finds it, highlight it and delete it
Close the dialogue box
…..
```

- SULFNBK.EXE è però un programma che è regolarmente parte di Windows!

phishing

- acquisizione illegale di informazioni confidenziali (es. passwords) ottenuto “impersonando” una entità fidata
- la vittima è adescata tipicamente via email
  - ma anche telefonicamente
- l’entità fidata viene spesso impersonata tramite clonazione del sito web
  - con url simili

phishing

- javascript può essere usato per cambiare l'url nella "address bar"
  - l'utente interagisce con il sito clonato ma l'url appare corretto
  - una occhiata attenta al certificato (se c'è) rivela il problema

cross-site scripting (XSS)

- vulnerabilità dei siti
- i server-side scripts possono usare parti dell'url per formare le pagine visualizzate
- dai parametri nell'url l'html può essere iniettato nella pagina di risposta
- html può contenere client-side scripts
- il codice iniettato può inviare dati immessi nella form a chiunque
- molto difficile da rilevare perché il sito è quello giusto!

cross-site scripting

- ciò che si vede nell'email
  - "La preghiamo di verificare che il suo conto corrente presso securebank.com non contenga addebiti illeciti."
- il sorgente
  - "… presso securebank.com …"
  - script iniettato: <script>... </script>

cross-site scripting

- gli script server site usano il parametro “t” per il titolo della pagina
- ciò che l’utente vede
  - una pagina con titolo “login sicuro”
- il sorgente che lo produce
  - <title> login sicuro <script>…</script> </title>
  - <script>…</script> viene eseguito dal browser
- lo script può essere sofisticato e inviare username e password all’attaccante