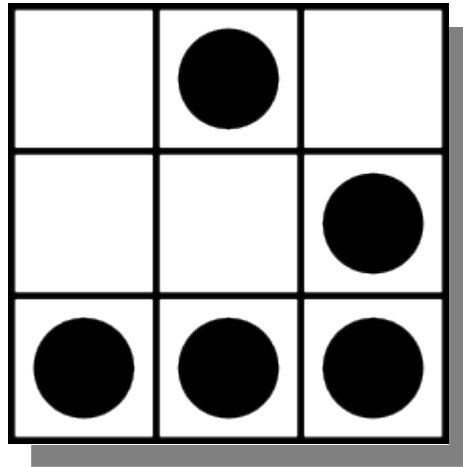


# Virus ed Anti-Virus...

---



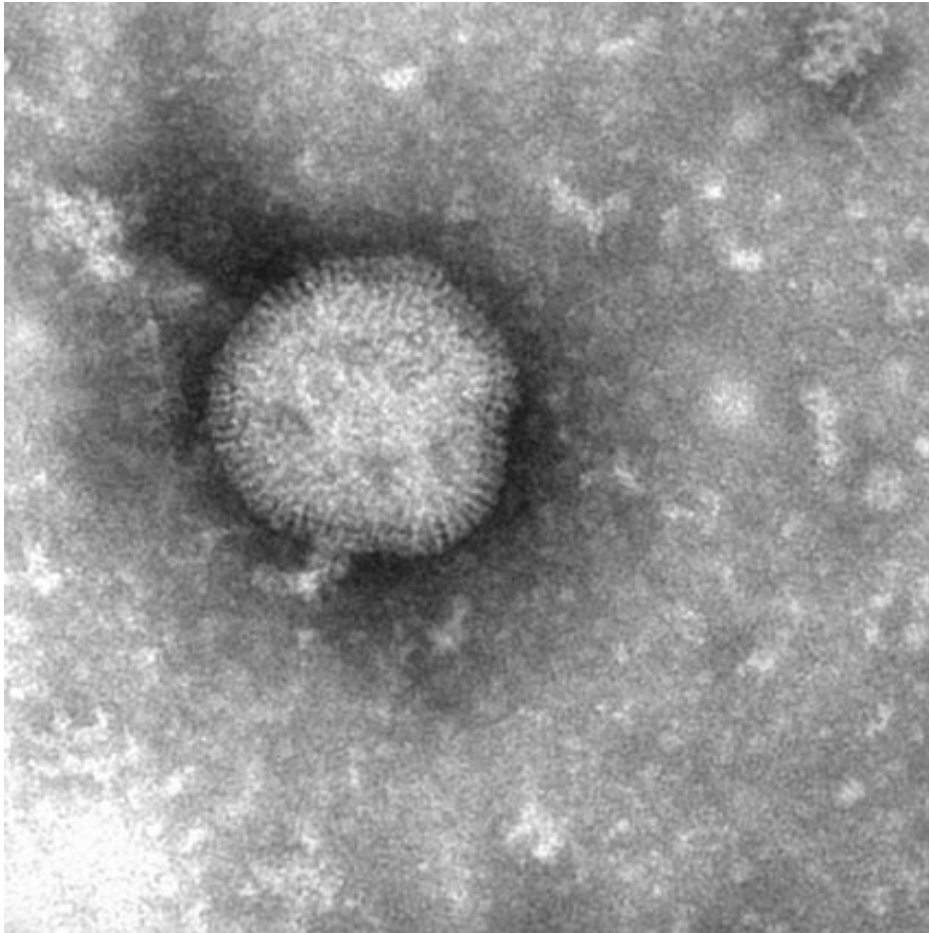
Giacomo Rizzo [ a.k.a. alt-os ]

alt-os@openlabs.it



# I virus: cosa sono?

---



Il virus dell'influenza.

- Una delle maggiori cause di problemi più sentiti dagli utenti di oggi (soprattutto Microsoft), sono certamente i Virus.
- Il termine “virus” è in realtà utilizzato in maniera completamente errata, a causa della scarsa conoscenza che i mass media hanno dell'informatica (e non solo)
- Prima di tutto, quindi, chiarezza!

# I virus: cosa sono?

---

- Il concetto che in genere si vuole indicare con il termine “Virus” ha un nome preciso, e si chiama “malware”
- Definizione da “Wikipedia.org”:

Si definisce malware un qualsiasi software creato con il solo scopo di causare danni più o meno estesi al computer su cui viene eseguito. Il termine deriva dalla contrazione delle parole inglesi *malicious* e *software* e ha dunque il significato letterale di "programma malvagio"; in italiano è detto anche *codice maligno*.
- Nella categoria dei “malware” troviamo una vasta quantità di categorie differenti, a seconda del loro metodo di propagazione e di funzionamento.
- Ne vedremo nelle prossime slides una lista, ma va detto da buon inizio che non si tratta certamente di un elenco esaustivo e preciso (possono esistere anche incroci tra diverse categorie).

# I virus: cosa sono?

---

- **Virus**

- Parti di codice che si diffondono copiandosi all'interno di altri programmi, o in particolari sezioni del disco fisso (ad esempio l'MBR, o “master boot record”), in modo da essere eseguiti ogni qual volta il file infatti viene aperto (o eseguito).
- Si propagano da un computer all'altro tramite lo scambio di files infetti da parte degli utenti.
- Utilizzano tecniche di “camuffamento” per evitare di essere riconosciuti ed individuati dall'utente per il tempo piu lungo possibile.
- Maggiore è il tempo che riescono a rimanere nascosti, maggiori le probabilità di infettare anche altri computer.
- Non sono necessariamente dannosi per il sistema operativo “ospitante”, ma sprecano comunque risorse (sono eseguiti).

# I virus: cosa sono?

---

- Si assume come regola generale che un virus danneggi solo il “software” presente sul sistema, ma può tranquillamente provocare anche danni all'hardware, ad esempio spegnendo le ventoline di raffreddamento, o portando le testine di lettura dei dischi fissi ad un super-lavoro.
- In genere ha dimensioni ridottissime, di pochi kilobytes (piu grande è, piu facilmente verrà individuato). Le ridottissime dimensioni lo costringono a poter eseguire solo pochissime istruzioni, a volte solo quelle che ne permettono la duplicazione.
- Il termine “Virus” appare la prima volta nel 1970, in un romanzo di fantascienza di David Gerrold intitolato “When H.A.R.L.I.E. was One”.
- Il primo “virus” noto, è “Elk Cloner”, del 1982, scritto da Rich Skrenta sul DOS 3.3 della Apple, e si propagava tramite scambio di floppy disk.

# I virus: cosa sono?

---

- Un virus “basilare” si compone di 2 diversi pezzi di codice:
  - Routine di ricerca
    - Serve a cercare sul sistema i files adatti ad essere infettati e che non lo siano già (inutile infettare due volte lo stesso file).
  - Routine di infezione
    - Ha il compito di copiare il codice del virus all'interno del file trovato dalla “routine di ricerca”.
- Spesso però, contengono anche routine aggiuntive:
  - Routine di attivazione
    - Il virus si può attivare in una particolare data, o secondo criteri scelti dal virus-writer
  - Payload
    - Una serie di istruzioni aggiuntive, solitamente dannose per il sistema ospitante.

# I virus: cosa sono?

---

- Più di recente, allo scopo di rendere più difficile il lavoro degli anti-virus, i virus-writer hanno cominciato ad introdurre routine di cifratura:
  - Routine di decifratura
    - Decifra il codice del virus, rendendolo di fatto eseguibile da parte del sistema operativo ospitante.
  - Routine di cifratura
    - Ha il compito di cifrare il codice del virus, rendendolo di fatto non eseguibile ma non riconoscibile al volo dall'anti-virus.
  - Routine di mutazione
    - Modifica i parametri di cifratura e decifratura, in modo che ogni nuova copia del virus sia “cifrata” diversamente dalla precedente, in modo che individuata una copia del virus, l'anti-virus non possa di fatto trovare le altre.

# I virus: cosa sono?

---

- La “routine di mutazione” rende vano il meccanismo di verifica dell'impronta da parte dell'antivirus, in quanto una volta modificata non è più riconoscibile. A seconda che la “routine di mutazione” modifichi tutto il codice, o ne esenti se stessa, i virus si dicono “metamorfici” o “polimorfici” (vedremo tra poco)
- Da segnalare oltretutto l'esistenza di “retrovirus”, che attaccano direttamente il software anti-virus, ibinandone o disabilitandone completamente il funzionamento (ed esempio cancellando la propria “impronta” dal database).
- Va detto che la scarsa conoscenza da parte degli utenti ma soprattutto dei “mass media” sull'argomento, favorisce la nascita e la diffusione di “hoax”, detti anche “virus burla”, che nient'altro sono se non false voci catastrofiche riguardo all'imminente diffusione di un virus “potentissimo ed ineliminabile”.

# I virus: cosa sono?

---

- Come dicevamo, non esistono solo i virus, anzi!
- **Worm**
  - Questi malware non hanno bisogno di infettare altri files per diffondersi, perchè sfruttano direttamente banchi del sistema operativo ospitante, al fine di introdursi, duplicarsi, e diffondersi, solitamente sfruttando la rete Internet.
  - Altre volte, sfruttano tecniche di “social engineering” per indurre gli utenti ad eseguirli, solitamente camuffati come allegati di messaggi di posta elettronica (esempio storico, il worm “I love you”).
    - “Ecco le nuove foto di \*\*\*\*\* nuda al mare”
    - “Ecco la nuovissima dieta dimagrante di \*\*\*\*\*”
    - “Allegata trovi la mia lettera d'amore” [I love you]

# I virus: cosa sono?

---

- Uno dei primi worm diffusi tramite la rete, “Internet Worm” o “Morris Worm”, fu scritto dal figlio di un alto dirigente della NSA (l'agenzia di sicurezza USA) il 2 novembre 1988, e riuscì a colpire oltre un terzo dei computer collegati in rete al tempo , per fortuna ancora piuttosto “pochi”.
- Poco più che una “prova”, secondo le dichiarazioni dell'autore (Robert Tappan Morris), il virus era stato progettato per “stimare” la dimensione della “rete” dell'epoca, infettando tutti i computer una sola volta.
- A causa di un errore di programmazione però, questo meccanismo non funzionò, portando ben presto alla saturazione della rete, e all'infezione di più di 6000 sistemi Unix, con una stima dei danni compresa da i 10 ed i 100 milioni di dollari. Al termine di un processo durato tre anni, Robert fu condannato a pagare 10.050 \$.

# I virus: cosa sono?

---

- I danni portati da un “worm” si possono catalogare in due grandi gruppi:
  - Danni Diretti
    - Spreco di risorse computazionali, spazio su disco ed in memoria, risorse di rete
    - Malfunzionamenti dei sistemi atti a scovarli (anti virus, firewall software)
    - Permettere l'installazione di altri malware (apertura di backdoor, keylogger, ecc ecc.)
  - Danni Indiretti
    - Miliardi di messaggi di posta elettronica invitanti ad aprire allegati di vario tipo, forma, colore e dimensione (SPAM)
    - Spreco di banda su internet

# I virus: cosa sono?

---

- **Trojan Horse**

- Il nome deriva dal “cavallo di Troia” di Ulisse.
- Si presenta sotto le sembianze di un programma utile e/o divertente, ma nasconde funzionalità tali da consentire ad un “attaccante” (in genere chi invia il file) di prendere il completo controllo del sistema sul quale il “trojan” viene eseguito (tramite, ad esempio, l'uso di backdoor)
- Esistono altri software con le stesse caratteristiche, come GoToMyPc o PcAnywhere, ma non sono da considerarsi cavalli di troia in quanto l'utente li installa appositamente per poter gestire da remoto il proprio sistema.
- La diffusione dei trojan non è solitamente automatizzata, e viene fatta volontariamente dall'attaccante. Sempre più spesso è la vittima stessa a scaricare ed installare il trojan sul proprio sistema, tramite il “peer to peer”.

# I virus: cosa sono?

---

- **Backdoor**

- Letteralmente “porta sul retro”, più che un genere di malware è la descrizione di una delle loro azioni, ma lo stesso viene utilizzato per applicativi con effetti molto simili ai “trojan”, ma che non cercano di camuffare il proprio comportamento, facendo completamente affidamento alla scelleratezza dell'utente finale.
- Le backdoor introdotte da altri tipi di malware, vengono utilizzate per moltissimi scopi, dalla creazione di “reti” di computer (atte ad esempio a compiere per interposta persona attacchi informatici di tipo DDoS, come nel recente passato con SCO), alla messa in condivisione sulle reti “peer to peer” di grandi quantità di files “piratati”
- Vengono a volte inserite direttamente da chi scrive il sistema operativo (Microsoft con Windows Media Player)

# I virus: cosa sono?

---

- **Spyware**

- Si tratta di un software che di nascosto “raccolle informazioni” riguardanti l'attività di un utente, e le spedisce poi tramite internet ad un'organizzazione che le utilizzerà per trarne profitto, tipicamente attraverso l'invio di pubblicità mirata (SPAM) o vendendole ad altri enti non sempre meglio intenzionati.
- Non sembra poi così pericoloso, ma ricordate che dal vostro computer passano molte più informazioni riservate di quante voi non immaginate: codici di carte di credito? Dati personali? Email che non vorreste far leggere ad altri? Semplici fatti vostri?
- Sono sempre più diffusi, purtroppo, e sempre più raramente gli utenti ne vengono a conoscenza. Kazaa è uno dei tanti diffusissimi software che installano anche spyware

# I virus: cosa sono?

---

- A volte, l'installazione avviene in maniera molto subdola, attraverso ad esempio pagine web appositamente formattate per sfruttare vulnerabilità del browser ed installare applicativi di vario tipo, forma, colore e dimensione, tra cui, naturalmente spyware.
- Altrimenti lo spyware ha difficilmente la possibilità di diffondersi autonomamente (simili ai trojan).
- Nella società dell'informazione, i dati personali assumono un valore sempre crescente, e i modi per “sottrarceli” sono sempre di più
- Anche l'uso dei cookies viene spesso utilizzato allo scopo di raccogliere informazioni che potremmo non voler concedere a chi gestisce un determinato sito web.
- Sistemi Windows non protetti adeguatamente possono raccogliere quantità notevoli di spyware in poco tempo.

# I virus: cosa sono?

---

- **Dialer**

- Si tratta di un programma che crea banalmente una “nuova connessione ad internet” in maniera automatica e non voluta dall'utente.
- Reso celebre dagli allarmismi (finalmente) da parte delle autorità competenti, questo genere di malware sta lentamente regredendo con il crescere del numero di connessioni a banda larga.
- La maggior parte dei dialer infatti, si basava sulle impostazioni del “modem”, che richiedevano l'inserimento di un numero di telefono, sostituendolo con un numero a tariffazione speciale.
- Il danno più grave che portano i dialer, è in genere di tipo economico. Fortunatamente si cominciano a vedere azioni di contrasto da parte di compagnie telefoniche e polizia.

# I virus: cosa sono?

---

- **Rootkit**

- Molto simili alle “backdoor”, come principio di funzionamento, i rootkit aggiungono loro la capacità di nascondersi efficacemente nel sistema, modificando appositamente tutte le applicazioni in grado di rilevarli.
- Particolarmente utilizzati per mantenere un accesso “root” a sistemi di tipo Unix (anche Linux) una volta violato un sistema.

- **Hijacker**

- Applicativo che prende il controllo del browser, impedendo ad esempio la modifica della pagina web di default, e dirigendolo di fatto su siti equivoci, o peggio, su pagine che sfruttano bug del sistema operativo per installare altri tipi di malware.

# Perchè non colpiscono GNU?

---

- Terminato l'elenco dei diversi tipi di malware e delle loro caratteristiche (che pare sempre più un bollettino di guerra), bisogna cercare solitamente di tranquillizzare gli utenti per evitare che cadano preda di allarmismi e “panico da rete” (spesso giustificato, peraltro).
- Questa operazione riesce particolarmente difficile agli utenti dei sistemi Microsoft Windows, ai quali viene solitamente consigliata l'installazione di firewall applicativi, software antivirus, antispyware, antitutto e via dicendo, nel (vano) tentativo di limitare i danni che un sistema operativo bacato può portare.
- Per i sistemi GNU/Linux, fortunatamente, la situazione è (ad oggi) più rosea e promettente.
- Ma perchè i virus non colpiscono GNU (oggi)?

# Perchè non colpiscono GNU?

---

- **Questione di numeri?**
  - Spesso alcune persone portano come giustificazione al fatto che su GNU/Linux manchino quasi completamente i virus, i diversi “numeri” che Linux fa registrare rispetto ai sistemi operativi di casa Microsoft.
  - In parole povere, visto che Windows è molto più diffuso, è molto più facile che qualcuno scriva un virus per Windows che non per Linux.
  - Siamo davvero sicuri che sia così? Mica troppo...
  - GNU/Linux sta prendendo negli anni sempre più piede, soprattutto lato server. A quale pirata informatico non farebbe gola il fatto di poter prendere il controllo tramite un worm di una gran quantità di server, tramite i quali poter poi veicolare ulteriori contaminazioni o attacchi?
  - E' una spiegazione che NON REGGE il confronto con la realtà.

# Perchè non colpiscono GNU?

---

- Questione di qualità?
  - Un'altra cosa che viene solitamente portata come “spiegazione” di questo strano ed oscuro fenomeno, è la supposta miglior qualità del software libero rispetto al software proprietario.
  - Si tratta di un falso mito
  - Il software libero non è intrinsecamente migliore del software proprietario, almeno non dal punto di vista prettamente tecnico
  - Esistono infatti software liberi di scarsissima qualità (WuFTPd, un buco con il server intorno?) e software proprietario di qualità decente

# Perchè non colpiscono GNU?

---

- Questione di architettura?
  - E' però interessante notare come in realtà i virus non colpiscano non solo GNU/Linux, ma anche tutti gli altri sistemi operativi che offrono una distinzione reale (non fasulla) tra i privilegi accordati agli utenti: MacOS X, Solaris, \*BSD... Si tratta allora di questo?
  - Un applicativo, anche con bug seri di sicurezza, può portare all'inserimento di un virus nel sistema. Ma se poi questi non è in grado di replicarsi come si deve sul sistema in modo da riprodursi adeguatamente, come può funzionare?
  - In realtà anche questo spiega la situazione solo in parte: esistono su Windows dei virus che non si installano sul sistema in modo da riavviarsi al riavvio successivo, ma che banalmente si inviano a tutti i contatti. Il client di posta lo può usare anche un utente non privilegiato...

# Perchè non colpiscono GNU?

---

- Questione di tempi di risposta!!
  - Il mio modesto parere è che si tratti essenzialmente dei tempi di risposta che la comunità OpenSource, forte dei suoi 10.000 occhi, è in grado di offrire.
  - Per costruire un virus degno di questo nome, che si propaghi in rete, bisogna sfruttare una falla diffusa.
  - Le falle diffuse stanno negli applicativi più utilizzati, non in quelli di secondo piano
  - I tempi di correzione dei bug per quanto riguarda gli applicativi di punta del software libero, sono ridicoli se paragonati a quelli di casa Microsoft.
  - Attendere 7 anni prima di “fixare” un bug critico che consente l'esecuzione da remoto di codice arbitrario, non è certo il modo migliore di evitare i virus...

# Perchè non colpiscono GNU?

---

- Probabilmente in realtà si tratta di una concomitanza di alcuni fattori che abbiamo citato.
- Questo non cambia la sostanza: in questo momento i virus, su GNU/Linux, non costituiscono un problema serio
- Stiamo tranquilli allora?
- Sicuramente siamo più tranquilli degli utenti MS. I sistemi Microsoft Windows sono talmente vulnerabili agli attacchi di virus e worms, che la stessa Sophos (azienda che si definisce “leader” nella protezione dai malware) ha banalmente consigliato di “cambiare sistema operativo” nel suo “Rapporto sulla sicurezza” del 11 luglio 2006.
- Non dobbiamo però abbassare la guardia

# Cose da fare

---

- Il primo modo per non abbassare la guardia, è quello di tenere bene a mente una serie di regolette basilari che ci risparmiano un sacco di problemi:
  - Usate la differenziazione degli utenti!
    - Non è una feature dedicata ai soli utenti inesperti: utilizzare il sistema come utente privilegiato costituisce di per se un possibile problema, anche quando “sapete quel che fate”
  - Niente programmi strani scaricati ed installati sul sistema senza prima averli prima verificati
    - Cercare su Google informazioni e pareri riguardo al software che volete scaricare ed installare, è un ottimo modo per identificare malware, ma anche per trovare alternative...
  - Niente siti web strani o sospetti
    - *www.casalingheannoiate.com* è da considerarsi sospetto, tanto quanto *www.oroscopi-gratis.it*

# Cose da fare

---

- Niente click a caso su finestre che appaiono e non si capisce cosa c'è scritto
  - Spesso capita che si aprano popup curiosi, che fanno domande apparentemente incomprensibili. Se non sapete cosa cliccare, chiudete la finestra, ma prima, LEGGETE!
- In parole povere, “Fidarsi è bene, non fidarsi è meglio”
  - E' una regola di massima che vale per la vita normale, non vedo perchè non dovrebbe valere anche sul web.
- Utilizzare il meno possibile software standard
  - Più “strano” è il software che usate, meno probabile è che qualcuno abbia scritto un malware in grado di sfruttarne le vulnerabilità. (Sì, Linux è da considerarsi “strano”)

# Cose da sapere

---

- Una delle cose piu importanti “da fare” è documentarsi.
- Una discreta padronanza dell'argomento “virus ed anti-virus” ci mette al riparo da una serie di errori e soprattutto ci garantisce di non essere colti impreparati nel momento in cui i virus facessero capolino anche nel mondo di GNU/Linux
- Per prima cosa, riflettiamo sulle funzioni di un software antivirus:
  - E' opinione comune che la principale funzione di un software antivirus sia quella di pulire il sistema dai malware presenti ed evitare che di nuovi possano infettarlo.
- In se non è sbagliato, ma non coglie il punto chiave della vicenda...

# Cose da sapere

---

- La cosa più importante (e più difficile) che si chiede ad un antivirus, è quella di DISCERNERE i files infetti dai files puliti, distinguere cioè se un file è stato attaccato da un malware ed eventualmente ripulirlo dell'ospite indesiderato.
- Sembra una banalità, ma non lo è, ed andremo a vedere quali sono le principali problematiche che si pongono quando si prova a sviluppare un software anti-virus.
- La complessità dei software anti-virus è andata aumentando esponenzialmente nel corso degli ultimi 5 anni, conseguentemente al miglioramento delle procedure di ricerca ed analisi, e in contrasto alla sempre maggiore astuzia con cui i virus-writer ideano soluzioni per sfuggire loro.

# Cose da sapere

---

- 10 anni fa, l'ambiente in cui si trovava ad operare un software antivirus era quello dei floppy-disk, assenza di connessione in rete.
- Come funzionavano gli anti-virus dei “tempi antichi”?
  - In un primo momento, cercavano banalmente una così detta “search string”, una stringa caratteristica che identificava il virus stesso.

# Cose da sapere

---

- 10 anni fa, l'ambiente in cui si trovava ad operare un software antivirus era quello dei floppy-disk, assenza di connessione in rete.
- Come funzionavano gli anti-virus dei “tempi antichi”?
  - In un primo momento, cercavano banalmente una così detta “search string”, una stringa caratteristica che identificava il virus stesso.

1010101010101010101010101

# Cose da sapere

---

- 10 anni fa, l'ambiente in cui si trovava ad operare un software antivirus era quello dei floppy-disk, assenza di connessione in rete.
- Come funzionavano gli anti-virus dei “tempi antichi”?
  - In un primo momento, cercavano banalmente una così detta “search string”, una stringa caratteristica che identificava il virus stesso.

1010101010101010101010101

```
10010010010010101001001
01010010110101001010001
10101101010100001010101
10101010101010101010101
10101010010110110101010
10101101010100100101010
10110100100100101010110
01001001001001010011010
01001000010010101010101
10100100100010101010101
```

# Cose da sapere

- 10 anni fa, l'ambiente in cui si trovava ad operare un software antivirus era quello dei floppy-disk, assenza di connessione in rete.
- Come funzionavano gli anti-virus dei “tempi antichi”?
  - In un primo momento, cercavano banalmente una così detta “search string”, una stringa caratteristica che identificava il virus stesso.

```
10010010010010101001001
01010010110101001010001
10101101010100001010101
10101010101010101010101
10101010010110110101010
10101101010100100101010
10110100100100101010110
01001001001001010011010
01001000010010101010101
10100100100010101010101
```

# Cose da sapere

---

- 10 anni fa, l'ambiente in cui si trovava ad operare un software antivirus era quello dei floppy-disk, assenza di connessione in rete.
- Come funzionavano gli anti-virus dei “tempi antichi”?
  - In un primo momento, cercavano banalmente una così detta “search string”, una stringa caratteristica che identificava il virus stesso.
  - In realtà, il virus si copiava solo nella zona di inizio esecuzione del file e quindi si poteva tralasciare la scansione di tutto il file, concentrandosi sull'entry point.
  - Inoltre la ricerca poteva essere limitata ad una ristretta serie di files: eseguibili, script BAT, MBR e poco più.
  - Il ridotto numero di virus inoltre, consentiva l'applicazione di questo modello di ricerca.

# Cose da sapere

---

- Poi, un giorno, apparirono i virus cifrati e polimorfici
- Questi malware si caratterizzano, dal punto di vista di un antivirus, perchè la loro “search string” è estremamente piccola (spesso la sola routine di decifratura) e talvolta espressamente pensata per vederla contenuta anche in applicativi legittimi (header del compilatore?)
- Il meccanismo della “search string” (ricerca per firme) viene messo radicalmente in crisi. E' necessario fare un passo tecnologico in avanti. Per individuare i virus cifrati vengono sviluppate due diverse tecnologie:
  - X-Raying
  - Emulazione

# Cose da sapere

---

- La tecnica dell'X-Raying è estremamente semplice:
  - Conoscendo il testo in chiaro (la search string) si tenta di decifrare “a forza bruta” (per tentativi) il codice del virus.
  - Si tratta di un processo molto lento, e non sempre da i frutti sperati (se il virus fosse ANCHE polimorfico?)
- La tecnica dell'emulazione invece risulta piu efficace:
  - Si esegue un'esecuzione “controllata” del file (eseguita via software dall'antivirus invece che dal processore vero e proprio, quindi sicura ma estremamente piu lenta) e si verifica se questo si comporta come il virus che stiamo ricercando.
- Per individuare invece i virus polimorfici, si esegue un'analisi statistica delle istruzioni: essendo il set delle istruzioni a loro disposizione piuttosto limitato (deve stare nel codice stesso), si distinguono facilmente.

# Cose da sapere

---

- Emersero poi i virus che tentavano di “offuscare il punto d'esecuzione”, inserendosi all'interno di eseguibili lontano dal punto d'inizio d'esecuzione
- Fortunatamente questi virus sono particolarmente difficili da scrivere, poco affidabili (spesso non funzionano come dovrebbero) e quindi poco diffusi.
- Non rappresentano un vero problema per i software antivirus, e su di essi si possono effettuare scansioni “on-demand” piu particolareggiate.
- Siamo ancora lontani dai tempi moderni. Nessuno poteva ad ogni modo prevedere che di li a poco, il numero di virus esistenti al mondo, sarebbe letteralmente esploso.

# Cose da sapere

---

- Con l'aumento vertiginoso del numero di virus, il problema maggiore che gli sviluppatori di software AV dovettero porsi, era quello dell'ottimizzazione delle performance dello scanner.
- Uno scanner antivirus lento infatti, può essere equiparato ad uno che non trova i virus. Se per fare la scansione giornaliera ci metto 26 ore, come posso usarlo? Nel frattempo, l'infezione non si è forse propagata?
- Inoltre i virus cominciano a non essere più scritti in ASM, ma in linguaggi di “alto” livello, come il C, che per effetto della compilazione, tendono ad avere maggiori somiglianze con gli applicativi legittimi (le sequenze di bytes dei compilatori sono piuttosto ben definite)

# Cose da sapere

---

- La soluzione fu l'abbandono del semplice meccanismo di ricerca di una stringa all'interno del codice eseguibile, ed il suo spostamento in zone più caratteristiche (tabelle di rilocalizzazione, stringhe di testo...)
- Inoltre, spesso e volentieri, si passò all'uso di checksums invece di intere stringhe
  - Un checksum è una specie di “riassunto univoco” in 32 bit di una stringa/testo
  - Le motivazioni sono molto semplici: una search string funzionante deve essere lunga almeno 8-12 lettere (8-12 bytes) mentre un checksum non ne occupa più di 4.
  - Si aggrava il problema della velocità degli scanner, perché fare un checksum di una stringa è piuttosto dispendioso, computazionalmente parlando.

# Cose da sapere

---

- Si introdussero allora dei controlli aggiuntivi sui files da analizzare, in modo da scartare una serie di files prima ancora di iniziare a fare il checksum (o l'esecuzione controllata che sia).
- Ad esempio il tipo di file può essere una valida informazione. Sapendo che un certo virus colpisce i soli file eseguibili (COM, EXE...) che senso ha cercare il checksum anche nei files di testo o nelle immagini?
- Inoltre si può inserire anche un controllo su una breve “search string” che deve assolutamente esserci (i frequenti falsi positivi vengono poi scartati dalla ricerca del checksum)
- L'uso di checksum portò anche un vantaggio collaterale: la possibilità di scovare i Trojan (4:1 su virus e worms)

# Cose da sapere

---

- Potevano le cose fermarsi qui? Eh no!
- Ecco che i malware cominciarono ad andarsi a infilare in altre tipologie di files: CAB, ZIP e altri archivi piu o meno compressi.
- Per trovare questi virus, il motore dell'AV deve poterli almeno leggere, complicandosi notevolmente
- Ad aumentare ancora una volta la complessità dei motori degli anti-virus, ci si misero gli worm, malware che non hanno bisogno di copiarsi in files, perchè modificano il sistema operativo stesso al fine di duplicarsi e di assicurarsi la riesecuzione all'avvio successivo, ed i virus che vivono all'interno del corpo delle email, e si propagano spedendosi come posta elettronica.

# Cose da sapere

---

- Continuiamo a parlare di “aumento della complessità del software antivirus”, ma come si è affrontato questo problema?
- Com'è strutturato al suo interno, un software antivirus?

# Cose da sapere

---

- Continuiamo a parlare di “aumento della complessità del software antivirus”, ma come si è affrontato questo problema?
- Com'è strutturato al suo interno, un software antivirus?
- Un software antivirus si compone di 2 parti:
  - Motore
    - Colui che esegue la scansione
  - Database
    - Colui che contiene le “definizioni dei virus”
- Ma è davvero così? Sempre più spesso, il punto dove finisce il motore ed inizia il database è davvero labile e difficilmente identificabile.

# Cose da sapere

---

- Possiamo dire, generalisticamente parlando, che il motore si aggiorna meno frequentemente rispetto al database, ma davvero poco di più.
- Per una questione di flessibilità infatti, sempre più spesso il database contiene codice eseguibile, parte integrante del processo di scansione.
  - A volte, addirittura, il “motore” non fa altro che “caricare” il database ed eseguirne il contenuto. Questo porta però a problemi di stabilità.
  - Viceversa, un motore molto “importante”, limita le potenzialità dell'AV a quanto disponibile al suo interno, finché non viene aggiornato)
- Il miglior compromesso lo si ottiene quando il database contiene un qualche linguaggio di “scripting” o “meta-eseguibile”, ed il motore non fa altro che interpretarlo

# Cose da sapere

---

- Si pone poi il problema delle “nuove” minacce, quelle che non sono ancora state identificate e per le quali quindi non sono ancora disponibili delle “definizioni”
- Si possono fermare queste minacce tramite un software antivirus?
- La risposta è “si”, usando un metodo “a punteggi” (simile ai software antispam) noto come “scansione euristica”
- E' normale un software che cerca di copiare se stesso in coda a tutti gli eseguibili, o cerca di auto-spedirsi tramite posta elettronica? No. Questo ci consente di riconoscerlo!
- Tramite esecuzione controllata (o search string, ma...), si può attribuire un punteggio ad ogni operazione richiesta. Passato un certo punteggio, il software è catalogato come pericoloso.

# Cose da sapere

---

- La ricerca inoltre, ha razionalizzato alcune interessanti esperienze, che potrebbero consentirci, in un futuro prossimo, di bloccare sul nascere le epidemie virali.
- Si tratta della modellizzazione dei meccanismi di propagazione.
- Uno studio condotto soprattutto sui malware di maggior “successo” (soprattutto worm) ha analizzato il traffico da loro generato, giungendo a catalogarne con notevole accuratezza le caratteristiche peculiari.
- Implementando dei meccanismi di “isolamento” delle reti che improvvisamente producono un traffico simile a quello del modello dell'infezione virale, si potrebbe limitare l'infezione ad una ristretta area facilmente “ripulibile”. Ci sono però da valutare i “contro”...

# Altro da tenere d'occhio

---

- La difesa dai malware in se per se, non garantisce la sicurezza del proprio sistema.
- Una serie di altre pratiche e accorgimenti, sono comunque da mettere in pratica per difendersi dalle minacce di tipo informatico:
  - Tenete il sistema operativo aggiornato!
    - Visto che vengono continuamente individuate e corrette vulnerabilità nel software, è utile che aggiorniate il software di frequente, di modo da sfruttarne la messa in sicurezza.
  - Attenti ai formati dei files!
    - Le estensioni possono ingannare l'utente sul reale formato di un file, mentre il sistema si lascia infettare senza troppi scrupoli. Evitare di aprire files sospetti con un doppio click, ma utilizzare il menu “File->Apri” dell'applicazione che dovrebbe visualizzarlo, può evitare parte dei problemi.

# Altro da tenere d'occhio

---

- Utilizzare, dove possibile, la crittografia
  - L'introduzione di SSL ha consentito ad una lunga serie di protocolli molto usati (SMTP, HTTP, POP, FTP, ...) di introdurre meccanismi di crittografia per verificare autenticità e riservatezza delle comunicazioni.
  
- Documentatevi, quando avete dubbi
  - Nelle prossime pagine, cercherò di darvi qualche informazione curiosa ed utile per capire molti dei problemi legati alla sicurezza informatica, che sono la maggior parte delle volte causati dalla mancanza di informazioni.
  - Ma l'informatica è una materia in continua e rapidissima espansione. Cose che oggi sono considerate “la frontiera”, domani saranno alla portata di tutti. Se non ve ne interesserete, vi esporrete ad attacchi e truffe.
  - Viviamo nella società dell'informazione.

# Altro da tenere d'occhio

---

- Email
  - Il mittente di una mail non è verificato. Creare una mail con mittente falsificato è di una semplicità disarmante, basta modificare le impostazioni del client di posta! Non fidatevi!
  - Per ovviare a questo problema, si può utilizzare la firma digitale e la crittografia messe a disposizione, ad esempio, da GNUPG, l'implementazione di PGP rilasciata sotto GPL.
  - Difficilmente banche e siti istituzionali vi chiedono di cambiare la vostra password tramite una pagina web! Spesso invece, mail che lo richiedono sono tentativi di truffa, che riproducono fedelmente la home page del sito in questione per indurvi ad inserirvi le vostre credenziali d'accesso.
  - Non inviate (e rifiutate) le email in formato HTML. L'utilizzo di HTML per formattare l'aspetto delle email, introduce una notevole quantità di vulnerabilità, senza introdurre alcun reale vantaggio. Usate il testo semplice, va benissimo ed è molto più sicuro.

# Altro da tenere d'occhio

---

- I vostri dati
  - Fare i backup non è solo una perdita di tempo.
  - Oltre che un ottimo modo per archiviare dati che al momento non vi servono ma potrebbero servire più tardi (non si sa mai), è l'ultima barriera quando qualcosa va storto altrove.
  - Quindi backup con cadenza commisurata al valore dei dati:
    - Più frequenti per i dati della /home
    - Meno frequenti (ma non inesistenti) per il resto del sistema
  - Spesso anche una semplice chiavetta USB può andare bene, fare un backup a settimana può essere sufficiente, magari riutilizzando i dispositivi contenenti backup superati i cui documenti sono disponibili su altri supporti.
  - [edit]: verificate i backup, una volta fatti. Sigh!

# Altro da tenere d'occhio

---

- Il web
  - Guardate prima di cliccare! Quando vi viene proposta l'apertura di una pagina web tramite un link, guardate dove punta realmente l'URL:
    - **HTML:** `<a href="http://www.sito-ladro.it">Polizia.it</a>`
    - **VEDI:** [Polizia.it](http://www.polizia.it)
    - Nella barra di stato, quando portate il cursore del mouse su un link, visualizzate il reale contenuto (il campo href) del link. Se appare qualcosa di diverso da quello che vi aspettate, non cliccate!
  - Siete davvero dove pensate di essere? Verificate l'URL una volta aperta la pagina, esistono le redirezioni!

# Altro da tenere d'occhio

---

- La sicurezza non è un dato di fatto, o una condizione, ma un compromesso, con l'usabilità.
- Più il livello di sicurezza si innalza, più difficile è trovare qualcuno in grado di violarla, ma la sicurezza assoluta non esiste e non può esistere.
- Tecniche come il “social engineering” (alla base di fenomeni recenti come il phishing via email o via web) fanno leva sul fatto che l'utente è comunque l'anello più debole del sistema.
- Attenzione, vigilanza, password sufficientemente complesse, password d'accesso al pc, un pizzico di paranoia.
- E informazione seria, non mass media.