Linux/Unix: i Sistemi Operativi non vulnerabili al classico concetto di "virus"

Marco Pratesi
pratesi@telug.it

Indice

1 Che cos'è un virus? Come Agisce?

1.1 Introduzione

Ciascuno di noi conosce almeno a livello elementare il concetto di "virus", se non in ambito informatico, almeno per il suo significato biologico. Potremmo dire che un virus è qualcosa che cerca di usare il nostro corpo e le sue risorse per aumentare la propria vitalità e riprodursi a spese della nostra salute e per infettare altri nostri simili.
In pratica, è qualcosa che, dal nostro punto di vista, usa in maniera impropria, indesiderata e dannosa il nostro corpo. Sottolineo il "dal nostro punto di vista": dal suo punto di vista, un virus fa esattamente ciò che le leggi biologiche gli dettano. E qui la prima precisazione... anche altri organismi vivono e si riproducono nel nostro corpo: ad esempio, gli enzimi. Un enzima, così come un virus, fa ciò che le leggi biologiche gli dettano; la differenza fondamentale sta nel fatto che, dal nostro punto di vista, un enzima fa qualcosa di desiderabile e non qualcosa di dannoso.

Proviamo ora a fare un parallelo informatico di ciò che è stato detto. Secondo l'esperienza comune, un virus è riconducibile a un pezzo di codice eseguibile in grado di generare copie di se stesso (cioè di riprodursi) e di introdursi in file di dati e nel codice di altri programmi (cioè di infettare), provocando così effetti indesiderati, che vanno da semplici disturbi a conseguenze ben più gravi [1], [2], [3].
Come vedremo nel seguito, questa definizione di virus è piuttosto elementare e non fa distinzioni che nel seguito si dimostreranno opportune e necessarie per una chiara comprensione dell'argomento e per l'individuazione di utili contromisure.

A questo punto, ipotizziamo per semplicità che un virus sia semplicemente un programma eseguibile; la sua esecuzione può essere avviata sia intenzionalmente che automaticamente e senza che l'utente lo desideri e ne sia completamente cosciente, ad esempio mediante un programma di posta elettronica configurato in maniera tale da "eseguire/aprire automaticamente" gli allegati.
Nel seguito si prescinderà da tale distinzione, dato che si cercherà di focalizzare l'attenzione sulle relazioni tra il concetto di virus e il S.O. sottostante, relazioni che prescindono da eventuali automatismi di qualunque programma applicativo possa avviare l'esecuzione di un virus.
Quindi la prima domanda "provocatoria". Se ci si pone il problema di capire se un S.O. è vulnerabile o no al concetto di virus, è logico classificare come "virus" - senza ulteriori precisazioni - ogni eseguibile che provochi effetti indesiderati per l'utente che - più o meno volontariamente - ne avvia l'esecuzione? Se vogliamo rispondere "si", allora dobbiamo osservare che anche l'esecuzione di un file manager, di un editor, magari di un applicativo malfunzionante, può provocare effetti indesiderati per l'utente... Esempio: un file manager permette all'utente di rimuovere dei file per errore. Come evitare/ridurre tale rischio? Per esempio, prevedendo una richiesta di conferma per la rimozione dei file, ma è davvero una soluzione? Il file manager che io uso, di default, si comporta proprio così; risultato: mi sono abituato a confermare sempre, senza pensarci, cosicché il rischio è praticamente invariato. Per eliminare davvero il rischio di rimozione errata si può fare una

sola cosa: interdirmi la rimozione... ma credo che concorderete che sarebbe una soluzione eccessiva, che limiterebbe in maniera pesante le funzionalità a disposizione dell'utente. Analogamente, se si vuole evitare che io possa per errore eseguire un virus, il rimedio ultimo e definitivo è uno solo: impedirmi di eseguire alcunché... ma a quel punto non potrei eseguire più nulla.

Insomma, è piuttosto facile convincersi che nessun S.O. potrà mai impedire all'utente di autodanneggiarsi eseguendo un virus, dato che, in fin dei conti, un virus agisce eseguendo, leggendo, scrivendo... insomma, compiendo le stesse azioni elementari di cui un utente ha bisogno per lavorare. Quindi un tale ipotetico S.O. sarebbe semplicemente inutile... oppure dovrebbe sostituirsi all'intelligenza e al discernimento umano... e mi auguro che non esisterà mai nessun software che cerchi di sostituire la volontà e l'intelligenza umana, neanche nel distinguere tra "virus" ed "enzimi".

Ma allora... non c'è speranza? I virus esistono e basta? Si può solo sperare che "non cadano tegole"?
Beh, non direi... proseguiamo il discorso.

1.2 Virus "per il sistema operativo" o "per l'utente"?

Ed eccoci alla prima distinzione. Consideriamo un "virus", per meglio dire, un eseguibile che provoca un effetto non desiderato dall'utente. Che tipo di effetto indesiderato? Danneggiamento dei file dell'utente e/o danneggiamento dell'ambiente di lavoro, costituito dal S.O. e dagli applicativi installati sul sistema? Come abbiamo già visto, è inutile sognare un S.O. che possa evitare il primo tipo di danneggiamento. Quindi concentriamoci sul secondo caso.
Anche se per un utente un danneggiamento dei propri file è cosa senz'altro negativa, il danneggiamento del S.O. ha un impatto ancora maggiore, perché inficia la funzionalità dello strumento di lavoro, anche per altri utenti, e può richiedere, oltre al solito backup (da fare anche per proteggersi contro il primo caso), magari anche la riparazione/reinstallazione del S.O. Quindi chiediamoci: può esistere un S.O. che sia in grado di autodifendersi dal concetto di "virus", cioè capace di non lasciarsi danneggiare dall'esecuzione di un virus da parte di un utente? La risposta è banalmente "si"; ad esempio, è sufficiente che il S.O. sia in qualche modo in grado di distinguere i propri file tra tutti quelli che gestisce e che non accetti da un utente normale una richiesta di modifica di uno di tali file.

1.3 È possibile difendersi? Ruolo del S.O.

Immaginiamo un eseguibile che cerchi di rimuovere un importante file di sistema, ad esempio un file indispensabile per l'avvio del sistema operativo. L'esperienza ci dice che, ad esempio, su Windows 98, tale eseguibile riesce senza problemi ad ottenere tale rimozione. Del pari, su Linux, se un generico utente prova ad eseguire un simile virus, non provoca danni, semplicemente perché i suoi diritti non sono sufficienti per rimuovere un file di sistema. In pratica, mentre Windows 98 non fa distinzioni e non è in grado di difendersi, Linux (più in generale, Unix), pur senza riconoscere se un file è "di sistema"

oppure no, decide se effettuare la rimozione in questione sulla base di un confronto tra i diritti necessari per eseguirla e i diritti di chi la richiede.
Quindi: ci si può difendere da danneggiamenti al S.O. ad opera di virus, se si usa un S.O. in grado di autodifendersi.

1.4 Scelta di una definizione di "virus"

Sulla base delle pur elementari considerazioni fatte fin qui, nel seguito si focalizza l'attenzione solo sui virus che cercano di danneggiare il S.O.

2 Virus e problemi di sicurezza

2.1 Introduzione

E qui affrontiamo una delle questioni più sottili di tutta la presente discussione.
Ipotizziamo che un generico utente Linux provi a lanciare l'eseguibile già menzionato, che chiede la rimozione di un file di sistema. Poiché l'utente non ha diritti sufficienti, la rimozione non viene eseguita dal S.O. Immaginiamo che a questo punto l'utente, sfruttando una debolezza dell'implementazione del S.O., riesca ad acquisire diritti maggiori; ad esempio, su Red Hat Linux 6.0, se il pacchetto `usermode` non veniva aggiornato con una correzione ufficiale, per un utente normale era possibile sfruttare un "exploit" noto per acquisire i massimi privilegi, cioè quelli di amministratore di sistema. E immaginiamo che, a questo punto, l'utente diventato "`root`" provi nuovamente a lanciare l'eseguibile già menzionato. A questo punto la rimozione richiesta viene eseguita.
Domanda: i passi effettuati dall'utente per acquisire diritti maggiori e l'eseguibile in questione, messi insieme, costituiscono un virus? Preciso che questo è il tipo di equivoco su cui vari detrattori di Linux/Unix e/o sostenitori di Microsoft hanno fatto leva per affermare che "finalmente esistono virus anche per Linux, finora non ne erano stati scritti solo perché nessuno se n'era curato".
Alla domanda posta è più che ragionevole rispondere "no". Infatti va precisato che la rimozione del file è stata eseguita solo perché l'utente è riuscito ad acquisire diritti maggiori di quelli che gli competono, sfruttando un'errata implementazione del sistema. Più chiaramente: l'architettura di un S.O. Unix senz'altro prevede che un utente normale possa acquisire i diritti di amministratore solo passando per un'opportuna procedura di autenticazione, durante la quale deve fornire la corrispondente password. L'utente in questione è riuscito ad acquisire tali diritti senza la corrispondente autenticazione solo perché ha sfruttato un errore di implementazione di un determinato pacchetto software. La soluzione di un problema di questo tipo richiede semplicemente la correzione dell'errore di implementazione e non richiede una rivisitazione del S.O. per ciò che riguarda l'architettura e la gestione dei permessi e dei diritti d'accesso. Inoltre, la soluzione di tale problema non danneggia il corretto funzionamento degli altri programmi installati sul sistema. Il tutto viene classificato come problema di sicurezza, corrispondendo ad

una non aderenza dell'implementazione alle specifiche di partenza. Queste considerazioni riguardano Linux/Unix... sono valide per qualunque sistema operativo?

2.2 Scelte architetturali, errori di implementazione

Come abbiamo appena visto, l'eventuale successo nella rimozione menzionata da parte dell'utente su un S.O. di tipo Unix sarebbe dovuto a un errore di implementazione e quindi a una non aderenza alle specifiche sui diritti di accesso. Quindi su Unix tale problema rientra nell'ambito dei problemi di sicurezza e come problema di sicurezza viene affrontato e risolto.

Invece ora supponiamo di tentare lo stesso tipo di rimozione su Windows 98; tale rimozione viene effettuata con successo in ogni caso, chiunque sia la persona che sta utilizzando il computer e, volontariamente o meno, la richiede. Tutto ciò è dovuto a un errore di implementazione? Tale rimozione ha successo perché, proprio per scelta architetturale, su Windows chiunque ha diritto di rimuovere qualunque file. Quindi su Windows il tutto non può essere considerato e affrontato come problema di sicurezza; va semplicemente considerato un problema di scelte architetturali, cosicché, a meno che non si voglia ristrutturare l'intero sistema a partire dalle sue specifiche, tale problema resta ineliminabile.

Se ne può facilmente dedurre che un virus che cerchi di danneggiare il S.O. è qualcosa che può esistere (ed esiste) per Windows e che invece non esiste per Unix. Ripeto, su Unix un tale virus può solo cercare di sfruttare un problema di sicurezza (o un amministratore di sistema particolarmente stupido... :) e allora si rientra nell'ambito degli attacchi alla sicurezza del sistema e si fa riferimento a una categoria di esperti informatici piuttosto diversa da quella dei "virus writer", cioè quella degli esperti delle problematiche di sicurezza.

2.3 Multiutenza come difesa?

Leggendo il paragrafo precedente, si intuisce qual è la differenza di base che rende Unix invulnerabile liddove Windows non ha difese: il concetto di multiutenza, più precisamente, la netta distinzione tra la "modalità utente" e la "modalità amministrativa" e i rispettivi diritti di accesso.
Windows 98 offre anche qualche strumento di gestione di diritti di accesso ai file e all'esecuzione di determinati applicativi e una qualche forma di multiutenza. Tuttavia non si tratta di una vera e propria multiutenza, ma di "regole" che un determinato utente imposta e che il sistema e gli applicativi sono pronti a rispettare... inutile dire che un virus certamente non si preoccupa di rispettare tali regole e può anche tranquillamente modificare gli attributi impostabili da MS-DOS (come la non rimovibilità)...
A questo punto si potrebbe obiettare che Windows NT offre una gestione della multiutenza e dei permessi di accesso in buona misura analoga a quella tradizionale di Unix, quindi l'utilizzo di Windows NT anziché 9x/ME dovrebbe risolvere il problema e annullare tale "distanza" tra Unix e Windows. Beh... cosa dire? Almeno in linea di principio, Windows

NT offre una gestione di utenti e permessi perfino leggermente più versatile rispetto a Unix. Tuttavia, Windows NT presenta importanti debolezze strutturali in confronto alla rigorosa architettura del "grande vecchio" Unix. Ad esempio, di default le proprietà e i diritti di accesso dei file e delle directory di sistema lasciano molte maglie aperte agli utenti normali (quelli che su Windows 2000 sono chiamati "utenti standard"), che possono perfino scrivere nelle directory di sistema, come \, `\winnt\`, `\winnt\system32` . In una situazione del genere risulta ben poco immediato identificare le parti di File System in cui un generico utente agisce e quindi diventa difficile anche limitare lo spazio occupato su disco da un generico utente, cosicché è concreto anche il rischio che un qualunque utente blocchi il sistema riempiendo il disco per aver contratto un qualunque virus. Si potrebbe obiettare che basterebbe "richiudere tali maglie", cioè ricalibrare opportunamente - alla Unix - proprietà e diritti di accesso. Beh... anche volendo prescindere da una valutazione dei tempi di lavoro aggiuntivi legati a tale ricalibrazione e dal rischio di commettere errori nell'effettuarla, bisogna notare che applicativi di uso comune (anche applicativi prodotti dalla stessa Microsoft), per il loro "corretto" funzionamento, hanno bisogno dei permessi laschi offerti di default da Windows NT. Quindi la soluzione del problema comporterebbe una rivisitazione delle scelte architetturali e un insieme di interventi che danneggerebbero il funzionamento di software già installati sul sistema... difendiamo il sistema o lo facciamo funzionare? :)
Inoltre, Windows NT non offre una buona protezione della memoria, quindi un utente normale, oltre a poter tranquillamente scrivere in directory di sistema, può lanciare in esecuzione dei thread che leggono e scrivono su memoria condivisa [3], [4], [5]. Faccio notare esplicitamente che su Unix a ciascun processo in esecuzione è associato l'utente che lo sta eseguendo, come si può facilmente leggere nella colonna "`USER`" dell'output generato (su Linux) dal comando "`ps aux`". Al contrario, come si può immediatamente notare lanciando il Task Manager, non sembra valere una considerazione analoga per Windows 2000...
Queste considerazioni dipingono un quadro in cui architetturalmente Windows NT, al contrario di Unix, offre un modello non molto robusto di protezione del S.O. dalle azioni degli utenti... si può facilmente intuire che, per chi è abituato al rigore dei sistemi Unix, è perlomeno inquietante (o divertente... :) sapere che un utente standard può scrivere anche nelle directory di sistema e che l'amministratore di sistema non rileva l'identità (USER) con cui è in esecuzione un generico processo. Tali vulnerabilità non dipendono dai tanti bachi di Windows NT (dei quali più di 65000 sono stati ufficialmente riconosciuti e ammessi da Microsoft nel rilasciare Windows 2000, cioè NT5... chissà quanti altri ce ne sono...): resterebbero invariate anche una volta corretti tutti gli errori di implementazione.

2.4 Definizione operativa di una distinzione tra "virus" e "problema di sicurezza"

A questo punto ci chiediamo nuovamente quando usare il termine "virus", cercando di fare distinzioni dove possibile. Lo si potrebbe usare per qualunque cosa sia in grado di danneggiare il S.O., ma questo non aiuterebbe la comprensione delle cose. Una ragionevole

definizione operativa potrebbe essere la seguente: un determinato caso di danneggiabilità del S.O. viene classificato come "problema di sicurezza" (e non "virus") quando la soluzione di un problema di sicurezza permette di risolvere il caso. Diversamente, nel presente contesto, per semplicità, possiamo decidere di etichettare il tutto come "virus" senza fare ulteriori distinzioni. Tale definizione operativa, oltre ad essere secondo me ragionevole da un punto di vista teorico, è senz'altro aderente alla realtà pratica e vissuta. Infatti, quando la correzione di un problema di sicurezza rende invulnerabile il S.O. a un "eseguibile maligno" che si appoggia a tale problema e non risulta necessario l'uso di nessun antivirus, state pur tranquilli che l'amministratore di sistema vede il tutto come "problema di sicurezza" e per tale eseguibile usa classicamente il termine "exploit" e non il termine "virus". Quando viceversa non è possibile difendersi risolvendo qualcosa che il produttore del S.O. classifica come "problema di sicurezza" e ci si trova di fronte a un problema architetturale, beh, l'amministratore di sistema si accorge di essere impotente e ha buoni motivi per usare il termine "virus".

2.5 Linux: i worm "Ramen" e "Adore"

Nel Gennaio 2001 è stata diffusa una "notizia bomba" destinata a sfatare il classico mito di invulnerabilità dei sistemi Unix ai virus (scusatemi se lo dico con evidente ironia...).

> "*Ramen: finalmente un virus per Linux; un virus con conseguenze devastanti; ecco, era solo questione di tempo e diffusione: finora nessuno si era curato di Linux, ma, ora che comincia a diffondersi, si vede come sia facile scrivere per esso dei virus estremamente maligni e dannosi e come Linux non sia affatto meglio di Windows, neanche sotto questo aspetto.*"

Quando ho letto questa "notizia bomba", mi sono limitato a ricordare le considerazioni teoriche che permettono di escludere la vulnerabilità di Unix ai virus e mi sono detto: "vediamo quali stupidaggini hanno scritto stavolta per attaccare Linux/Unix". E già dopo aver letto alcune righe ho capito che, ancora una volta, si stava cercando di attaccare Linux con l'arma del FUD (Fear, Uncertainty, Doubt), cioè sollevando polverone e confusione per poter fare di tutta l'erba un fascio.
Questo violentissimo "virus", come appare evidente dalla sua descrizione tecnica [6], non è altro che un programmino che esplora una rete per cercare macchine che usano Red Hat Linux 6.2 o 7.0 (tecnologicamente questo non ha nulla di nuovo, esistono innumerevoli programmi - anche con codice sorgente pubblicamente noto - che fanno cose di questo tipo) e attacca quelle che trova, utilizzando exploit noti che sfruttano problemi di sicurezza di vecchie versioni di alcuni pacchetti server. Una volta che l'attacco ha avuto successo, vengono fatti "scherzetti" come ad esempio la sostituzione della home page dei sistemi violati. Alla luce delle considerazioni già fatte, risulta piuttosto velleitario cercare di usare il termine "virus" per questo "Ramen" e per "Adore" [7], che agisce in maniera del tutto analoga. Il termine corretto classicamente usato in questi casi è "worm". Infatti, Ramen e Adore non fanno altro che appoggiarsi a problemi di sicurezza noti e muoversi sulla rete per automatizzare l'utilizzo di exploit noti degli stessi. Per chiamare "virus"

la "automatizzazione di un exploit" - secondo me - bisogna essere distratti e/o ignoranti e/o palesemente in malafede. Se si è distratti e/o ignoranti, bisognerebbe evitare di fare "informazione" (ma non sarà che invece si tratta di malafede bella e buona?).
Per completare la ridicolizzazione della "notizia bomba" in questione, si può aggiungere che il problema non richiede certamente un antivirus per essere risolto e che, ai tempi dell'annuncio, i problemi di sicurezza in questione erano noti e risolti già da molti mesi. Per dirlo più chiaramente: quando è stato annunciato Ramen, già da tempo la Red Hat Inc. aveva pubblicamente rilasciato i pacchetti di correzione che risolvevano il problema di sicurezza in questione. Tali pacchetti di correzione erano e sono tuttora reperibili su una ben nota pagina web linkata perfino sul desktop di Red Hat Linux; su tale pagina si trovano tutti i pacchetti di aggiornamento e correzione, che Red Hat Inc., come tutti i distributori Linux, rilascia con una tempestività che storicamente Microsoft non sembra in grado di eguagliare né di avvicinare... meraviglie del modello di sviluppo Open Source, cioè a codice aperto e pubblicamente noto...
Ultima precisazione: i worm Ramen e Adore non si appoggiano nemmeno a una lacuna del S.O. Linux in sé; si appoggiano a errori di implementazione di alcuni pacchetti server. Quindi non mettono minimamente in discussione Linux, l'organizzazione del S.O., la sua architettura e così via.
Insomma... che cosa dire di chi ha sollevato e alimentato il polverone?
"Non ti curar di lor, ma guarda e passa... a Linux" :)

3 È possibile difendersi? Come?

3.1 Unix/Linux

Tutto sommato non c'è molto da cui difendersi... Vale la raccomandazione classica (a prescindere dal problema "virus") di usare il sistema con l'identità di utente, ricorrendo all'identità di amministratore ("`root`") solo quando è realmente necessario. In particolare, è bene non accedere mai a Internet (navigazione compresa) con l'identità di `root`. Tale raccomandazione, oltre a rispondere al buon senso, non comporta un reale disagio, dato che Unix offre il comando "`su`", che permette di cambiare identità - e quindi, in particolare, di assumere l'identità di `root` fornendo la corrispondente password - in qualunque contesto, con interfaccia grafica o anche solo su terminale testuale. Inoltre, come su qualunque S.O., l'amministratore deve evitare di installare software di provenienza non chiara. Per il resto, per l'amministratore di sistema non c'è molto da temere: il S.O., se mantenuto aggiornato con le correzioni dei problemi di sicurezza, non può essere danneggiato dagli utenti.
Per ciò che riguarda l'utenza del sistema, gli utenti incauti possono far danni a se stessi ma non possono danneggiare né il S.O. né gli altri utenti (nessun utente può scrivere nella home directory di un altro utente, se non ha per questo una esplicita autorizzazione), quindi ciascun utente può dormire sonni tranquilli anche se un altro utente della stessa macchina è "un po' troppo disinvolto". L'utente deve solo evitare comportamenti troppo incauti, per non provocare danneggiamenti dei propri file.

3.2 Windows NT

È bene essere coscienti che non valgono i pregi elencati per Unix riguardo all'isolamento tra utente e S.O. e tra utente e utente e non si ha una buona protezione della memoria [3]. Se si può rinunciare a usare programmi che necessitano dei permessi laschi tipici di Windows NT, allora si può procedere a "blindare" file e directory di sistema, imitando Unix per le proprietà e i diritti di accesso. Se non si può rinunciare a usare tali programmi, è bene ricorrere ad antivirus aggiornandoli periodicamente e raccomandare agli utenti di non comportarsi in modo troppo pericoloso (e augurarsi che obbediscano...). Inoltre, come su Unix, è bene assumere l'identità di amministratore solo quando è realmente necessario. È da notare che su Windows NT non esiste un equivalente del comando "`su`" di Unix; non esistendo neanche la possibilità di aprire più sessioni o più desktop su console distinte (cosa tranquillamente disponibile su Linux...), un cambio di identità comporta la chiusura della sessione e la riapertura di un'altra sessione con un'altra identità. Per evitare tale disagio, spesso su NT si finisce per lavorare sempre con l'identità di amministratore e/o per dare al proprio utente i diritti di amministrazione... resta il fatto che non è affatto una sana abitudine, infatti è ciò in cui confida solitamente chiunque voglia scrivere un virus per Windows NT...

Riguardo al browsing: parlando di Unix, ho ricordato l'inopportunità di navigare da "`root`". Su Unix questo significa solo che è bene evitare di lanciare, ad esempio, Netscape, Mozilla, Galeon, Konqueror, ecc. da `root`.
Su NT5 (Windows 2000), Windows ed Explorer sono strettamente integrati, quindi appare praticamente impossibile agire da amministratore evitando di eseguire un browser con l'identità e i diritti, appunto, di amministratore... ovvio che tocca ignorare e violare quella che è una classica, antica e sana raccomandazione...
Ultima precisazione: i vantaggi derivanti dalla multiutenza di Windows NT e dalla sua gestione di proprietà e diritti di accesso su file e directory vengono in buona parte annullati se non si usa NTFS, cioè il file system nativo di NT. Se, come si fa spesso, Windows NT viene installato sulla "classica" FAT (o se almeno una delle partizioni usate dal sistema è formattata come FAT), molte delle caratteristiche specifiche di NT non sono più valide e si ricade in una situazione per molti versi analoga a quella di Windows 3.x, 9x, ME, considerata di seguito.

3.3 Windows 3.x, 9x, ME

Le versioni di Windows in questione non offrono una vera gestione della multiutenza e non permettono di imporre proprietà e diritti di accesso a file e directory. Quindi, da un punto di vista architetturale, semplicemente non c'è nessuna protezione. Per ridurre i rischi è bene fare ricorso ad antivirus, disabilitare gli automatismi che comportano esecuzioni all'insaputa dell'utente (di default Windows e vari applicativi Microsoft ne prevedono molti), evitare di far usare il computer a chi non è conscio dei pericoli, istruire opportunamente gli utenti, evitare di usare software di provenienza non chiara (quindi anche molti software pirata...) e, se si tratta del computer di casa, sperare che i propri

figli non facciano i "birichini", anche perché non sono disponibili funzionalità di logging sufficienti a ricostruire che cosa combinano...

4 Conclusioni

È stata presentata una panoramica (ben lungi dall'essere esaustiva) riguardante le relazioni tra virus e sistemi operativi, cercando di illustrare che cosa si intende per "virus", distinguendo i danni provocati in danni per l'utente e danni per il S.O.
È stata proposta una definizione operativa di un confine tra "virus" e "problema di sicurezza" e sono stati portati degli esempi a supporto di tale definizione.
Quindi sono state evidenziate le differenze in merito tra Unix e le varie versioni di Windows, evidenziando i punti di forza di Unix e le debolezze di Windows e fornendo alcuni consigli classici per minimizzare i rischi di infezione sui S.O. considerati.

Ringraziamenti

Ringrazio Gianluca Camozzi <gc@xcos.it> per i suggerimenti forniti e le informazioni riguardanti Windows NT.

Riferimenti bibliografici

[1] Marco Beltrame, "1999, attacco a Unix", 15 Maggio 1999, http://www.infn.it/pub/galileo/archivio/mag/990515/2_art.html

[2] Marco Beltrame, "Virus: analisi di un contagio", 8 Gennaio 2001, http://194.185.199.161/hightech/freesoft/antivirus/contagio.shtml

[3] Kurt Seifried <seifried@securityportal.com>, "UNIX (and Linux especially) Viruses - The Real Story", 8 Marzo 2001, http://securityportal.com/closet/closet20000308.html

[4] Il virus "Bolzano", http://www.f-secure.com/v-descs/bolzano.shtml , http://www.avp.ch/avpve/NewExe/win32/bolzano.stm

[5] Il virus "FunLove", http://www.f-secure.com/v-descs/funlove.shtml , http://www.avp.ch/avpve/newexe/win32/flc.stm

[6] "Ramen Worm", http://www.sans.org/y2k/ramen.htm

[7] "Adore Worm" http://www.sans.org/y2k/adore.htm

Appendice A: virus manuale per Unix/Linux :)

Questo è un virus manuale per Unix/Linux. Il suo sviluppatore, nonostante studi e indagini approfondite, non ha trovato il modo di sviluppare un virus in grado di danneggiare i Sistemi Operativi di tipo Unix, che sembrano praticamente invulnerabili al concetto stesso di virus. Quindi vi chiede un po' di solidarietà e collaborazione:

- scegliete cortesemente i primi 50 indirizzi della vostra rubrica e inoltrate loro il presente virus;
- poi cancellate qualche importante file di sistema;
- infine, se è venerdì 17, formattate il disco rigido.

Grazie per la collaborazione :)

Appendice B: Copyright

Appendice C – The GNU Free Documentation License

La licenza qui riportata è reperibile agli URL
`http://www.fsf.org/copyleft/fdl.html`
`http://fly.cnuce.cnr.it/gnu/doc.it/fdl.it.html`

```
GNU Free Documentation License
   Version 1.1, March 2000

 Copyright (C) 2000  Free Software Foundation, Inc.
     59 Temple Place, Suite 330, Boston, MA  02111-1307  USA
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.


0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other
written document "free" in the sense of freedom: to assure everyone
the effective freedom to copy and redistribute it, with or without
modifying it, either commercially or noncommercially.  Secondarily,
this License preserves for the author and publisher a way to get
credit for their work, while not being considered responsible for
modifications made by others.

This License is a kind of "copyleft", which means that derivative
works of the document must themselves be free in the same sense.  It
complements the GNU General Public License, which is a copyleft
license designed for free software.

We have designed this License in order to use it for manuals for free
software, because free software needs free documentation: a free
program should come with manuals providing the same freedoms that the
software does.  But this License is not limited to software manuals;
it can be used for any textual work, regardless of subject matter or
whether it is published as a printed book.  We recommend this License
principally for works whose purpose is instruction or reference.


1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work that contains a
notice placed by the copyright holder saying it can be distributed
```

under the terms of this License. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you".

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (For example, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, whose contents can be viewed and edited directly and straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup has been designed to thwart or discourage subsequent modification by readers is not Transparent. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML designed for human modification. Opaque formats include

PostScript, PDF, proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies of the Document numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a publicly-accessible computer-network location containing a complete Transparent copy of the Document, free of added material, which the general network-using public has access to download anonymously at no charge using public-standard network protocols. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has less than five).

C. State on the Title page the name of the publisher of the
   Modified Version, as the publisher.
D. Preserve all the copyright notices of the Document.
E. Add an appropriate copyright notice for your modifications
   adjacent to the other copyright notices.
F. Include, immediately after the copyright notices, a license notice
   giving the public permission to use the Modified Version under the
   terms of this License, in the form shown in the Addendum below.
G. Preserve in that license notice the full lists of Invariant Sections
   and required Cover Texts given in the Document's license notice.
H. Include an unaltered copy of this License.
I. Preserve the section entitled "History", and its title, and add to
   it an item stating at least the title, year, new authors, and
   publisher of the Modified Version as given on the Title Page. If
   there is no section entitled "History" in the Document, create one
   stating the title, year, authors, and publisher of the Document as
   given on its Title Page, then add an item describing the Modified
   Version as stated in the previous sentence.
J. Preserve the network location, if any, given in the Document for
   public access to a Transparent copy of the Document, and likewise
   the network locations given in the Document for previous versions
   it was based on. These may be placed in the "History" section.
   You may omit a network location for a work that was published at
   least four years before the Document itself, or if the original
   publisher of the version it refers to gives permission.
K. In any section entitled "Acknowledgements" or "Dedications",
   preserve the section's title, and preserve in the section all the
   substance and tone of each of the contributor acknowledgements
   and/or dedications given therein.
L. Preserve all the Invariant Sections of the Document,
   unaltered in their text and in their titles. Section numbers
   or the equivalent are not considered part of the section titles.
M. Delete any section entitled "Endorsements". Such a section
   may not be included in the Modified Version.
N. Do not retitle any existing section as "Endorsements"
   or to conflict in title with any Invariant Section.

If the Modified Version includes new front-matter sections or
appendices that qualify as Secondary Sections and contain no material
copied from the Document, you may at your option designate some or all
of these sections as invariant. To do this, add their titles to the
list of Invariant Sections in the Modified Version's license notice.
These titles must be distinct from any other section titles.

You may add a section entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections entitled "History" in the various original documents, forming one section entitled "History"; likewise combine any sections entitled "Acknowledgements",

and any sections entitled "Dedications". You must delete all sections entitled "Endorsements."

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, does not as a whole count as a Modified Version of the Document, provided no compilation copyright is claimed for the compilation. Such a compilation is called an "aggregate", and this License does not apply to the other self-contained works thus compiled with the Document, on account of their being thus compiled, if they are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one quarter of the entire aggregate, the Document's Cover Texts may be placed on covers that surround only the Document within the aggregate. Otherwise they must appear on covers around the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include

translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License provided that you also include the original English version of this License. In case of a disagreement between the translation and the original English version of this License, the original English version will prevail.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http:///www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page: