Corso Integrato di statistica,informatica e analisi dei dati sperimentali

Prof Carlo Meneghini
Dip. di Fisica "E. Amaldi"
via della Vasca Navale 84
meneghini@fis.uniroma3.it
tel.: 06 57337217

http://www.fis.uniroma3.it/~meneghini

Malware & Co.

Virus (Malware):

È una sequenza di istruzioni che il sistema operativo del PC è in grado di interpretare ed eseguire. A differenza di altri programmi un malware può provocare danni e/o malfunzionamenti nel sistema operativo.

Come un virus biologico può **replicarsi** infettando un "file" ospite: programma, documento, boot sector etc…

Non può essere generato da un errore (in tal caso si tratta di un **bug**) ma, al contrario, è frutto di cosciente programmazione

Fred Cohen (http://www.all.net/books/virus/index.html) un virus è un programma in grado di infettare altri programmi aggiungendovi una copia (eventualmente evoluta) di se stesso. (cose interessanti: http://www.all.net/journal/50/index.html)

Solo I programmi in grado di replicarsi sono propriamente virus, in modo più generico un programma dannoso è detto: MALWARE da: MALicious softWARE

Articoli interessanti e letteratura

http://education.mondadori.it/libri/Download/Capitoli/88-8331-334-8_cap04.pdf
http://sicurezza.html.it
http://sicurezza.html.it/guide/lezione/3365/una-classificazione/
http://it.wikipedia.org/wiki/Portale:Informatica
http://www.computerflash.net/index.php?modulo=directory&cat=146
http://www.safer-networking.org/it/targetpolicy/index.html

Virus codici che si diffondono copiandosi all'interno di altri programmi o in alcune sezioni particolari del disco fisso (es. boot sector). Si diffondono da PC a PC via via che vengono copiati i file infetti.

Worm non necessitano dell'apertura del file infettato per diffondersi: modificano il sistema operativo del PC ospite in modo da essere eseguiti automaticamente in modo da replicarsi e diffondersi (canale privilegiato internet, mail). Per indurre gli utenti ad eseguirli usano tecniche di Social Engineering, o sfruttano alcuni difetti (i cosiddetti Bug) di alcuni programmi o di alcuni sistemi operativ.

Trojan horse codici che si nascondono all'interno di programmi con funzionalità lecite e che effettuano azioni dannose all'insaputa dell'utente.

Backdoor: Sono software che consentono un accesso illegittimo e non autorizzato al sistema su cui sono in esecuzione. Tipicamente si diffondono in abbinamento a trojan o worms.

Spyware: vengono utilizzati per trasmettere informazioni sul sistema al destinatario interessato. Lo spyware registra informazioni presenti sul PC infettato e le invia a terze parti.

Dialer: dirottano le connessioni dei modem classici (obsoleti)

Hijackers: si occupano di dirottare la connessione verso pagine web indesiderate (contenuto illecito, pubblicitario o pornografico).

Adaware: installano sul pc contenuti pubblicitari non desiderati (es. finestre di pop-up e avvisi)

Rootkit sono composti da driver o copie modificate di normali programmi inseriti nel sistema. Hanno la funzione di mascherare sia all'utente che a programmi tipo antivirus la presenza di particolar file o impostazioni del sistema. Possono essere utilizzati per nascondere o mascherare altro software dannoso.

Rabbit: sono programmi che esauriscono le risorse del sistema moltiplicandosi ad altissima velocità,

Batch: i Batch sono i cosiddetti "virus amatoriali": semplici files patch che, se eseguiti, contengono istruzioni dannose.

Keylogger: sono programmi in grado di registrare tutto ciò che un utente digita su una tastiera o col copia e incolla rendendo così possibile il furto di password o di dati che potrebbero interessare qualcun'altro.

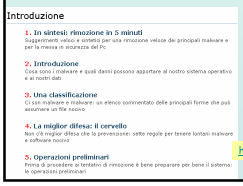
Assistendi del browser (BOH) I Plug-in sono programmi di piccole dimensioni che aumentano le funzionalità di un programma o di una applicazione. I Browser plug-in sono simili a dei plug-in ma con caratteristiche rivolte alla navigazione e ricerca su Internet. Un BHO non è di per se una minaccia fintanto che non si installa segretamente e non monitora il comportamento dell'utente.

Hoax, Spam, Phishing, PopUp

Wikipedia - Sicurezza.html.it

- **Regolare** le impostazioni del **browser** (Explorer, Firefox, Opera, etc….)
- **Regolare** le impostazioni del **firewall** (imparare ad usare il firewall in "experto mode")
- **Regolare** le impostazioni dell'**antivirus** (aggiornamento e scansione)
- **Regolare** le impostazioni per l'**aggiornamento** sel **SO**
- **Non** accettare **download** da **fonti sconosciute** e controllare quello di fonti conosciute.
- Diffidare delle offerte **GRATIS**
- Imparare a conoscere il proprio PC e notare i comportamenti anomali (pagine web non selezionate, cambiano le impostazioni di sistema, risposte particolarmente lente)
- Imparare cercare ed usare gli strumenti di rimozione (gruppi di discussione, forums, siti antivirus)
- Informarsi sulle tecniche di infezione e sul funzionamento dei malware

http://www.symantec.com/business/security_response/threatexplorer/index.jsp



Informarsi su siti e blog di assistenza e informazione

http://www.xraysite.it/

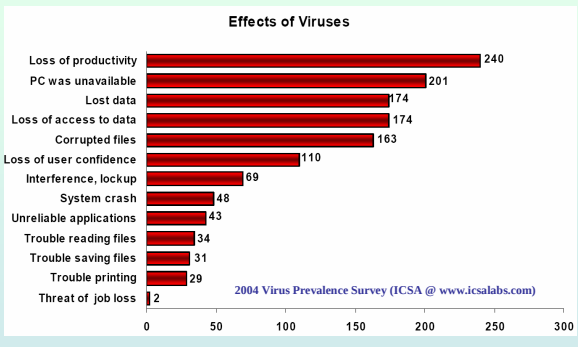
http://sicurezza.html.it/guide/leggi/132/guida-rimozione-malware/

I virus informatici

Un virus codice in grado di **infettare un programma ospite** tramite il quale replicarsi e **propagarsi ad altri programmi** (nota: il sistema operativo è un insieme di programmi) con lo scopo di provocare danni e malfunzionamenti:

- Visualizzare messaggi o effetti video.
- Cancellare files o formattare unità a disco.
- **Cifrare il contenuto di un disco rigido rendendolo illeggibile.**
- Rendere instabile il comportamento del sistema.
- Impedire l'avviamento del Pc o di programmi.
- Modificare i dati all'interno di documenti.
- Inviare messaggi di posta elettronica in modo massiccio.

I virus informatici, analogamente ai virus biologici, necessitano di un programma ospite per operare. Come i virus biologici tendono a dar luogo ad epidemie più o meno gravi diffendendosi tramite files e programmi infetti da un computer ad un altro. Le connessioni in rete favoriscono il diffondersi delle infezioni.



I virus sono caratterizzati da una speciale sequenza di comandi, quindi una particolare sequenza (stringa) nel codice del programma.

Queste stringhe, conservate nei database degli antivirus, consentono l'individuazione del virus

I generazione

1. Replicazione in programmi non infetti
2. azioni di disturbo e danneggiamento.

II generazione: virus residenti

1. Istallazione nella memoria RAM o nell'area di Boot
2. Infezione di programmi in modo selettivo
3. Azioni di disturbo e danneggiamento.

III generazione: virus mutanti

1. Mutazione: la stringa di codice viene alterata.
2. Istallazione
3. Infezione di programmi
4. Azioni di disturbo e danneggiamento.

IV generazione

Virus del BIOS: indipendenti dal sistema operativo

... generazione

Virus delle Macro: attaccano le configurazione di programmi come word processor, fogli elettronici, programmi per la posta elettronica, etc...

Logic bombs & time bombs: virus dormienti che si attivano quando si verificano date condizioni o ad una data specifica

... etc...

Classificazione dei Virus

Virus di Macro

Sono i virus più semplici da realizzare e proprio per questo i più diffusi. Usano come veicolo le macro, cioè "strumenti" in programmi wordprocessor e fogli elettronici che permettono di registrare ed eseguire automaticamente sequenze di operazioni.

Il virus si nasconde nelle macro di un documento e si avvia non appena questo viene aperto. Modifica le sequenze di operazioni, l'aspetto e il funzionamento del programma principale. Infetta i documenti e si propaga ad altri utenti mediante lo scambio dei files. E' in grado di cancellare i file, di rinominarli e di modificarne il contenuto, modificare l'aspetto e il funzionamento dei programmi.

Virus di avvio (o Bootsector)

Si installano nella zona di avvio del disco rigido (il Bootsector) o dei floppy disk. Si attivano all'avvio del computer e si riproducono nei programmi diffondendosi. Non vengono rimossi durante le normali operazioni di "pulizia come la formattazione dei dischi.

Virus di file eseguibili

Questi virus viaggiano tra i programmi installati nel pc sostituendosi al software sano e avviandosi al suo posto. Dopo aver concluso la sua missione distruttrice, passano ad un altro programma, paralizzando via via tutte le applicazioni presenti nel pc malcapitato.

Virus polimorfi

Sono virus in grado di modificare il proprio codice in modo da rendersi irriconoscibili all'antivirus. Possono mutare meccanismi di azione e di disturbo producendo cloni sempre diversi.

Regole di sicurezza

1. Limitare lo scambio e la trasmissione di files .EXE, .COM, .OVR, .OVL, .SYS, .DOC, .XLS fra computers.
2. Per principio sottoporre a controllo (scansione) qualsiasi file (di qualunque provenienza) prima di eseguire o leggerne il contenuto.
3. Ridurre l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza. (Non accettare download da fonti sconosciute).
4. Tenersi informati sulle nuove strategie e sui nuovi comportamenti virali e aggiornare regolarmente gli antivirus e il S.O. Effettuare CONTROLLI PERIODICI con programmi "antivirus".
5. Prestate attenzione a qualunque comportamento "strano"del vostro Pc.
6. Sviluppare una cultura della sicurezza come prerequisito per l'utilizzo del computer in modo da diminuire il più possibile i rischi di "infezione" da sorgenti interne e/o esterne.
7. Sapere come recuperare i dati e i programmi dopo un'infezione virale. Munirsi di strumenti per la rimozione specificatamente mirati.
8. Effettuare frequenti BACKUP dei dati e programmi "critici".
9. Evitate i siti "ambigui"
10. Sviluppare procedure per contenere un'infezione quando incontrata.

Non seminare il panico inoltrando messaggi idioti ma informarsi sulla veridicità degli allarmi (Hoax).

La migliore difesa cointro un'infezione consiste nel tenersi costantemente informati sulle caratteristiche dei virus

Database e informazioni

www.viruslist.com

www.icsalabs.com

www.symantec.com/business/security_response/threatexplorer/index.jsp

www.wildlist.org

www.ilsoftware.it/av.asp

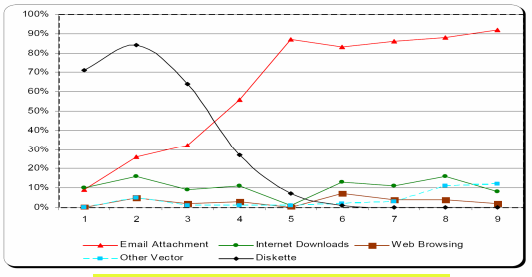
Storia

Ipotizzati fin dagli anni 70 (fantascienza) il primo virus compare nel 1982: "Elk Cloner". Si propagava scambiando i floppy disk infettando il boot sector del sistema DOS 3.3 dei PC AppleII provocando effetti grafici, testo lampeggiante e la poesia:

ELK CLONER:
THE PROGRAM WITH A PERSONALITY
IT WILL GET ON ALL YOUR DISKS
IT WILL INFILTRATE YOUR CHIPS
YES, IT'S CLONER
IT WILL STICK TO YOU LIKE GLUE
IT WILL MODIFY RAM, TOO
SEND IN THE CLONER!

Metodi di propagazione

Virus Source	1996	1997	1998	1999	2000	2001	2002	2003	2004
Email Attachment	9%	26%	32%	56%	87%	83%	86%	88%	92%
Internet Downloads	10%	16%	9%	11%	1%	13%	11%	16%	8%
Web Browsing	0%	5%	2%	3%	0%	7%	4%	4%	2%
Other Vector	0%	5%	1%	1%	1%	2%	3%	11%	12%
Software Distribution	0%	3%	3%	0%	1%	2%	0%	0%	0%
Diskette	71%	84%	64%	27%	7%	1%	0%	0%	0%



2004 Virus Prevalence Survey (ICSA @ www.icsalabs.com)

I peggiori della storia

11. **CIH (1998)**
Stima danni: da 20 a 80 milioni di dollari, dati distrutti in quantità incalcolabile. Tutto inizia nel 1998. **Cih** viene diffuso da Taiwan: è conosciuto come uno dei peggiori della storia perché in grado di sovrascrivere file e **cancellare il Bios** del computer infettato, rendendone impossibile l'avvio. Sulle sue vittime erano installati Windows 95, 98 e Millenium Edition, ma è stato reso innocuo dall'evoluzione della sicurezza di Windows 2000

10. **MELISSA** (1999)
Stima danni: da 300 a 600 milioni di dollari. Si suppone che questo macrovirus per Word abbia infettato il 15-20 % di tutti i computer usati negli uffici del mondo. Attivato il 26 marzo 1999, usava Outlook per inviarsi, sottoforma di messaggio (*"Questo è il documento che mi hai chiesto... non farlo vedere a nessuno ;-)"*) a 50 nomi presenti nella rubrica della vittima. Intel, Microsoft e altre aziende hanno dovuto chiudere momentaneamente l'intero sistema interno di posta elettronica per riuscire a fermare il contagio. Il virus, tra l'altro, modificava i documenti Word inserendo citazioni dei personaggi dei Simpson.

9. **ILOVEYOU** (2000)
Apparso il 3 maggio 2000 a Hong Kong, viaggiava sotto forma di un file chiamato LOVE-LETTER-FOR-YOU.TXT.vbs. **A chi nascondeva l'estensione dei file sembrava ujn file ASCII (testo)**, invece era uno script Visual Basic che veniva inviato sempre attraverso Outlook Express. L'autore, filippino, non venne mai processato perché al tempo le Filippine non avevano una legislazione antivirus. I danni furono comunque ingenti.

8. **CODE RED** (2001)
Colpì il 13 luglio 2001, prendendo di mira i server con software IIS Microsoft. La falla era stata già tappata da Microsoft con un update di un mese prima, ma **un numero enorme di computer non era aggiornato**. Il totale delle vittime si stima in 400 mila server e un milione di stazioni di lavoro in totale.

7. **SQL SLAMMER** (2003)
Il **worm** colpì di sabato, il 25 gennaio 2003, attaccò mezzo milione di server in tutto il mondo e fece fuori per dodici ore Internet in tutta la Corea del Sud. Sfruttava un baco nel motore di SQL Server di Microsofted era lungo 376 byte, che gli bastavano per infettare, creare numeri IP a caso e autospedirsi ai numeri suddetti. Nei primi dieci minuti di vita attaccò 75 mila server.

6. **BLASTER** (2003)
Una vulnerabilità di Windows 2000 e XP fu dall'11 agosto 2003 la via di accesso di questo **worm** verso centinaia di migliaia di computer, che improvvisamente videro apparire sullo schermo una finestra di dialogo ad annunciare uno spegnimento imminente del sistema. Nel codice dell'eseguibile era nascosto il messaggio "Bill Gates, perché rendi possibile questo? Smettila di fare soldi e sistema il tuo software!".

5. **SOBIG.F** (2003)
Il debutto di Sobig.F avvenne il 19 agosto 2003 e fu un record; il 20 agosto si era già riprodotto in oltre un milione di copie, tramite allegati postali apparentemente innocui di nome **application.pif** e **thank_you.pif**. Il 10 settembre il virus si disattivò da solo. Microsoft ha messo una taglia di 250 mila dollari sulla testa dell'autore, che non è mai stato scoperto.

4. **BAGLE** (2004)
Il problema del **worm** Bagle (o anche Beagle) e delle sue decine di varianti è l'apertura di **backdoor** verso una porta che può essere usata da un criminale informatico per estrarre dati e informazioni di ogni tipo dal computer infettato.

3. **MYDOOM** (2004)
Ha rallentato le prestazioni globali di Internet del 10 percento e rallentato il funzionamento del web del 50 percento. Nelle prime ore di vita del **worm**, il 26 gennaio 2004, alcuni esperti ritengono che un messaggio di posta elettronica ogni dieci in tutto il mondo stesse trasportando una copia del virus, il quale cercava di diffondersi anche attraverso le cartelle condivise della rete p2p di Kazaa. Fortunatamente MyDoom è stato programmato per disattivarsi il 12 febbraio 2004.

2. **SASSER** (2004)
Per molti al primo posto della classifica. Abbastanza distruttivo da troncare le comunicazioni via satellite nelle reti di alcune agenzie di comunicazione, annullare voli e chiusura di reti telematiche di alcune compagnie aeree. Invece che trasmettersi via posta elettronica questo worm sfruttava una falla di sicurezza di Windows 2000 e XP **non aggiornati**.

1. Per voi potrebbe essere quello che vi cancella l'unica versione definitiva della tesi il giorno prima della consegna!!!!

Virus... un po' restrittivo come concetto

Malware (*Malicious Software (UK)- Codice Maligno (IT)*): qualsiasi software creato con il solo scopo di creare danni più o meno gravi all'interno del computer nel quale viene eseguito o installato.

Molti utenti possiedono un computer infestato da malware di diverso genere senza nemmeno esserne a conoscenza

A livello internazionale la regolamentazione in merito alla legalità di diversi tipi di malware è estremamente variabile ed è continuamente in evoluzione. **Virus**, i **worm** e i **trojan** sono illegali in quasi ogni parte del mondo, per altre categorie è diverso. Es.: i **dialer** sono, di per sé, assolutamente legali, è l'**uso** che ne viene fatto che **potrebbe essere illegale**. L'ambiguità legislativa è alimentata anche dal semplice fatto che non sempre è possibile distinguere quale sia un software realmente **dannoso** e quale sia, al contrario, un software che si limita a svolgere **attività fastidiose (addons)**.

La tutela spetta in ultima istanza all'utente, che deve conoscere il software maligno per poterlo combattere e per poter difendere i propri dati personali, i propri interessi, nonché la propria privacy.

Programmi per la sicurezza e la pulizia

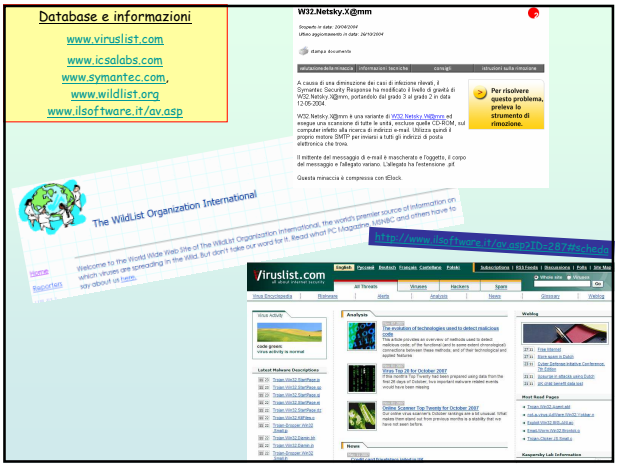
http://sicurezza.html.it/guide/lezione/3365/una-classificazione/

mywebpages.comcast.net/SupportCD/OptimizeXP.html

www.manuali.it/forum/viewtopic.php?p=98861&sid=b7b2f44b2a658f540475429dff10962e

Database e informazioni

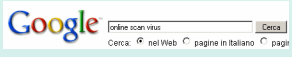
www.viruslist.com
www.icsalabs.com
www.symantec.com,
www.wildlist.org
www.ilsoftware.it/av.asp



In caso di infezione

- Non scambiare file con altri utenti.
- Non continuare a lavorare con la macchina infetta
- Cercare informazioni su Internet. Si possono trovare sul WEB le procedure e le utility per rimuovere il virus e (forse) recuperare i dati danneggiati.
- Ripristinare la funzionalità del computer.

In caso di sospetta infezione è utile eseguire lo scan del PC utilizzando windows in modalità provvisoria (tasto F8 all'avvio) e utilizzando utility di scansione on-line



Molti produttori di AV mettono a disposizione strumenti di scansione online:

Trend Micro: housecall.trendmicro.com/it/

Kaspersky: www.kaspersky.com/virusscanner

BitDefender: www.bitdefender.com/scan8/ie.html

Symantec: Security Check for Home Users (www.symantec.it).

Panda Software, www.pandasoftware.com … **e molti altri**

Worms

Un **worm**, come un virus, è un malware in grado di diffondersi, autoreplicarsi e causare danni ma, a differenza di un virus non necessita di un programma ospite per funzionare. Utilizza la rete internet per propagarsi. Di solito influenza le prestazioni di connessione in rete.

Prendono il nome da un "virus" descritto in un romanzo di fantascienza (*The Shockwave Rider*, J. Brunner - 1975) in grado di propagarsi in una rete di computers. I primi worms compaiono intorno alla fine degli anni 80 (~1988)

Tipologie di Worms

e-mail worms: si propagano attraverso la posta elettronica. Il worm i replica e si autoinvia a liste di corrispondenti vie e-mail fasulle mascherando il mittente.

Instant messaging worms: si diffonde usando i messagi istantanei (es.: windows messenger) fornendo link a siti infetti.

IRC worms: usano i canali delle chat come bersaglio e metodo di infezione.

File sharing network worms: si istallano nelle directories condivise con nomi innocui

Internet Worms: usano protocolli di basso livello (TCP/IP) per propagarsi. Spesso utilizzando vulnerabilità specifiche del sistema.

Effetti

Molto spesso un worm è fatto per disturbare le comunicazioni via rete occupando la banda. Tuttavia un worm può contentere codici per danneggiare il sistema ospite, cancellare i files o diffondere informazioni sensibili. Un azione tipica del worm è quella di aprire una connessione (backdoor) sul PC infetto che consente ad altri di utilizzarlo via rete. Si parla di Zombie computer: PC la cui sicurezza è stata compromessa e sotto il controllo di altri Sobig & Mydoom sono tipici esempi di worms di questo tipo.

I worms si diffondono soprattutto utilizzando **vulnerabilità dei sistemi operativi** o **ingannando gli utenti**. Per limitare i rischi di infezione è fondamentale **istallare gli aggiornamenti di sicurezza**.

W32.Sobig.F@mm

* Damage Level: Medium
* Large Scale E-mailing: Sends email to addresses collected from files with the following extensions: .wab, .dbx, .htm, .html, .eml, .txt.
* Releases Confidential Info: May steal system information, including passwords.

19

W32.Mydoom.AS@mm

Discovered: February 9, 2005
Updated: March 15, 2005 10:32:25 AM PST
Also Known As: Win32.Mydoom.AP [Computer Associates], Email-Worm.Win32.Mydoom.ak [Kaspersky Lab], W32/Mydoom.ba@MM [McAfee], W32/MyDoom-AR [Sophos], WORM_MYDOOM.AR [Trend Micro]
Type: Worm
Infection Length: 33,792 bytes
Systems Affected: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP

W32.Mydoom.AS@mm is a mass-mailing worm that uses its own SMTP engine to send itself to email addresses that it finds on the compromised computer. It also propagates through file sharing networks.

The email will have a variable subject and attachment name. The attachment will have a .bat, .cmd, .exe, .pif, .scr, or .zip file extension.

Damage
* Damage Level: Medium
* Large Scale E-mailing: Sends itself to email addresses gathered from the compromised computer.
* Modifies Files: Modifies the hosts file.
* Compromises Security Settings: Disables antivirus and firewall applications, blocks access to security-related Web sites.

Distribution
* Distribution Level: High
* Subject of Email: Varies
* Name of Attachment: Varies with a .bat, .cmd, .exe, .pif, .scr, or .zip file extension

Trojan

Un cavallo di Troia (trojan horse) è un malware che deve il suo nome al fatto di essere celato all'interno di un programma apparentemente utile. Sono ampiamente utilizzati per inviare spam, registrare dati personali (password e numeri di carte di credito), danneggiare files. A differenza di un virus i trojan (di solito) non si auto-replicano.

On the Microsoft Windows platform, an attacker might attach a Trojan horse with an innocent-looking filename to an email message which entices the recipient into opening the file. The Trojan horse itself would typically be a Windows executable program file, and thus must have an executable filename extension such as .exe, .com, .scr, .bat, or .pif. Since Windows is configured by default to hide filename extensions from a user, the Trojan horse is an extension that might be "masked" by giving it a name such as 'Readme.txt.exe'. With file extensions hidden, the user would only see 'Readme.txt' and could mistake it for a harmless text file. Icons can also be chosen to imitate the icon associated with a different and benign program, or file type, and (types)

When the recipient double-clicks on the attachment, the Trojan horse might superficially do what the user expects it to do (open a text file, for example), so as to keep the victim unaware of its real, concealed, objectives. Meanwhile, it might discreetly modify or delete files, change the configuration of the computer, or even use the computer as a base from which to attack local or other networks - possibly joining many other similarly infected computers as part of a distributed denial-of-service attack (zombie PC)

A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive.

en.wikipedia.org

Tipi di Trojan horses

Remote Access Trojans
Data Sending Trojans
Destructive Trojans
Proxy Trojans
FTP Trojans
Security software disabler Trojans
Denial-of-service attack (DoS) Trojans
URL Trojans

Trasmissione:

Messagistica istantanea
IRC (Internet Relay Chat)
Allegati
File Sharing
Bachi del Browser e E-mail

Effetti

cancellazione dei dati.
criptare i files a scopo di ricatto.
danneggiare i files.
mandare e ricevere files.
registrazione di screenshots.
registrazione di informazioni di login
registrazione di dati bancari
istallazione di backdoor su un PC.
raccolta di indirizzari e spamming.
permettere l'accesso remopto ad altri (RAT-remote administration tool)
favorire la diffusione di virus e malvare (vettore o untore)
creare network di computer zombie per spamming e attivita' illecite (DOS attack)

www.aboutonlinetips.com/it/what-is-trojan-horse-and-how-to-recover-from-a-trojan-horse-infection/

Spyware

en.wikipedia.org/wiki/Spyware

Uno spyware è un programma che raccoglie in modo subdolo informazioni personali dell'utente. Termine coniato intorno al '95 e rapidamente diffuso dopo il 2000. Uno spyware utilizza tecniche subdole quali il keylogging (registrazione dell'attività sulla tastiera), la registrazione dell'attività di surfing, analisi dei documenti sull'HD, etc... al fine di carpire informazioni

Possono registrare e inviare ad altri dati sensibili o semplicemente registrare le abitudini dell'utente per consentire una pubblicità mirata. Spyware sono spesso istallati insieme a programmi shareware e multimediaali. Informarsi: www.spywareguide.com

Adware

Deriva da advertising (advertising-supported software) e si riferisce a programmi pubblicitari, spesso senza il consenso dell'utente. Eudora invia messaggi pubblicitari per la versione free.

Tracking

Alcuni adware fanno uso di codici che registrano l'attività in rete (tracking cookies) per tracciare un profilo utente e sottomettere pubblicità mirata.

Protezione da Spy e Ad

Diffidare di freeware e shareware: informarsi prima di istallare un software dichiarato freeware, shareware, gratuito etc... Nota: La maggiore espansione di virus su sistemi microsoft non è dovuta, alla maggiore vulnerabilità del sistema windows ma deve essere attribuita alla minore esperienza e maggiore ingenuità dell'utente medio windows (nel 2005 di circa 5000 vulnerabilità meno di 1000 sono state osservate su sistemi microsoft, circa 2000 su SO unix/Linux e circa 2000 multipiattaforma).

utilizzare un firewall
Kerio Personal Firewall (30day full free dopo free con alcune limitazioni)
www.sunbelt-software.com/Kerio.cfm

istallare un filtro anti-spy e Ad-remover
spybot search and destroy (www.spybot.info).
ad-aware (SE porsonal) (Lavasoft) (www.lavasoft.com)

Spam, Hoax & Phishing

La maggiore espansione di virus su sistemi microsoft non è dovuta, alla maggiore vulnerabilità del sistema windows ma deve essere attribuita alla minore esperienza e maggiore ingenuità dell'utente medio windows

Spam: comunicazioni non richieste e insistenti di prodotti anche illeciti e illegali. I messaggi Spam contengono spesso link a siti contente materiale pornografico, offensivo, illegale etc...

Il danno è principalmente nell'occupazione della capacità dei servers (fino a 1/3 delle mail di AOL è occupata da messaggi spam)

Lo spam si diffonde via mail in modo diretto o sfruttando l'ingenuità e buona fede degli utenti.

Catene di messaggi, inviti a diffondere notizie etc.. sono un mezzo per diffondere messaggi spam.

NON RISPONDERE ALLE MAIL SPAM rispondere ad un messaggio di spam indica allo spammer che l'account è attivo!

NON DIFFONDERE IN MODO A-CRITICO AVVISI, ANNUNCI, APPELLI

Gli **Hoax** (bufale/burle) sono informazioni false o artefatte con avvisi di virus disastrosi, malattie, richieste di auito, casi umanitari etc... che quasi mai risultano vere. Un elenco aggiornato (italiano) si può trovare su www.attivissimo.net/antibufala. Prima di inviare queste mail fare una rapida ricerca sulla rete per controllarne la veridicità

http://attivissimo.blogspot.com/2008/07/antibufala-allarme-per-il-piombo-nei.html

HOAX

FATE ATTENZIONE!!!!!!!!!!!!
FATELA GIRARE , ANCHE PER CHI NON USA PRATICAMENTE MAI IL ROSSETTO!

L'articolo scritto dal dott. Nahid Neman del reparto di senologia oncologica dell'ospedale Mount Sinai di Toronto.

Soggetto: ROSSETTO

Di recente la ditta produttrice del rossetto ' RED EARTH' ha diminuito i prezzi da $ 67 a $ 9.90.
Conteneva piombo.
Il piombo causa il cancro. Le marche di rossetto che contengono piombo sono:

- CHRISTIAN DIOR - LANCOME – CLINIQUE - Y.S.L. - ESTEE LAUDER
- SHISEIDO - CHANEL (lip conditioner) - MARKET AMERICA-MOTNES - LIPSTICK

Più è alto il contenuto di piombo, più aumenta il rischio di cancro.
Si è trovato il più alto contenuto di piombo nel rossetto di Y..S.L.
Fate attenzione ai rossetti che durano (sulle labbra) più a lungo. Se il vostro rossetto dura molto è perchè contiene più piombo.

Ecco un test che potete fare da sole:

1. Mettete del rossetto sulla mano.
2. Usate un anello d'oro da strofinare sul rossetto.
3. Se il colore del rossetto diventa nero saprete che contiene piombo.

Questi dati vengono fatti conoscere al Centro Medico dell'Esercito Walter Reed.

I carcinogeni Dioxin causano il cancro, specie il cancro della mammella!!!!!

- Non esiste nessun *"Nahid Neman del reparto di senologia oncologica dell'ospedale Mount Sinai di Toronto"*.
- Non c'è nulla riguardo a quest'appello presso il Walter Reed Army Medical Center.
- Il piombo non ha il cancro fra i suoi effetti principali, come nota la US Environmental Protection Agency: causa semmai crescita ridotta, iperattività, calo dell'udito e danni cerebrali. Quindi chi ha scritto quest'appello non è particolarmente esperto in medicina e ha preso una cantonata, e questo rende probabile che l'abbia presa anche per quel che concerne il resto dell'appello.
- Vi sono effettivamente tracce di piombo in alcuni coloranti utilizzati nei rossetti, ma si tratta di quantità minuscole (nel caso peggiore verificato, 0,65 parti per milione), al di sotto dei livelli ritenuti pericolosi, secondo la risposta della American Cancer Society a quest'allarme; in proporzione, si tratta di livelli insignificanti rispetto alle altre fonti di inquinamento da piombo con cui veniamo a contatto. Vi sono fonti di piombo ben più significative e probabili, come le **vecchie vernici**, il **kajal** e certi **digestivi d'importazione parallela**, le **vecchie tubature** dell'acqua, la **ceramica**, le **lattine** saldate con il piombo usate per alimenti importati da alcuni paesi esteri; potete consultare l'elenco stilato dall'FDA.
- Come nota sempre la FDA (Food and Drug Administration), i prodotti cosmetici di dubbia provenienza, per esempio provenienti da paesi dove i controlli sono meno severi, possono contenere piombo in quantità potenzialmente pericolose.
- L'effetto di lunga durata dei rossetti non dipende dalla presenza di piombo.

Il **phishing** è un'attività criminale, illegale a tutti gli effetti, tramite cui vengono acquisite informazioni sensibili (carte di credito, coordinate bancarie, password, etc...) mascherandosi da ente/società/persona di fiducia.

Il phishing avviene tramite e-mail o instant message. Spesso si danno link a siti web copia di siti accreditati (banche, enti etc...).

Alcuni di questi siti sono disabilitati in Explorer, Mozilla, Opera etc...

NON FORNIRE PER ALCUN MOTIVO DATI SENSIBILI (password, numeri CC, coordinate bancarie, etc...) via web o e-mail

Antivirus

Un antivirus è un programma in grado di rilevare e rimuovere codici malware quali virus, worms, dialers, trojan.

Funzionamento:

1) ricerca in RAM e nei files del codice identificativo (firma) del virus.

2) controllo in tempo reale di files e programmi in transito (mail, WEB, download, etc...)

L'antivirus controlla la presenza di codici virali nei files utilizzando liste di virus. Il successo di questi programmi risiede nel continuo aggiornamento delle liste di firme dei virus conosciti (almeno settimanale, in caso di connessioni veloci è utile e poco dispendioso l'aggiornamento giornaliero)

Antivirus

Elementi di un AV:

1. il file delle firme
2. il codice in grado di cercare i virus nel PC
3. il codice che controlla i files in tempo reale
4. il codice per eseguire l'aggiornamento automatico delle liste

Un virus attivo (virus, trojan, etc...) può disattivare in toto o in parte l'antivirus.

Un antivirus può rimuovere i files infetti ma spesso è inefficiente contro i virus residenti per i quali è necessario uno strumento di rimozione opportuno e procedure a volte complesse

In caso di infezione può essere utile effettuare una scansione usando programmi esterni (via rete: es. trend-micro package)

Esistono diversi AV freeware, a pagamento, a costo ridotto per uso provato

I firewall

Un firewall è lo strumento che monitorizza il traffico che si genera nel nostro computer sia in qualità di connessioni entranti che di quelle uscenti, quindi si occupa di gestire i **pacchetti** filtrandoli permette di controllare l'accesso al proprio PC, selezionare le applicazioni da eseguire, limitare l'accesso in base a **regole opportune**,

www.manuali.it/forum/viewtopic.php?p=98861&sid=b7b2f44b2a658f540475429dff10962e

Pulizia da malware/spyware

CCleaner è un programma freeware che rimuove i file non utilizzati velocizzando Windows e liberando spazio disco.

Ad-aware è un software freeware per rimuovere Spyware, Adware, hijackers a altro malware

Spybot - Search and Destroy è un software freeware per rimuovere Spyware, Adware, hijackers a altro malware

Microsoft Windows Defender è un software freeware che aiuta a difendere il PC da danni dovuti a malware. Attenzione: Microsoft Windows Defender indica come spyware molti programmi Peer to Peer. Prima di rimuovere un'applicazione o altro assicurarsi di quello che si vuole fare (www.spywareguide.com)

Protezione dagli spyware

Diffidare di freeware e shareware: informarsi prima di istallare un software dichiarato freeware, shareware, gratuito etc.. Verificare sul sito: www.spywareguide.com

Spybot - Search and Destroy

SpywareBlaster 3.5.1
Prevent the installation of spyware and other potentially unwanted software!

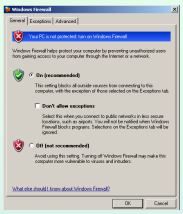
Impedisce l'istallazione di spyware basati su applicazioni Active-X

Firewall

Windows XP firewall

(start > settings > firewall)

E' incluso nella distribuzione WXP e automaticamente attivo nella SP2. Manca un rapporto di attività, utile per utenti più esperti.



Zone Allarm è un ottimo Firewall, freeware per uso personale.

Nota: non utilizzare più di un firewall attivo per evitare competizioni dannose

35

Zone Allarm KPF sono freeware per uso personale.

Zone Allarm

Sunbelt Kerio Personal Firewal

Features:	ZoneAlarm® Internet Security Suite	ZoneAlarm® Pro	ZoneAlarm® Anti-Spyware	ZoneAlarm® Antivirus	ZAsecure® Pro	ZoneAlarm® Free Download For non-business use only
	DOWNLOAD	DOWNLOAD	DOWNLOAD	DOWNLOAD	DOWNLOAD	DOWNLOAD
Basic Network and Program Firewall	x	x	x	x		x
Advanced Network and Program Firewall	x	x	x	x		
Operating System Firewall (OSFirewall™)	x	x	x	x		
Anti-Spyware	x	x	x			
Antivirus Protection	x			x		
Identity Theft Protection	x	x				
Game Mode	x	x	x	x		
Spy Site Blocking	x	x	x			
Privacy Protection	x	x				
Anti-Spam & Anti-Phishing	x					
Email Security	x	x	x	x		
IM Protection	x				x	
Wireless PC Protection	x	x	x	x		

Product:	SKPF 4 - free	SKPF 4 - full
NETWORK SECURITY		
Packet filter	YES	YES
File integrity control	YES	YES
Application communication control	YES	YES
Application launch control	YES	YES
Network Intrusion Prevention System	YES	YES
Host-based Intrusion Prevention System	NO	YES
CONTENT FILTERING		
Identity Theft Protection	NO	YES
Script blocking (JavaScript, VB script)	NO	YES
Referrer and Cookies blocking	NO	YES
Ad blocking	NO	YES
Pop-up windows blocking	NO	YES
STATISTICS, LOGGING		
Statistics of attacks and blocked ads	YES	YES
Automatic update checker	YES	YES
Extended logging	YES	YES
Syslog	NO	YES
Runs as Internet Gateway	NO	YES
ADMINISTRATION		
Remote administration	NO	YES
Password protected configuration	NO	YES

Utilities (www.grc.com/unpnp/unpnp.htm)

Unplug n' Pray:

Disabilita il servizio Universal Plug and Play networking.

Il servizio Universal Plug & Play non è connesso con il sistema standard di Plug & Play dell'hardware.

DCOMbobulator

Il sistema DCOM (Distributed Component Object Model) permette di attivare in modo remoto componenti del vostro S.O. e di utilizzare sulla rete!!!

WXP SP2 non è vulnerabile

shoot the messenger

Il servizio "Messenger" è utilizzato per diffondere messaggi SPAM.

In WXP SP2 è (o dovrebbe essere) disabilitato.

Software libero (Freeware)