BESSONE ELISA - RAMONDETTI MARCO

MACROVIRUS

programma eseguito dal processore
si diffonde attraverso i PROGRAMMI DI VIDEOSCRITTURA

PARTICOLARMENTE DANNOSO, RISCHIANDO ADDIRITTURA DI COMPROMETTERE, INFETTARE E CANCELLARE AD ESEMPIO FILE FONDAMENTALI PER IL SISTEMA OPERATIVO.

realizzata tramite un linguaggio che permette di creare dei piccoli codici detti **macrofunzioni:** eseguono una serie di comandi che consentono di velocizzare le operazioni più frequenti come la *selezione di un'opzione in una finestra di dialogo, oppure operazioni di modifica e formattazione o automatizzare una serie complessa di operazioni.*

I macro virus sono considerati dai programmatori **virus facili da realizzare, ma difficili da "depurare"** anche per i moderni antivirus.

MACROVIRUS

LA *LOCAZIONE FISICA* DEL MACRO VIRUS DIPENDE DAL **FORMATO** DEL FILE

AGISCONO SECONDO LE **ISTRUZIONI** DEL PROGRAMMATORE CHE LI HA CREATI

Si inseriscono in memoria sia quando viene caricato il documento infetto sia quando vengono compiute determinate operazioni come per esempio il salvataggio automatico
--> **prendono il controllo del programma in questione**.

I virus delle macro possono portare *molti problemi* come la possibilità di salvare il documento, cancellazione di intere directory di file, occupazione di memoria portata all'eccesso fino al blocco totale del sistema.

Una volta installato, può inibire varie funzioni di Word come l'apertura e chiusura di un documento, la modifica, il salvataggio di file e altro.

WORD

Formato generale ***Normal.dot*** che è quello che viene caricato normalmente all'avviamento di Word.

MACROVIRUS

POSTA ELETTRONICA

Può **trasmettere** virus informatici ma ***non li può mai trasmettere nel pc*** (a meno che non sia consentito eseguire automaticamente istruzioni macro senza il consenso dell'utente)

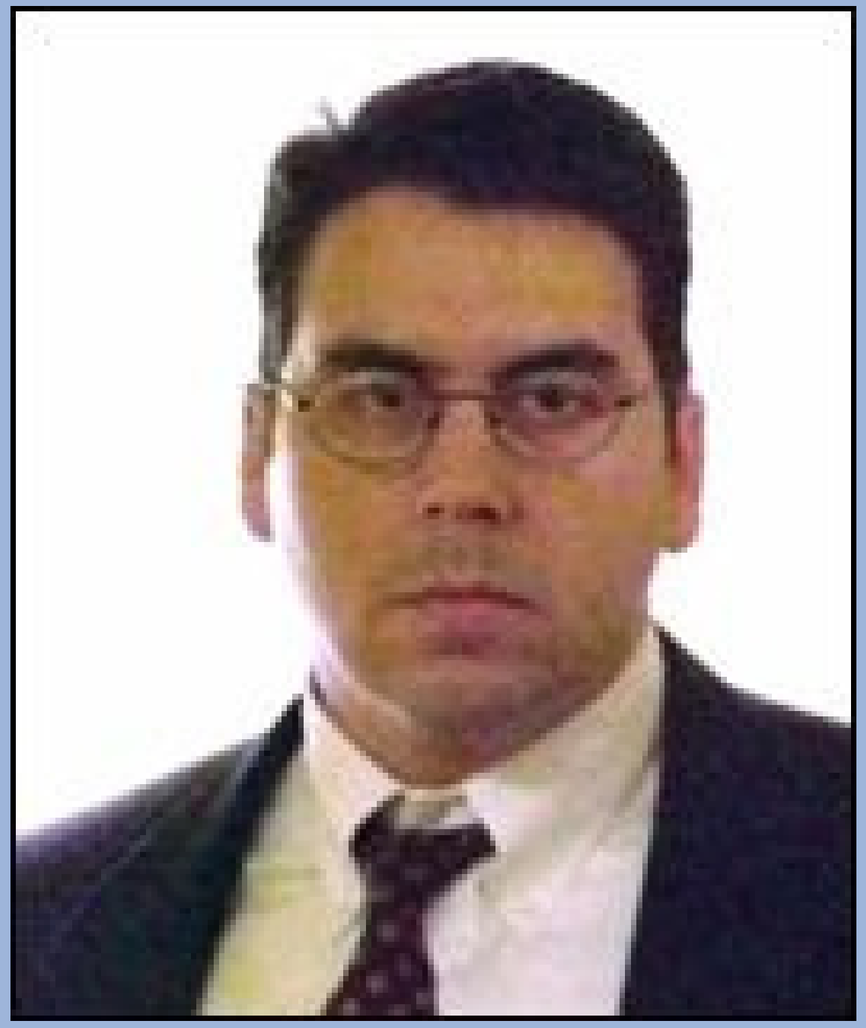
Appare SEMPRE la finestra con la quale si autorizza l'apertura di tali funzioni.
Il virus per cui non si può diffondere con i dati.

è **compito dell'utente** giudicare se eseguire il programma allegato o aprire il documento.

buona norma controllare i file allegati con un programma antivirus

David Lee Smith

MELISSA VIRUS
26 marzo 1999



Era un ex-programmatore di AT&T, azienda telefonica statunitense

Ammiratore della **striptease Melissa di Miami** da cui deriva il nome del virus.

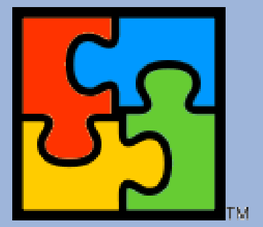
Collaborò con le autorità ammettendo le sue colpe e ottenne uno sconto della **pena in cambio di ore di lavoro presso l'FBI come ricercatore di virus e worm**, fu condannato a 20 mesi di carcere e ad una sanzione di 5.000 dollari

Melissa virus **infettò oltre un milione di sistemi**, provocò danni diretti stimati in oltre 80 milioni di dollari.

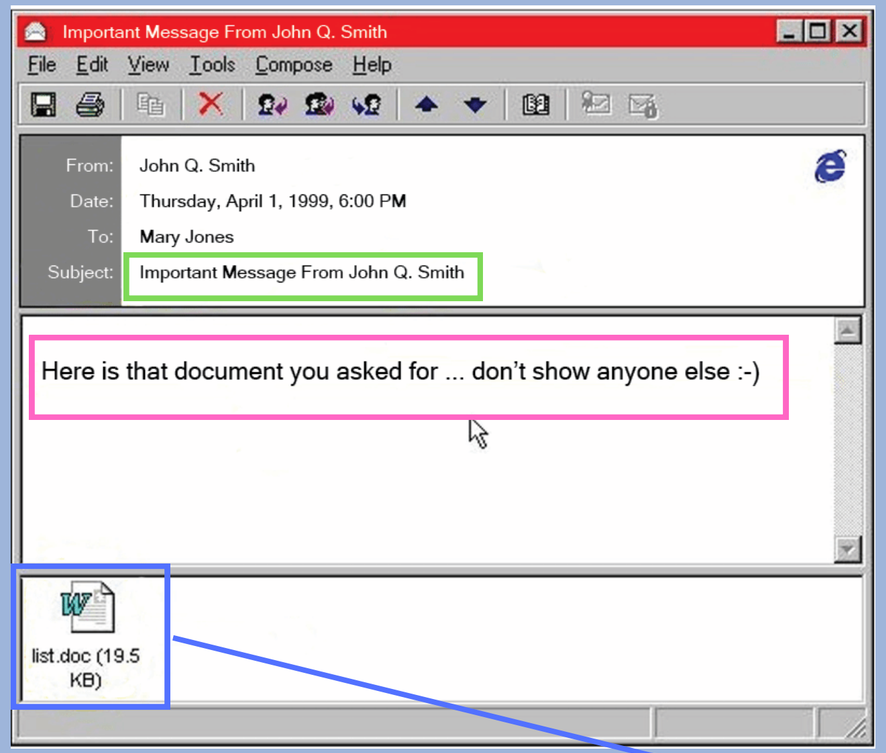
MELISSA VIRUS

macrolinguaggio di programmazione

L'infezione colpisce i sistemi operativi *Microsoft Windows 95, Windows 98 e Windows NT* con installata la suite *Microsoft Office 97 oppure Microsoft Office 2000*.



COME SI DIFFONDE?



tramite la posta elettronica, arriva come allegato di un messaggio e-mail: ***list.doc*** contenente una lista di siti pornografici con le *credenziali di accesso*

UPDATED MARCH 26 !!

ADULTCHECKGOLD - 4273ronronron 9082ronronron
ADULTCHECKGOLD - 4272ronronron 9342ronronron
ADULTCHECKGOLD - 4271ronronron 9645ronronron

1.http://www.cyberclub.com/ignite/members 1:6527582 p:GCMK
2.http://hotbox.danni.com/hotbox/1:heidi p:heidi
3.http://www.powerflow.com/members/135798642.html 1:r5g7s p:4t8y6
4.http://www.allasians1.com/membersonly/gallery/1:dragon p:gha04126@
5.http://www.breathlessbabes.com/protected1:gars p:sgar
6.http://www.caughtceleb.com/cmlogin.html L:cpsan5 P:citizen
7.http://www.pornmountain.com/members L:shawn P:shawn
8.http://www.sexillustrated.com/1stquarter/members2.htm L:manioo@innocent.com P:ts6jp69t
9.http://www.redlight.com/members 1:abc p:abc
10.http://www.freeamsterdamsex.com/members 1:forb p:bfor
11.http://www.allasians1.com/membersonly/gallery/ L:1111 P:1111

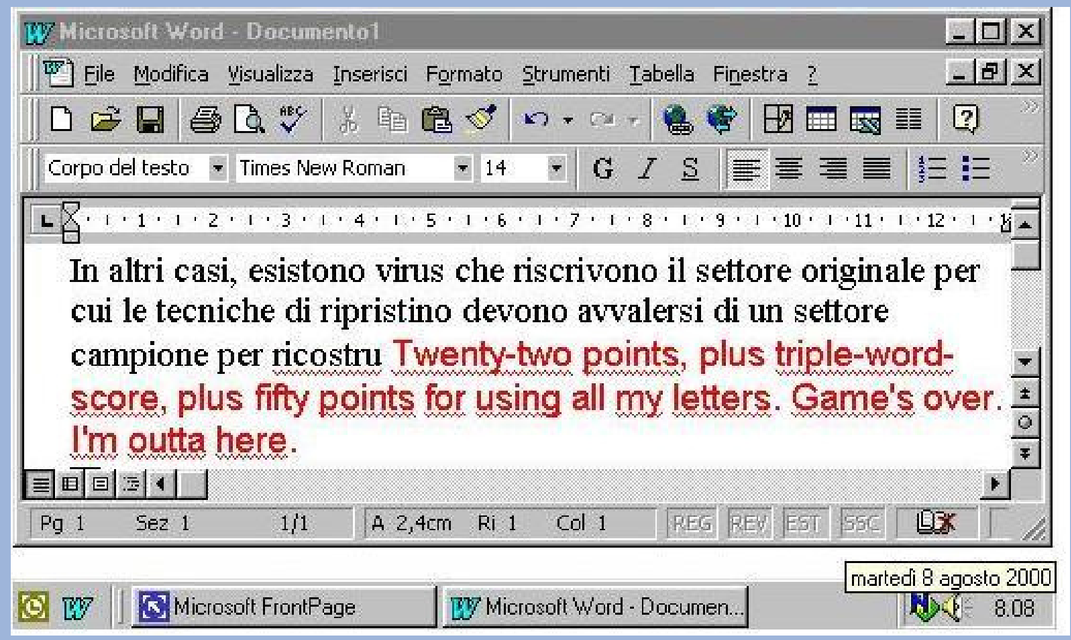
COME SI DIFFONDE?

il sistema esegue il codice del virus usando l'interprete VBA della suite Office e controlla se nel file di registro è presente la chiave **HKEY_CURRENT_USERSoftwareMicrosoftOffice"Melissa?"="...by Kwyjibo"**

se non è presente la chiave disattiva le protezioni che *evitano l'esecuzione delle macro* e poi **modifica il file "Normal.dot"** usato da Office come modello per tutti i documenti scritti con Microsoft Word, inserendovi il suo codice, da quel momento in poi tutti i file salvati con questo programma di videoscrittura risulteranno infetti.

se sul sistema è presente **Microsoft Outlook** spedisce una copia di sé stesso ai primi 50 nominativi presenti nella rubrica dei contatti.

Se l'utente sta usando Word in un determinato momento il virus altera i documenti quando i minuti dell'orario corrispondono al numero del giorno.



Ad esempio, se è l'11 aprile e l'utente sta aprendo o salvando un documento con Word all'undicesimo minuto di una qualunque ora di quel giorno (ad esempio le 14:11), il virus introduce nel testo la frase «**Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here**», che è un riferimento all'episodio "Bart the genius" della serie di cartoni animati The Simpson.

VARIANTI

Melissa.A

Melissa.I
verifica se nell'orario il numero dei minuti corrisponde a quello delle ore: in caso affermativo, inserisce il testo «**All empires fall, you just have to know where to push.**» nel documento attivo.

Melissa.O
invia le e-mail infette ai primi 100 contatti della rubrica. L'e-mail contiene il soggetto «***Duhalde Presidente Body: Programa de gobierno 1999 - 2004***.».

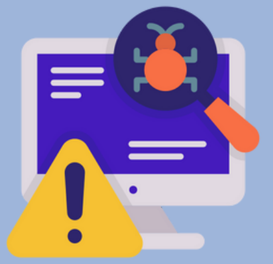
Melissa.U
è una variante più distruttiva. Spedisce le e-mail solo a 4 contatti ma, per contro, cancella alcuni file di sistema **c:\command.com - c:\io.sys - d:\command.com - d:\io.sys - c:\Ntdetect.com - c:\Suhdlog.dat - d:\Suhdlog.dat**

Melissa.V
è simile a Melissa.U rispetto alla quale si differenzia per il fatto che invia 40 e-mail. Fatto questo, essa cancella tutti i file presenti nella cartella radice dei dischi e poi visualizza una finestra di dialogo contenente il testo «**Hint: Get Norton 2000 not McAfee 4.02**»

Melissa.W
non disattiva le impostazioni relative all'esecuzione delle macro in Office 2000. Per il resto è identica a Melissa.A.

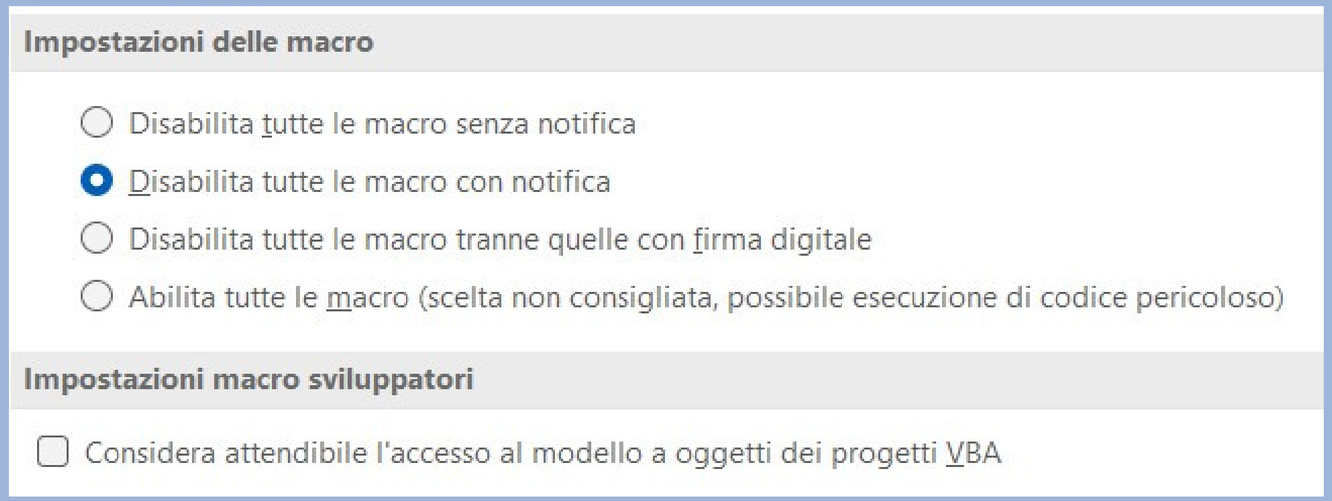
Melissa.AO
invia un messaggio con un testo differente rispetto a quello di Melissa.A nonché inserisce il testo «**Worm! Let's We Enjoy**» nel documento aperto alle ore 10 di ogni giorno 10 del mese.

RIMEDI



Per proteggersi dai Macro Virus si deve attivare perciò la protezione selezionandone l'opportuno livello, mediante il menu *Strumenti/Macro/Protezione*.

A questo punto risulta perciò opportuno alla ricezione di un file contenente macrodefinizioni con estensione .doc, .xls, durante l'apertura dell'avviso di conferma di attivazione della macro, prevenire cliccando sulla voce "**disattiva macro**", sia se si conosca la fonte del file, sia altresì se non si conosca la fonte.



Quest'azione permetterà di entrare nel documento in modalità di sola lettura: le macro sono disattivate (quindi l'eventuale macro virus è innocuo), non sarà possibile modificare il documento ma solo leggerne il contenuto.

SITOGRAFIA

Virus:W32/Melissa Description | F-Secure Labs

Technical details and removal instructions for programs and files detected by F-Secure products.

f-secure.com

What is the Melissa Virus?

This definition explains the Melissa virus and its impact as one of the first email viruses. Learn how to avoid similar viruses using the tips cited here.

Security

Melissa rinasce ed è velocissima

Le maggiori case antivirus sono in allarme, pare che la nuova versione di Melissa sia capace di riprodursi molto velocemente. Symantec, F-Secure e McAfee mettono tutt...

Punto Informatico / Jan 21, 2001

Virus Melissa: 20 anni dopo cosa abbiamo imparato?

Il virus provocò danni diretti stimati in oltre 80 milioni di dollari e bloccò l'operatività dei server mail di aziende ed enti governativi.

Key4biz / Mar 28, 2019

Melissa: il virus informatico che il 26 marzo 1999 paralizzò il mondo

Melissa, virus informatico creato da David Lee

http://www.di-srv.unisa.it/~ads/corso-security/www/CORSO-0102/macrovirus/melissa%20come_funziona.htm