

Ah AhnLab

TREND
MICRO

KASPERSKY

F-SECURE[®]

RISE
UNUSUAL SECURITY

avast!

bitdefender

eset

Norton[™]
from symantec

GLI ANTI VIRUS

K7 Computing
ウイルスセキュリティ

PANDA
SECURITY

BULLGUARD

ca

webroot

pc tools

Quick Heal

G DATA

McAfee[®]

AVG

Microsoft[®]
Security
Essentials

def i n i z i o n e

Un anti virus è un programma o una raccolta di programmi progettati per rilevare e rimuovere software nocivi.

st o r i a

Solamente anni dopo la comparsa dei primi virus (1982) si ebbe la necessità di progettare dei software in grado di rilevarli e contrastarli.

st o r i a

Inizialmente gli antivirus facevano unicamente riferimento ad una lista di «signatures» o firme, che veniva costantemente aggiornata.

Tale lista permetteva di identificare virus già noti come tali.

st o r i a

i p r o g e t t a t o r i d i v i r u s i n i z i a r o n o
q u i n d i a s c r i v e r e d e l c o d i c e c a p a c e
d i m u t a r e , i n m o d o d a i n g a n n a r e g l i
a n t i v i r u s d u r a n t e l ' a n a l i s i . Q u e s t i
v i r u s s i d i c o n o p o l i m o r f i.

st o r i a

Per far fronte a questo nuovo tipo di malware i programmatori svilupparono la tecnologia euristica. Questo sistema, che è indipendente dalle firme, utilizza una tecnologia ad intelligenza artificiale per rilevare i nuovi virus.

COMPONENTI

- File delle firme
- File binario dedicato alla ram
- File binario dedicato alla memoria interna
- File binario che aggiorna le firme

FUNZIONAMENTO

- Ricerca nella memoria RAM e/o all'interno dei file presenti in un computer;
- Utilizzo della scansione euristica, con l'analisi delle proprietà dei file oppure sul comportamento anomalo del sistema;

FUNZIONAMENTO

- Monitoraggio in tempo reale con controllo in background di tutti i file in entrata e in uscita nel / dal computer e analisi dei nuovi documenti;
- Run-time di file eseguibili in una sandbox;