Malware

A cura di: Maria Grazia Venturini
Classe: V Dsa
Anno: 2016-2017

Definizione

- Si definisce malware un qualsiasi software creato con il solo scopo di causare danni più o meno gravi al computer su cui viene eseguito.
  Il termine deriva dalla contrazione delle parole “malicious” e “software” ovvero "programma malvagio".

- Il termine malware è stato coniato nel 1990 da Yisrael Radai, precedentemente veniva chiamato virus per computer.

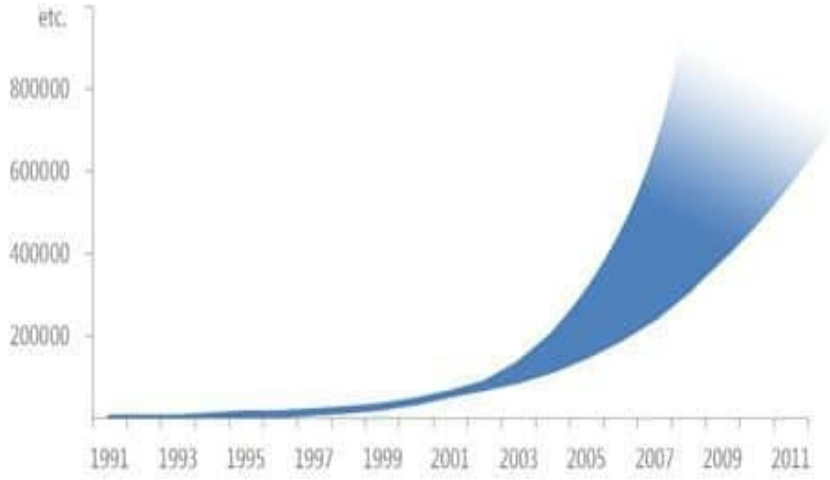
Perchè esistono i malware?

- I primi malware erano stati creati per scherzo o sfida da hackers individuali.
  Con il passare del tempo, la produzione di malware è diventata un'attività a scopo di lucro (anche definita cybercrime).

- I malware sono usati principalmente per rubare informazioni personali sensibili, in particolare i dati di accesso ai conti bancari, per pubblicizzare in modo intrusivo prodotti o servizi, essi rappresentano un problema anche a livello militare e industriale.

Il report Microsoft di fine 2012 sull'evoluzione del malware nel decennio 1991-2011 mostra la sua crescita:

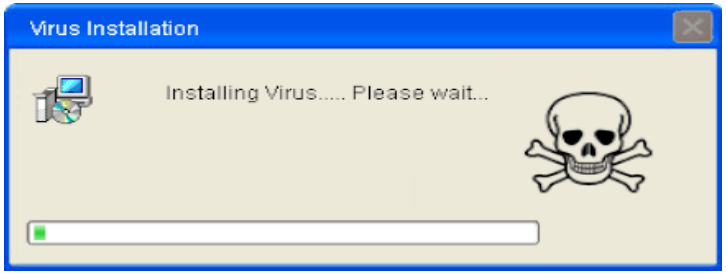
*Da circa 6mila nel 1991 si è passati a 60mila nel 2001



Categorie di Malware

Si distinguono molte categorie di malware, ecco le più conosciute e le più diffuse:

- Virus
- Worm
- Trojan Horse
- Rootkit
- Backdoor



Virus: Un virus è un software che è in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di sé stesso, generalmente senza farsi rilevare dall'utente.

Worm: (letteralmente "verme") è una particolare categoria di malware in grado di autoreplicarsi. È simile ad un virus, ma a differenza di questo non necessita di legarsi ad altri eseguibili per diffondersi.

Trojan horse: (Cavallo di Troia), è un tipo di malware. Deve il suo nome al fatto che le sue funzionalità sono nascoste all'interno di un programma apparentemente utile; è dunque l'utente stesso che installando ed eseguendo un certo programma, inconsapevolmente, installa ed esegue anche il codice trojan nascosto.

Rootkit: è un programma software creato per avere il controllo completo sul sistema senza bisogno di autorizzazione da parte di utente o amministratore

Backdoor: in informatica sono paragonabili a porte che consentono di superare in parte o in tutto le procedure di sicurezza attivate in un sistema informatico.

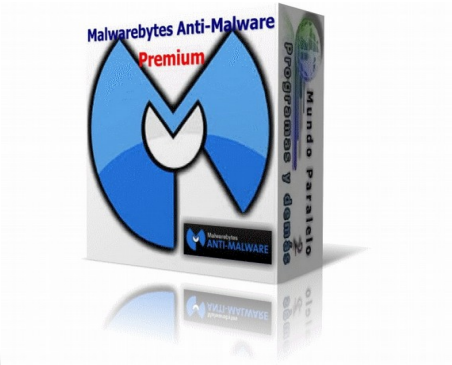
Protezione

- E’ bene dotare il computer di un buon sistema antivirus, capace di riparare il danno causato dall’infezione.

- I **programmi antivirus** sono in grado di scandire le memorie del computer per ricercare del codice sospetto che viene comparato con modelli di codice malware conosciuti (definizioni, firme, impronte).

- Se il codice esaminato corrisponde a una definizione, viene qualificato come malware e reso innocuo.

- Se non esiste la certezza che il codice sia del malware, il programma antivirus lo isola in una zona virtuale denominata quarantena.



Sitografia

- https://it.wikipedia.org/wiki/Malware
- https://en.wikipedia.org/wiki/Malware
- http://informaticaperanziani.it/2016/02/26/che-cose-un-malware-i-malware-sono-virus/
- http://viralblog2k9.blogspot.it/2009/05/definizione-di-malware.html