

**ITE “P. Savi”**  
**Formazione Ambito 28 ATA - Assistenti tecnici**  
**10/11/2017**  
**Introduzione alla sicurezza informatica**



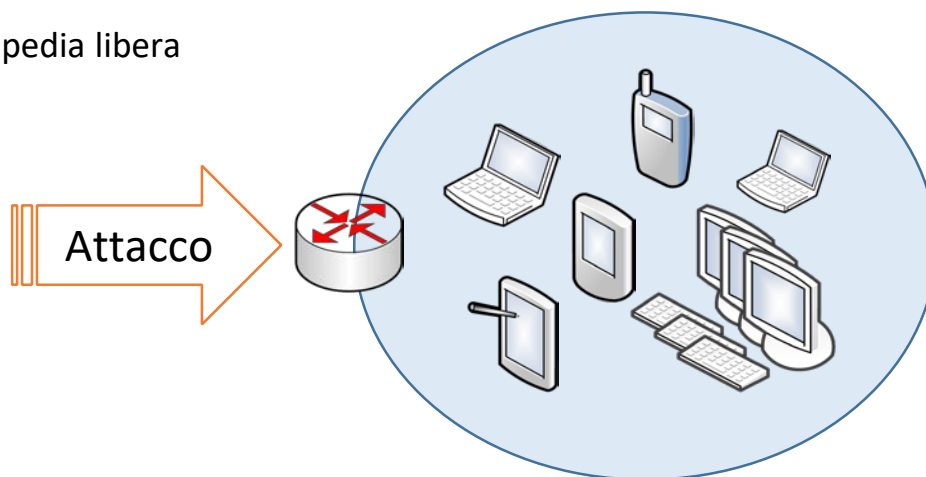
**Prof. Pier Giorgio Galli**  
**[piergiorgio.galli@istruzione.it](mailto:piergiorgio.galli@istruzione.it)**

# Sicurezza informatica

Con il termine sicurezza informatica si intende quel ramo dell'informatica che si occupa dell'analisi delle vulnerabilità, del rischio, delle minacce o attacchi e della successiva protezione dell'integrità fisica (hardware) e logico-funzionale (software) di un sistema informatico e dei dati in esso contenuti o scambiati in una comunicazione con un utente. Tale protezione è ottenuta attraverso misure di carattere tecnico-organizzativo e funzionali tese ad assicurarne:

1. l'accesso fisico e/o logico solo ad utenti autorizzati (autenticazione);
2. la fruizione di tutti e soli i servizi previsti per quell'utente nei tempi e nelle modalità previste dal sistema (disponibilità);
3. la correttezza dei dati (integrità);
4. l'oscuramento dei dati (cifratura);
5. la protezione del sistema da attacchi di software malevoli per garantire i precedenti requisiti.

Da Wikipedia, l'enciclopedia libera



# Malware

Nella sicurezza informatica il termine malware indica genericamente un qualsiasi software creato con il solo scopo di causare danni al sistema informatico su cui viene eseguito. Il termine deriva dalla contrazione delle parole inglesi malicious e software e ha dunque il significato letterale di "programma malvagio"; in italiano è detto anche codice maligno. Il malware viene catalogato in:

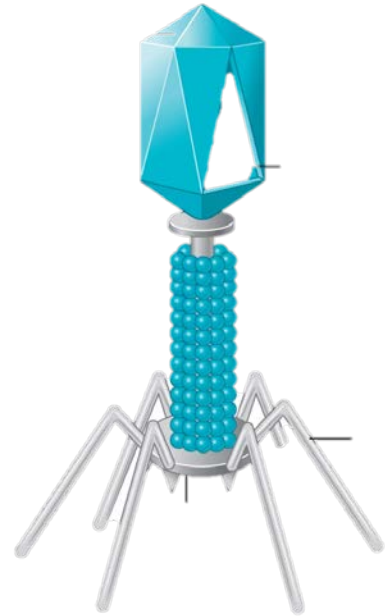
- Virus
- Worm
- Trojan
- Ransomware
- Spyware
- Hijacker
- Keylogger
- ecc.



# Virus (1)

Nella sicurezza informatica un virus è un software, appartenente alla categoria dei malware, che è in grado, una volta eseguito, di infettare dei **file eseguibili** in modo da riprodursi facendo copie di se stesso, generalmente senza farsi rilevare dall'utente (da questo punto di vista il nome è in perfetta analogia con i virus in campo biologico).

I virus possono essere o non essere dannosi per il sistema che li ospita, ma anche nel caso migliore comportano comunque un certo spreco di risorse in termini di RAM, CPU e spazio sul disco fisso. Come regola generale si assume che un virus possa danneggiare direttamente solo il software della macchina che lo ospita, anche se esso può indirettamente provocare danni anche all'hardware (ad esempio causando il surriscaldamento delle componenti fermando la ventola di raffreddamento).

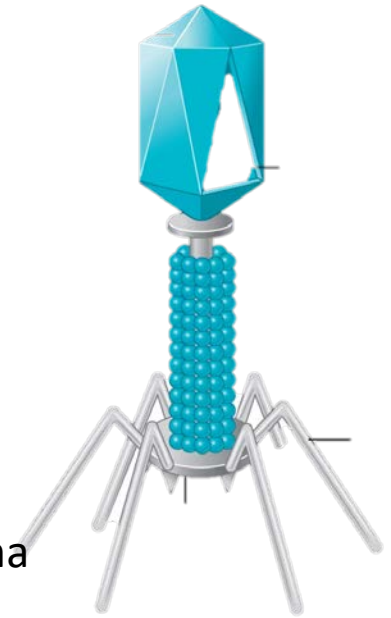


# Virus (2)

Un programma è composto da istruzioni in linguaggio macchina che vengono eseguite dalla CPU.

L'infezione di un virus in un programma consiste **nell'aggiungere** alle istruzioni del programma ospite blocchi di istruzioni con lo scopo:

- di ricercare altri file adatti ad essere infettati dal virus;
- di copiare il codice virale all'interno di ogni file adatto;
- di attivare la routine che contiene i criteri in base ai quali il virus decide se effettuare o meno l'attacco (es. una data, o l'estrazione di un numero a caso);
- il payload, una sequenza di istruzioni in genere dannosa per il sistema ospite.



## Sintesi:

1. il virus **non è un programma autonomo**, il suo codice viene eseguito **insieme** al codice del programma (infetto) che lo ospita;
2. il virus quando eseguito, **prima replica se stesso in altri file eseguibili** poi fa **qualsiasi** altra cosa: installare [altre] applicazioni maligne, cancellare file, danneggiare il sistema operativo, disinstallare periferiche, ecc.

# Worm

Un 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 programmi eseguibili per diffondersi.

Tipicamente un worm modifica il sistema che infetta, in modo da venire eseguito ogni volta che si avvia la macchina e rimanere attivo finché non si spegne il computer o non si arresta il processo corrispondente. Il worm tenta di replicarsi sfruttando Internet in diverse maniere: spesso i mezzi di diffusione sono più di uno per uno stesso worm.

Il mezzo più comune impiegato dai worm per diffondersi è la posta elettronica: il programma maligno ricerca indirizzi e-mail memorizzati nel computer ospite ed invia una copia di sé stesso come file allegato (attachment) a tutti o parte degli indirizzi che è riuscito a raccogliere.

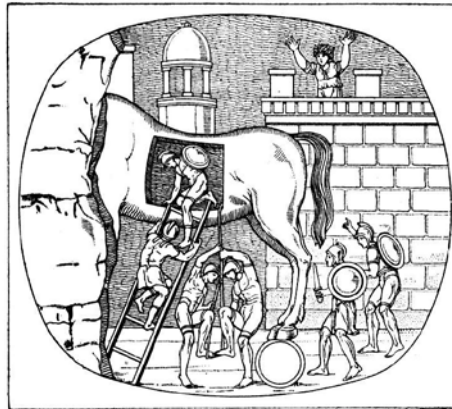
La tipologia forse più subdola di worm sfrutta dei bug di alcuni software o sistemi operativi, in modo da diffondersi automaticamente a tutti i computer vulnerabili connessi in rete.

Sintesi:

1. il worm è un **programma autonomo**;
2. il worm quando eseguito, **prima replica se stesso negli altri computer che riesce a raggiungere** poi fa **qualsiasi** altra cosa: installare [altre] applicazioni maligne, cancellare file, danneggiare il sistema operativo, disinstallare periferiche, ecc.

# Trojan (horse)

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.



## Sintesi:

1. il trojan è generalmente nascosto all'interno di un'applicazione all'apparenza utile;
2. il trojan alla prima esecuzione installa se stesso nel sistema ospite **diventando indipendente dall'applicazione che lo ha veicolato**. Dopo l'installazione il trojan, generalmente, viene eseguito ogni volta che viene avviato il computer.
3. il trojan in esecuzione fa qualsiasi altra cosa. Spesso i trojan si comportano come una backdoor, un programma che letteralmente "apre" il computer ospite ai criminali informatici per farne l'uso che più desiderano.

# Ransomware

Ransomware è un malware che cripta i file memorizzati nella memoria di massa del computer della vittima.

Il ransomware primo avvio si connette a uno dei server di comando e controllo per ottenere la chiave pubblica RSA che utilizzerà per cifrare tutti i file del disco rigido e di tutte le memorie di massa raggiungibili dal computer infetto. Il processo tipicamente cifra solo i file con alcune estensioni come quelle di Microsoft Office, Open document ecc. Al termine il malware informa l'utente che i suoi file non possono più essere aperti dalle applicazioni chiedendogli il pagamento di un riscatto per poter ottenere il software e la chiave privata necessaria per decifrare i file. A pagamento avvenuto l'utente potrà scaricare l'applicazione di decifrazione con la chiave privata già precaricata, in caso contrario i file rimarranno per sempre irrimediabilmente non utilizzabili.

## Sintesi:

1. il malware viene installato inconsapevolmente dall'utente o tramite un worm;
2. il malware alla prima esecuzione ottiene la chiave pubblica di un algoritmo di crittografia asimmetrica e con esso cripta i file dati dell'utente;
3. il malware informa la vittima che può ottenere la chiave privata, necessaria per decriptare i file, pagando un riscatto;
4. l'organizzazione criminale, una volta ottenuto il pagamento con modalità non tracciabili, invia alla vittima un software e la chiave privata per decriptare i file.



...e ancora:

- Spyware – malware che "ruba" i dati personali degli utenti presenti nelle memorie di massa e li trasmette al pirata informatico;
- Hijacker – malware che "dirotta" il browser verso pagine web indesiderate;
- Keylogger – software che cattura la sequenza dei tasti digitati sulla tastiera (**comprese le password!**) e le trasmette al pirata informatico;
- ecc.



# Antivirus

Un antivirus è un programma che blocca l'esecuzione o la memorizzazione nel sistema del malware.

L'antivirus viene immediatamente avviato dal sistema operativo e viene invocato **prima** che un programma venga eseguito e **prima** che un file venga memorizzato nel sistema (download da Internet, copia da chiavetta, ecc.).

L'antivirus verifica se il programma in procinto di essere eseguito o il file in corso di memorizzazione è **presente nel catalogo delle definizioni del malware**. Se è così l'antivirus blocca l'esecuzione del programma o la memorizzazione del file.

Il catalogo delle definizioni è continuamente aggiornato dalla casa produttrice dell'antivirus. Il catalogo delle definizioni presente nel computer che si intende proteggere deve essere allineato **con frequenza** (via internet) con il catalogo aggiornato dalla casa produttrice, in caso contrario l'antivirus perde di efficacia. L'allineamento del catalogo delle definizioni viene, di norma, eseguito automaticamente dall'antivirus all'avvio del computer.

**Il catalogo delle definizioni è aggiornato dalla casa produttrice dell'antivirus DOPO che il malware è stato rilasciato. Per questo nessun antivirus può assicurare una protezione sicura al 100%**

# Firewall

Il firewall è un apparato di rete hardware o un software che filtra i pacchetti entranti ed uscenti, da e verso una rete o un computer, secondo regole prestabilite. Configurando opportunamente le regole è possibile bloccare i pacchetti non desiderati cercando così di proteggere la rete o il singolo computer da attacchi diretti da parte di pirati informatici o da software che cercano di violare il sistema.

