# IL MALWARE
# CHE COS'È E COME DIFENDERSI?


Il termine **Malware** è l'abbreviazione di "**malicious software"** (software dannoso), indica un qualsiasi software usato per disturbare le operazioni svolte da un computer, rubare informazioni sensibili, accedere a sistemi informatici privati o mostrare pubblicità indesiderata.

Oltre a questo, un malware è creato per recare un danno al sistema informatico inoltre possono persino inviare finte email utilizzando i tuoi account di posta senza che il proprietario ne sia a conoscenza. Malware è un termine generico che fa riferimento a varie tipologie di software intrusivo o malevolo, ecco alcuni tipi di malware più comuni:

- **Virus**: programma informatico dannoso in grado di replicarsi e infettare un computer;
- **Worm**: programma informatico dannoso che invia copie di sé stesso ad altri computer attraverso una rete.
- **Spyware**: malware che raccoglie i dati delle persone senza il loro consenso.
- **Adware**: software che automaticamente riproduce, visualizza e scarica pubblicità su un computer.
- **Ransomware**: malware che "prendono in ostaggio" i dati dell'utente, cifrandoli, e li liberano fornendo la chiave di decifratura, dopo il pagamento di un riscatto pagato in una moneta virtuale, come i Bitcoin.
- **Cavallo di Troia:** un programma dannoso che assume le sembianze di un'applicazione utile ma che in realtà danneggia il computer o ruba dati una volta installato.

I primi malware sono stati scritti come esperimento o scherzo, oggi è costruito con intenti criminali in rete con l'obiettivo di guadagnare denaro, rubare password, informazioni utili e account bancari.

Per la prima volta dopo molti anni, la crescita del numero di nuovi malware ha subito una battuta d'arresto; ma non c'è da festeggiare: questo dato può semplicemente significare che i malware vecchi funzionano ancora bene e non è così urgente la necessità di sviluppare attacchi nuovi. Il numero di malware in circolazione è talmente elevato che chiunque abbia un computer, un tablet o uno smartphone prima o poi sarà attaccato.

Insieme al numero e alla varietà delle minacce stanno crescendo anche gli strumenti che gli utenti possono utilizzare per proteggersi. Ma è necessario conoscerli, comprenderne a fondo il funzionamento e i limiti, e mettere in campo una strategia di protezione complessiva, che copra vari aspetti: dall'aggiornamento dei programmi alla protezione delle connessioni, dal backup dei documenti alla tutela della privacy durante la navigazione.

## Come difendersi dal Malware?

La prima linea di difesa dagli attacchi del malware è rappresentato dal sistema operativo stesso: negli ultimi anni Windows è diventato molto più sicuro rispetto al passato, tanto che oggi la maggior parte degli exploit (ossia dei bug che possono consentire l'accesso agli hacker) non riguarda più il sistema operativo, quanto le applicazioni di terze parti installate al suo interno.

Ma mentre il sistema operativo diventa più sicuro, al suo interno si moltiplicano gli ambienti in cui è possibile eseguire codice: quasi tutti i pc moderni hanno installato il runtime Java, almeno un browser, il framework .NET e il plug-in Flash. E naturalmente bisogna anche considerare le funzioni di automazione integrate in molti software, come le suite di produttività o i pacchetti di disegno professionali. Per questo Microsoft non poteva limitarsi a rinforzare i componenti di un sistema operativo, ma doveva fornire una serie di funzioni e pacchetti di sicurezza che permettessero di garantire un livello minimo di protezione fin dal primo istante, senza dover installare un software di terze parti prima di iniziare a utilizzare il computer.

In un primo tempo ha aggiunto a Windows un firewall bidirezionale, poi **l'antispyware Defender**, che ha fatto la sua comparsa in Windows Vista, è cresciuto fino a incorporare anche le funzioni di protezione dai virus. Attualmente, fin dal primo avvio Windows offre una prima linea di protezione che garantisce un livello di sicurezza ragionevole.

Inoltre Microsoft offre **antimalware gratuiti e affidabili**, cioè software capaci di prevenire le infezioni e bloccare i pericoli prima che possano fare danni.

## Antimalware gratuiti.

La protezione garantita da Windows Defender è di sicuro meglio di niente, ma non è neppure eccezionale. Vediamo quali sono gli antimalware gratuiti più diffusi:

- **AVAST:** è un software antivirus sviluppato dalla AVAST Software di Praga, produce da sempre una versione gratuita del suo antivirus, affiancata da altre 2 a pagamento con funzioni aggiuntive. Nella sua offerta si trovano oggi security suite, servizi Vpn, password manager e utility di ottimizzazione per i mercati consumer, ma l'antivirus gratuito è ancor oggi il prodotto più noto e scaricato. Per scaricarlo basta raggiungere l'homepage del produttore (https://www.avast.com/). L'interfaccia del programma è molto semplice, la pagina principale mostra in modo chiaro lo stato della protezione, ed è dominata da un grande pulsante per avviare la scansione del computer. Le funzioni antimalware comprendono la protezione di in tempo reale, che analizza i file scaricati, aperti o manipolati, la classica scansione del computer e alcuni strumenti per verificare le estensioni del browser o controllare lo stato di protezione della rete domestica. Avast aggiunge un componente ai principali browser, per analizzare le pagine visitate ed evitare sorprese sgradite durante la navigazione. La sua presenza non è intrusiva, entra in azione soltanto quando si tenta di accedere a una pagina potenzialmente pericolosa. Le sue prestazioni sono buone, e i molti test a cui è stato sottoposto hanno certificato una buona affidabilità nella prevenzione e nella rimozione dei pericoli.
- **AVIRA:** anche Avira è un nome storico nel campo degli antivirus gratuiti; l'azienda tedesca offre un prodotto gratuito per uso non commerciale, a cui affianca varie soluzioni commerciali. L'antivirus integra naturalmente le funzioni di protezione in tempo reale e di scansione del sistema; propone molte funzioni di analisi del sistema, dedicate ai documenti, ai dischi locali e a quelli rimovibili, ai processi attivi e così via. Le scansioni possono essere avviate automaticamente, grazie a un semplice scheduler che propone una procedura guidata di configurazione molto chiara. Nel complesso Avira è un prodotto molto interessante; offre alcune utili funzioni di gestione e propone vari strumenti avanzati. Purtroppo non offre un sistema per creare direttamente un pen drive avviabile per la scansione e la pulizia dei computer senza dover passare da utility di terze parti.
- **AVG:** anche AVG propone da molti anni un antivirus gratuito, e anche in questo caso la versione free è affiancata da prodotti commerciali che offrono un numero maggiore di funzioni. Le funzioni antimalware comprendono naturalmente la protezione in tempo reale e le scansioni on demand; Avg propone tre diverse

tipologie di scansione (Intero Pc, file e cartelle specifiche, e un'analisi per scovare i rootkit). Inoltre aggiunge al browser un plug-in che verifica la sicurezza dei siti Web e offre altre funzioni di utilità come la pulizia delle tracce della navigazione.

- **BITDEFENDER:** l'antivirus di orige romena è nata all'inizio dello scorso decennio ma ha conquistato rapidamente quote di mercato interessanti, grazie agli ottimi risultati conseguiti nei test. Una volta installato, il programma effettuerà una rapida scansione iniziale del sistema, per verificare che non sia già compromesso. Una volta completato il setup, l'antivirus dovrà scaricare gli ultimi aggiornamenti al database delle firme. L'impostazione del programma è piuttosto diversa rispetto a quella degli altri prodotti di questo settore: mostra soltanto un semplice pannello popup, che indica lo stato della protezione, la data dell'ultimo aggiornamento, e un paio di switch per attivare o disattivare la protezione in tempo reale e la scansione. Nel complesso si tratta di un'ottima soluzione per proteggere il computer dai malware, ma manca di tutte le funzioni accessorie che invece sono patrimonio comune nella maggior parte dei concorrenti.