MALWARE

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 dalle parole inglesi **mal**icious e soft**ware** e significa "programma malvagio".

MALWARE

Nell'uso comune il termine virus viene utilizzato come sinonimo di malware.

Gli antivirus si sono evoluti e permettono di rilevare e rimuovere varie categorie di software maligno oltre ai comunemente detti virus.

MALWARE

Alcuni motivi per cui vengono creati:

- creare danni ai computer
- rubare dati sensibili
- bloccare l'attività di un'impresa
- intasare le caselle di posta elettronica

MALWARE

La diffusione di tali software risulta in continuo aumento.

Nel solo 2008 su Internet sono girati 15 milioni di malware, più di quelli contati nei 17 anni precedenti.

Nel 2012 sono circa 100 milioni.

MALWARE

Sorgente: Microsoft Security Intelligence Report,
Panda Security, Consumer Reports
Data di verifica: 07/11/2012

Statistiche Virus in USA	Valori
Famiglie che hanno avuto problemi seri di spam	24 milioni
Famiglie che hanno avuto problemi seri di virus negli ultimi 2 anni	16 milioni
Famiglie che hanno avuto problemi seri di spyware negli ultimi 6 mesi	8 milioni
Famiglie a cui è stato rubato del denaro anche tramite phishing	1 milione
Costo stimato per risolvere problemi di virus	4,55 miliardi di dollari
Famiglie colpite da virus	40%
Virus più diffuso per numero di infezioni	“Conficker Virus” 9 milioni

MALWARE

Sorgente: Microsoft Security Intelligence Report, Panda Security, Consumer Reports
Data di verifica: 07/11/2012

Virus per tipologia	Percentuali
Virus generici	57%
Misc. Trojans	21%
Trojan downloaders and droppers	7%
Software dannosi non catalogati	4%
Adware	4%
Exploits	3%
Worms	2%
Spyware	2%
Backdoors	1%

MALWARE

Quali sono i sintomi:

Il PC rallenta. Alcuni programmi cessano di funzionare. L'antivirus non si aggiorna. Escono messaggi d'errore. Si aprono siti non richiesti. Riceviamo posta indesiderata. Ci avvertono di aver ricevuto da noi email contenenti virus che non ci risultano.

MALWARE

Virus

Si nascondono all'interno di altri programmi, o nel disco fisso e si avviano ogni volta che il file infetto viene aperto.

Si trasmettono da un computer a un altro, ad opera degli utenti, tramite la copia di file infetti.

MALWARE

Worm

Si diffondono tramite email o sfruttando dei difetti (bug) di alcuni programmi e modificano il sistema operativo in modo da essere eseguiti automaticamente.

Agiscono rallentando il sistema con operazioni inutili o dannose.

MALWARE

Trojan horse

Si nasconde all'interno di un programma apparentemente utile. È l'utente che installando e/o eseguendo quel programma, inconsapevolmente, installa anche il software dannoso.

Non si autoreplicano e quindi devono essere deliberatamente inviati alla vittima.

MALWARE

Backdoor

Consentono ad un utente esterno di prendere il controllo remoto della macchina senza autorizzazione.

Sono creati da cracker intenzionati a manomettere il sistema o si diffondono in abbinamento a worm o trojan.

MALWARE

Spyware

Costituiscono una minaccia per la privacy dell'utente perché raccolgono, senza il suo consenso, informazioni riguardanti l'attività online (siti visitati, acquisti in rete), ma anche dati riservati (email, password, ecc.).

MALWARE

Dialer

Vengono utilizzati, a insaputa dell'utente, per modificare il numero telefonico di chi utilizza una connessione analogica o isdn con uno a tariffazione speciale con costo al minuto molto elevato.

MALWARE

Hijacker

Questi programmi si appropriano di applicazioni di navigazione in rete (browser) e causano l'apertura automatica di pagine Web indesiderate.

MALWARE

Rootkit

Sono copie modificate di programmi di sistema. Hanno la funzione di nascondere, sia all'utente che a programmi antivirus, la presenza di spyware e trojan.

MALWARE

Rabbit

Sono programmi che, creando velocemente copie di sé stessi, esauriscono le risorse del computer riempiendo la memoria RAM o il disco rigido.

MALWARE

Adware

Aprono continuamente finestre popup contenenti messaggi pubblicitari.

Creano rallentamenti del pc e rischi per la privacy in quanto inviano ad un server su internet le abitudini di navigazione dell'utente.

MALWARE

Batch

Sono i cosiddetti "virus amatoriali" e non sono rilevati dagli antivirus. Vengono inviati via email e deve essere l'utente ad aprirli. Per proteggersi basta eliminare i messaggi con file allegati di cui non si conosce la provenienza .

MALWARE

Keylogger

Sono in grado di registrare tutto ciò che l'utente digita sulla tastiera rubando i dati sensibili. Vengono installati sul computer dai trojan o dai worm o da persone che accedono al pc dell'utente attraverso internet.

MALWARE

Rogue antispyware

Rilevano falsi virus spingendo gli utenti ad installarlo e successivamente acquistare la licenza del programma.

MALWARE

Phishing

Frode online che usa e-mail, identiche a quelle di istituzioni note al destinatario (banche, poste, visa, ecc.), che rimandano ad un falso sito Web per estorcere i dati di accesso al conto corrente o della carta di credito.

MALWARE

Spam

Sono messaggi email che non sono stati in alcun modo richiesti.

Sono conosciuti anche come "e-mail commerciali non richieste" oppure come "mail spazzatura".