



# Cybersecurity I – I Virus informatici

Spesso si sente parlare di ransomware, malware, trojan ma da dove sono nati e come si sono sviluppati i **virus informatici**? Se ne parla spesso perché sono uno dei mezzi più utilizzati per veicolare attacchi informatici e commettere crimini sfruttando il mondo digitale. Sappiamo tutti quanto nel mondo di oggi questi attacchi siano frequenti, anzi, ormai possiamo dire di averci fatto l'abitudine.

## UN PO' DI STORIA

La storia dei virus si intreccia con la storia dell'informatica e, fin dai suoi inizi, viaggia di pari passo con la storia di Internet. Infatti è proprio per mezzo dell'antenato di Internet, Arpanet, la rete a uso militare e universitario sviluppata negli Stati Uniti, che inizia a circolare un programma capace di attivarsi da sé, di eseguire alcune operazioni in automatico e, sempre in automatico, di spostarsi verso un diverso nodo collegato in rete. Nel **1971** nasce **Creeper**, ovvero quello che è considerato il primo worm della storia; si tratta di un virus dimostrativo e abbastanza innocuo che oltre ad autoreplicarsi, caratteristica principale dei worm, visualizza sullo schermo una frase che schernisce l'utente.

È però negli **anni '80** che si assiste a una prima vera diffusione dei virus, favorita dalla vendita di volumi crescenti di dispositivi informatici e dallo sviluppo dei software; viene anche utilizzato nel 1983 per la prima volta il termine virus in contesto informatico. In quegli anni i virus si diffondono principalmente per mezzo di floppy disk, due esempi famosi sono **Elk Cloner** e **Brain**. Quest'ultimo, dopo aver infettato il sistema, mostra a video la frase "Beware of this VIRUS.... Contact us for vaccination" riportando i contatti di un negozio di computer a Lahore in Pakistan; i proprietari del negozio lo avevano sviluppato inizialmente come strumento anti pirateria non immaginando che si sarebbe presto diffuso a livello

internazionale.

Gli **anni '90** sono una pietra miliare della storia dei virus, sia per la rapida diffusione dei computer, diventati ormai un prodotto commerciale, dei loro sistemi operativi e dei relativi software, sia per l'evento che segnerà per sempre l'era moderna, la **nascita di Internet**, che tra le altre cose dà il via a un fenomeno di massa che rende estremamente facile diffondere trojan, worm e malware di ogni tipo. All'inizio degli **anni 2000** la posta elettronica diventa un terreno estremamente fertile perché permette di colpire l'anello più debole della sicurezza informatica: l'inconsapevole utente.

Un esempio celebre è **ILOVEYOU**, un virus che in un tempo estremamente rapido infetta milioni di computer in tutto il mondo attraverso messaggi apparentemente innocui aventi come oggetto "ILOVEYOU" inviate da conoscenti o amici: appena aperto l'allegato, il worm invia una copia di se stesso a tutti i contatti presenti nella rubrica. Questo virus è particolarmente interessante perché sfrutta modalità utilizzate ancora oggi: abbina allo sfruttamento (exploit) di una **vulnerabilità**, che in questo caso consentiva l'esecuzione automatica degli allegati, a tecniche di **ingegneria sociale** per ingaggiare gli utenti ad aprire l'allegato e assicurarsi la sua propagazione.

## COSA SUCCEDDE OGGI?

Oggi la situazione è molto più complessa e i virus vengono sfruttati anche dagli Stati per portare avanti azioni di spionaggio o vera e propria guerra cibernetica (Cyber Warfare). Un caso studio particolarmente interessante è il virus **Stuxnet**, un trojan che si diffonde nel **2010** sui sistemi industriali Iraniani per l'estrazione dell'uranio a partire da un aggiornamento software distribuito attraverso una chiavetta USB infetta.

Altri malware interessanti e attuali sono i **Ransomware** tra cui ricordiamo **Cryptolocker**, comparso nel **2013** e diffuso via Internet, che permette agli attaccanti di criptare tutti i dati contenuti in un disco fisso per chiedere un riscatto in cambio del codice di sblocco. Anche **WannaCry**, che presenta caratteristiche simili a Cryptolocker, ha colpito oltre 230 000 computer in tutto il mondo, rendendolo uno dei maggiori contagi informatici mai avvenuti.

## E IN FUTURO?

Una cosa è certa: gli attacchi informatici non diminuiranno nel prossimo futuro, anzi probabilmente aumenteranno. Basti pensare all'avvento dell'Internet of Things: le possibilità che questi device semplici e iperconnessi offrono agli sviluppatori di software malevolo sono enormi; inoltre siamo perennemente connessi alla rete e dipendiamo fortemente dai sistemi informatici per numerose attività in ambito professionale e privato.

È quindi fondamentale dedicare sempre maggiore **attenzione alla sicurezza** informatica: è importante acquisire questa **consapevolezza** fin dalle scuole per poter essere cittadini consapevoli del mondo digitale e imparare ad adottare comportamenti sicuri, a partire dall'attenzione alle password, agli aggiornamenti di sicurezza dei nostri device e alla cautela nell'interazione con siti web o email sospette.

## APPROFONDIMENTI

- <https://www.wired.it/internet/web/2021/02/20/creeper-primo-worm-informatica-cybersecurity/>
- <https://www.cybersecurity360.it/nuove-minacce/ransomware/ransomware-cose-come-rimuoverlo-e-come-difendersi/>