WannaCry: il malware che ha quasi infettato tutto il mondo

I CONSIGLI DELLO YOUTUBER

DI MARCO AGNESE

21/04/2026

SICUREZZA INFORMATICA | PRIMO BIENNIO

LICEO, TECNICO



In questo video Marco, studente di ingegneria, spiega che cos'è WannaCry, come si è diffuso e perchè aggiornare il computer è fondamentale per la sicurezza.

Quando compare l'avviso di aggiornare il sistema operativo, spesso la tentazione è rimandare. Sembra una seccatura da poco, ma proprio questa abitudine ha favorito nel 2017 la diffusione di **WannaCry**, uno dei malware più pericolosi degli ultimi anni.

Il termine **malware** nasce dall'unione delle parole inglesi *malicious* e *software* e indica un programma progettato per infiltrarsi in un dispositivo, danneggiarlo o compromettere i dati dell'utente. WannaCry era un malware "ibrido": agiva sia come **worm**, cioè capace di diffondersi automaticamente in rete da un computer all'altro, sia come **ransomware**, perché cifrava i file della vittima chiedendo un riscatto per sbloccarli. L'attacco è stato attribuito al **Lazarus Group**, gruppo di hacker legato alla Corea del Nord.

La diffusione fu possibile grazie a una vulnerabilità di Windows chiamata **EternalBlue**, sottratta e pubblicata online nel 2017. Microsoft rilasciò una correzione, ma molti utenti non installarono l'aggiornamento. Così, il **12 maggio 2017**, WannaCry iniziò a propagarsi rapidamente, infettando in poco tempo centinaia di migliaia di computer in oltre 150 Paesi. Tra i bersagli ci furono ospedali del sistema sanitario britannico, grandi aziende internazionali come **Deutsche Bahn**, **FedEx** e **TSMC**, e in Italia anche l'**Università Bicocca di Milano**, seppure in modo marginale.

Uno degli aspetti più sorprendenti di questa vicenda riguarda il modo in cui il malware fu fermato. Nel suo codice era presente un **kill-switch**, una sorta di interruttore nascosto. A scoprirlo fu **Marcus Hutchins**, giovane ricercatore britannico, che notò un collegamento verso un dominio web non registrato e decise di attivarlo. Questo gesto bloccò la diffusione del virus e limitò i danni nei giorni successivi.

Il caso WannaCry dimostra in modo molto concreto che aggiornare il sistema operativo non è un fastidio inutile, ma una forma essenziale di protezione. Dietro un semplice clic rimandato possono nascondersi conseguenze enormi, non solo per i singoli utenti ma anche per ospedali, aziende e servizi fondamentali.

Il video

WannaCry: il malware che ha quasi infettato tutto il mondo



Autori



MARCO AGNESE

Studia Ingegneria Informatica e ha un canale YouTube molto seguito. Nei suoi video affronta temi relativi alla tecnologia e alla vita da studente universitario.