Esercitazione W14D1 - Pratica 2

Infezione malware

Fabio Benevento - 07/02/2024

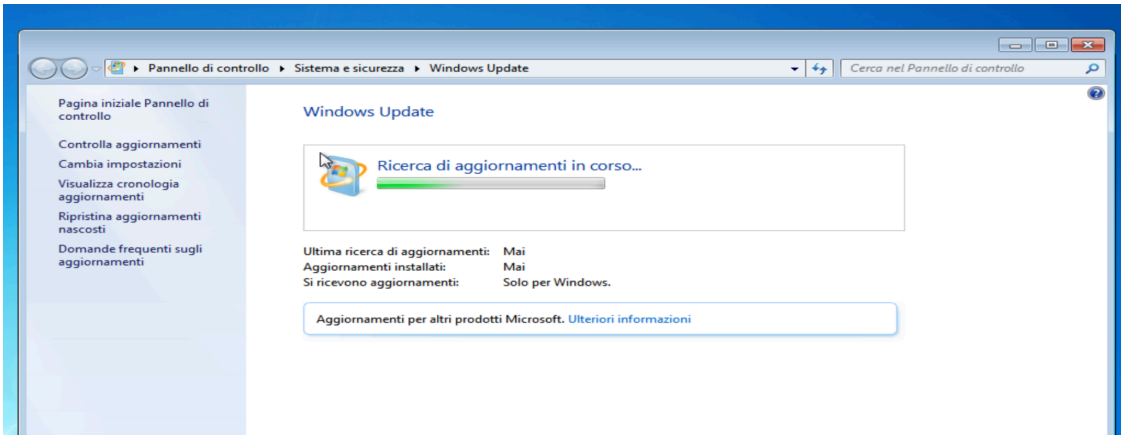
Traccia

Hai appena scoperto che l'azienda che segui come consulente di sicurezza ha un computer con Windows 7 è stato infettato dal malware WannaCry.
Cosa fai per mettere in sicurezza il tuo sistema? Descrivere le attività solte tenendo conto che:

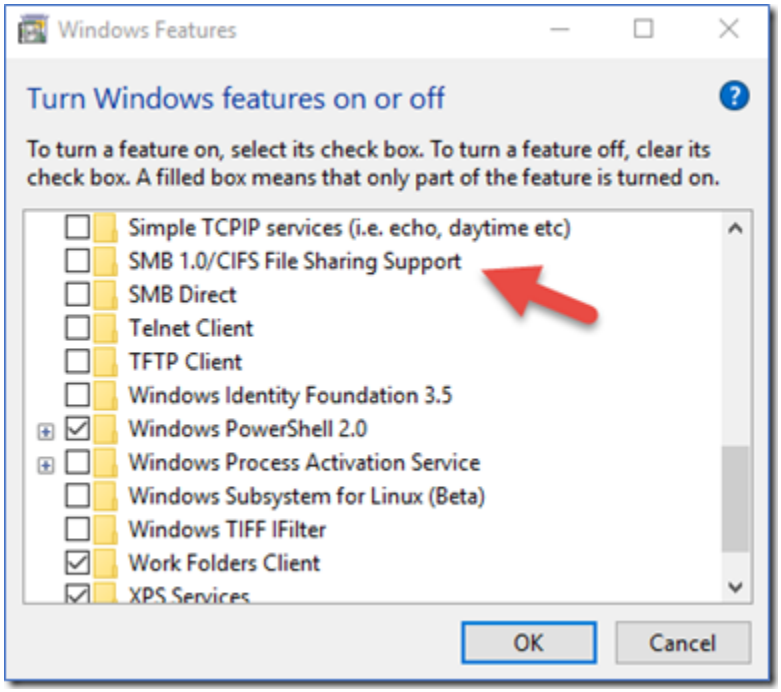
- Per prima cosa occorre intervenire tempestivamente sul sistema infetto
- In seguito, preparare un elenco delle varie possibilità di messa in sicurezza del sistema
- Per ogni possibilità valutare i pro e i contro

Implementazione

In caso di sistema Windows 7 infettatto dal malware WannaCry, una volta isolato il computer dalla rete interna in maniera tale da evitare che il virus si diffonda, è bene come prima cosa procedere con un aggiornamento del sistema agli ultimi update.
Per fare ciò è necessario verificare la disponibilità di aggiornamenti in Windows Update e nel caso procedere con gli aggiornamenti.



Il ransomware WannaCry sfrutta nello specifico una falla del protocollo SMB version 1. Come remediation per maggiore protezione è possibile quindi disabilitare in Windows 7 il supporto a SMBv1 accedendo alla voce “Turn Windows feature on or off” dal menù Start e spuntando la voce SMB 1.0/CIFS File Sharing Support



Infine è possibile applicare alcune regole generiche per il mitigare le vulnerabilità, ovvero l’esecuzione periodica di un software antivirus alla ricerca di malware e la modifica periodica della password con requisiti di complessità ai fini da rendere difficile l’individuazione delle credenziali.