WannaCry è un **ransomware**, un particolare tipo di malware che rende inaccessibili i dati dei nostri computer e chiede un riscatto da pagare in bitcoin, per la decodifica. Il malware colpisce chi ha il proprio computer collegato alla Rete e ha un sistema operativo **Windows** (dato che il software malevolo si propaga grazie a EternalBlue, uno strumento che sfrutta la vulnerabilità di un protocollo di condivisione di file di rete, **SMB** --Server Message Block--, usato da sistemi Microsoft Windows).

Inizialmente, si pensava che il vettore d'attacco originario fosse la posta elettronica. Successivamente, però, la tesi più accreditata è che il malware si diffonda **attraverso computer vulnerabili esposti su internet con la porte 139 e 445**. Una volta che un solo computer di una rete locale viene infettato, il malware automaticamente si propaga usando il protocollo SMB.

La peculiarità originale di WannaCry è che si tratta di un malware costituito da due componenti che operano in successione:

1. Un exploit che sfrutta la vulnerabilità SMBv1 per attaccare il computer obbiettivo.
2. Un ransomware vero e proprio che esegue la cifratura dei files usando una crittografia RSA a 2048 bit

WannaCry provvede inoltre ad eliminare le "Shadows copies" di Windows e va a scrivere in alcune tipiche cartelle di sistema, quali:

- %SystemRoot%
- %SystemDrive%
- %ProgramData%.

Il ransomware è in grado di diffondersi ed installarsi su ogni pc presente sulla rete che abbia la port a139 o 445 aperta, quindi, per arginare il problema, prima di tutto, scolleghiamo il pc infetto dalla rete e blocchiamo le porte 139 e 445 in tutta la rete tramite firewall, o cambiare la porta usata per il protocollo RDP.

Pagare il riscatto non e' mai una sicurezza per riavere il proprio pc, spesso, dopo il pagamento, nonviene decifrato il contenuto del pc.

Per "liberare" il pc infetto e poter leggere i vari file compromessi, l'unica maniera è affidarci al software WanaDecrypt che cercherà di decifrare la cifratura di wannacry in base ai dati raccolti sugli attacchi del passato.

Per prevenire gli ipotetici attacchi, si suggerisce di tenere sempre aggiornato il software windows (anche se spesso non e’ possibile)