Rimozione malware: WannaCry Ramsonware

Per la messa in sicurezza del sistema infetto come prima cosa bisogna capire in a quale scenario siamo sottoposti: se il malware è stato attivato o se sia dormiente. Nel secondo caso sarebbe giusto togliere immediatamente il pc dalla rete in cui si trova in quanto WannaCry cerca di infettare automaticamente gli host connessi alla rete del sistema infetto. A questo punto si potrebbe pensare di scansionare il pc con un apposito antivirus/antimalware per la rimozione.

Nel caso in cui invece WC sia stato attivato possiamo come prima soluzione quella di pagare il riscatto per liberare il sistema. Ovviamente questa soluzione non è sicuramente la migliore (unico pro sarebbe la rapidità con cui si mitiga il problema) in quanto si pagherebbe una cifra alta senza la sicurezza che il computer venga “liberato” da WC.
Quello che si potrebbe fare invece è attenersi alle linee guida dei report di analisi eseguiti da vari ricercatori. Si potrebbero usare dei tool di decrittazione come WanaKiwi o WannaKey per poter recuperare i propri dati e poi eliminare il malware con un apposito software.

Altrimenti se si ha un punto di ripristino del sistema si potrebbe manualmente (tramite safe mode di windows) creare il processo che porta al “system restore” di windows tramite riga di comando. A questo punto si ripristina il sistema e si esegue una scansione per verificare che non ci siano residui di WannaCry nel sistema. Queste ultime due ipotesi sono le migliori in termini di sicurezza anche se sicuramente sarebbe più laborioso rispetto al pagamento del riscatto.