Negli ultimi anni continua ad evolversi senza sosta l'evoluzione di ransomware, malware atti a estorcere denaro in seguito ad un crittografia asimmetrica di file all'interno del sistema infetto.

Lo scopo principale dell'attacco è quello di chiedere un riscatto sui file presenti nel sistema, semplicemente prendendoli in ostaggio tramite una cryptazione con chiave asimmetrica. I file così indecifrabili sono alla merce dei "sequestratori" che tramite delle istruzioni ben dettagliate, guidano la vittima sulle procedure da seguire per pagare il riscatto ed ottenere la key necessaria a decyptare i file.

La diffusione del malware ha compito principalmente gli utenti finali, ma purtroppo si è diffuso anche sui terminali di professionisti, aziende e Pubbliche amministrazioni, creando un danno per miglia di euro, oltre a paralizzare intere amministrazioni o peggio chiudere le attività per la perdita di dati. Non tutti hanno ceduto al pagamento del riscatto, provando a recuperare i dati ma senza risultato portando alla definitiva perdita degli stessi.

Andiamo al punto di questo articolo.

Da una prima analisi, possiamo apertamente supporre che la diffusione di questo malware sia qualcosa di dannoso, atto ad arrecare un danno alla vittime e recuperare soldi per finanziare gli estorsori e creatori del malware.

Ma da un analisi alternativa, possiamo supporre che se le vittime dell'infezione se avessero avuto l'accortezza di creare dei backup dei propri file, adesso non avrebbero il problema di pagare un riscatto per poter recuperare i propri file.

Esatto, se tutti quanti avessero avuto dei backup su dei supporti esterni, sicuramente il danno sarebbe minimo o nullo, al massimo perdere qualche file delle ultime ore, ma niente di più, invece? Purtroppo la facilità di diventare "informatici" e di avere un accesso alla tecnologia con una certa facilità, ci ha fatto cullare, fidandoci di queste apparecchiature elettroniche e affidando loro tutta la nostra vita personale e il nostro lavoro.

Sicuramente oggi la semplicità di avere storage e device di stoccaggio esterni, sistemi di cloud e quant' altro ci potrebbero dare una certa flessibilità nella scelta del backup e sulla loro procedura di contenimento, con relative policy di mantenimento e detenzione. Quindi, perchè questo malware è così temuto? Eppure dovrebbe essere semplice poter attutire al suo

passaggio, invece?

Invece no! perchè siamo incoscienti, ignoranti ed incapaci.

I backup non sono necessari, o peggio vengono fatti ma mai verificati. I file, anche se importanti vengono tenuti sui pc o server, e al massimo vengono copiati su un server con accesso su condivisione file.

Ecco come tutte queste mancanze o incapacità fanno si che questo malware diventi temuto da tutti.

Quindi, riponiamo nuovamente la domanda: I ransomware sono così pericolosi?

I ransomware è sicuramente una famiglia di malware che non va sottovalutata, e le ultime versioni sono sempre più sofisticate, ma una buona cultura informatica, sopratutto nelle aziende, e delle corrette policy di backup & recovery possono fare la differenza nella prevenzione da questi malware.