VareseNews

Ransomware, attacchi informatici e recupero dati su un hard disk

Pubblicato: Lunedì 24 Gennaio 2022

La **sicurezza informatica** è un tema assolutamente centrale nel dibattito odierno. Lo sviluppo di nuove tecnologie, la digitalizzazione di molti servizi ha avuto come conseguenza anche una maggiore esposizione alle minacce informatiche.

Vedremo in particolare il problema dei **ransomware**. Malware la cui diffusione è cresciuta in modo importante negli ultimi anni. Un problema che riguarda sia il mondo delle aziende, che quello dei privati cittadini. Infine daremo qualche spunto sul **recupero dei dati dagli hard disk** colpiti da problematiche legate ai malware di questo tipo.

Vedi anche l'approfondimento su: attacco informatico, ecco che cosa fare.

Cosa sono i ransomware

Un ransomware è un particolare tipo di malware che fonde le parole ransom (riscatto) con appunto l'espressione malware.

Il nome ci permette già di intuire come agisce un ransomware. Il dispositivo della vittima diventa inaccessibile e con esso, ovviamente, anche tutti i dati e i file ivi presenti.

L'autore del ransomware (ne esistono di diversi tipi e gradi di "raffinatezza") in genere a questo punto richiede un riscatto alla vittima per restituirgli l'accesso al proprio PC o dispositivo infettato.

Il pagamento del riscatto stesso, nella maggior parte dei casi, è richiesto in criptovalute (Bitcoin o altre cripto). L'ammontare del pagamento, in molti di questi attacchi, non è elevatissimo. Per questo le vittime tendono in alcuni casi a procedere al pagamento.

Il saldo del riscatto ovviamente non è una garanzia dello sblocco del dispositivo. Alcuni di questi ransomware però sono così ben fatti che spesso non lasciano alternative al pagamento.

Alcuni esempi recenti di **ransomware tristemente famosi** sono i seguenti:

- Cryptolocker
- Virus CTB Locker
- Virus CryptoWall
- DearCry ransomware

Si tratta solo di alcuni nomi che sono saliti alla ribalta anche nel mondo giornalistico. Ma i tipi di ransomware e le relative varianti sono davvero tante e la produzione di questo tipo di malware è in costante evoluzione.

Vediamo però cosa si può fare se il proprio **hard disk è "bloccato"** e si vuole recuperare i dati senza cedere al riscatto.

Si possono recuperare i dati da dispositivo bloccato?

Il recupero dei dati su un device colpito da ransomware si presenta spesso come piuttosto complesso. Un primo consiglio è la **tempestività**. Attivarsi subito nel rivolgersi a **esperti** nel recupero dei dati sugli hard disk o su altri dispositivi.

Molti di questi malware non lasciano moltissimo tempo per decidere i da farsi (spesso il pagamento del riscatto è fissato a 2-3 giorni al massimo).

La fattibilità delle operazioni di recupero è strettamente legata al tipo di ransomware. Se si tratta di un applicativo rudimentale è possibile che presenti delle debolezze che consentano di superare il blocco.

L'estensione con la quale sono stati criptati i file ci può fornire qualche spunto in può sul tipo di malware in azione. Una falla nello stesso potrebbe consentire di recuperare la chiave di cifratura e vederci restituiti i nostri preziosi dati e file.

Una guida generale al recupero è impossibile in quanto i ransomware possono essere molto diversi gli uni dagli altri. Inoltre l'attività di contrasto in genere non può essere fatta home made, ma è fondamentale rivolgersi a dei professionisti (e farlo velocemente).

Gli ultimi consigli che vi diamo riguardano la prevenzione. Massima attenzione alle mail che si ricevono, a cosa si scarica e ai siti che andiamo a navigare. Dotarsi poi di un buon **antivirus** e tenerlo sempre aggiornato.

Redazione VareseNews
redazione@varesenews.it