# Pagare il riscatto dopo un attacco? Assolutamente no!

Da **Redazione BitMAT** - 12/05/2022

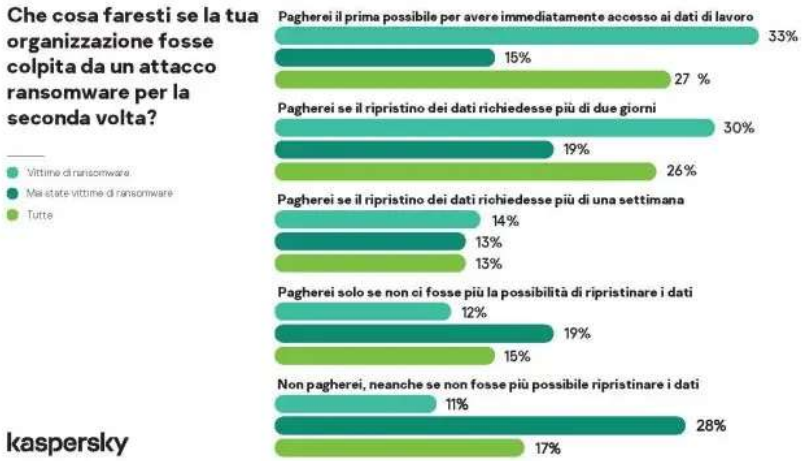
Secondo l'ultima indagine Kaspersky 1 azienda su 10 che ha subito un attacco ransomware preferisce pagare il riscatto. Ma non è la cosa giusta da fare.

Secondo quanto emerso dal nuovo report di **Kaspersky** "**How business executives perceive ransomware threat**", i dirigenti dell'88% delle organizzazioni che sono già state vittime di un attacco ransomware, sceglierebbero di pagare il riscatto se dovessero subirne un altro. Tra le organizzazioni che non sono ancora state vittime di ransomware, il 67% sarebbe disposto a pagare ma non subito. Sebbene i ransomware rimangano una delle minacce più diffuse, con due terzi (64%) delle aziende che hanno già subito un attacco, il pagamento del riscatto sembra essere percepito dai dirigenti come un modo sicuro di affrontare il problema.

La parola ransomware è ormai nota nel mondo aziendale soprattutto dopo i grandi attacchi alle imprese che recentemente sono stati protagonisti dei titoli dei giornali di tutto il mondo e dopo aver rilevato, nel 2021, un aumento del numero di attacchi che utilizzano i ransomware. A questo proposito Kaspersky ha indagato su come reagirebbero le aziende in caso di attacco e su come si comporterebbero di fronte alla possibilità di pagare un riscatto.

Secondo quanto emerso dal report, se un'organizzazione è stata vittima di ransomware in passato, è più propensa a pagare il riscatto in caso di nuovo attacco (88%). Queste aziende sono anche più propense a pagare il prima possibile per ottenere l'accesso immediato ai propri dati (33% delle aziende già attaccate in passato contro il 15% delle aziende che non sono mai state vittime), o a pagare

dopo un paio di giorni di tentativi di decriptazione non andati a buon fine (30% contro il 19%).




I dirigenti aziendali che hanno già pagato un riscatto sembrano ritenere che questo sia il modo più efficace per riavere i propri dati e il 97% di loro è disposto a farlo di nuovo. Questa disponibilità delle aziende a pagare potrebbe essere attribuita alla scarsa consapevolezza su come rispondere a tali minacce, o al troppo tempo necessario a ripristinare i dati, poiché l'attesa prolungata potrebbe far perdere loro molto più denaro di quello impiegato per pagare il riscatto.

I ransomware rimangono una minaccia reale per la sicurezza informatica. Due terzi (64%) delle aziende confermano di aver subito un incidente di questo tipo mentre il 66% prevede che prima o poi ne subirà uno simile, ritenendolo più probabile rispetto ad altri tipi di minacce come ad esempio attacchi DDoS, alle supply-chain, APT, cryptomining o cyberspionaggio.

*"La nascita di nuovi sample e l'utilizzo dei ransomware da parte di alcuni gruppi APT in attacchi avanzati li ha resi una minaccia molto seria per le aziende. Anche un'infezione accidentale può causare gravi danni e compromettere la continuità aziendale, ecco perché i dirigenti sono costretti a prendere decisioni difficili in merito alla possibilità di pagare il riscatto. Tuttavia, non è mai consigliabile inviare denaro ai criminali, in quanto ciò non garantisce la restituzione dei dati crittografati e incoraggia gli attaccanti a ripetere l'operazione. Noi di Kaspersky stiamo lavorando duramente per aiutare la comunità aziendale a evitare questo tipo di situazioni. È importante che le aziende seguano i principi di sicurezza di base e cerchino soluzioni di sicurezza affidabili per ridurre al minimo il rischio di un incidente ransomware. In occasione dell'Anti-Ransomware Day, vale la pena ricordare queste pratiche"*, ha dichiarato **Sergey Martsynkyan, VP, Corporate Product Marketing di Kaspersky.**

Ecco i passaggi chiave consigliati da Kaspersky per migliorare la protezione delle aziende contro i ransomware:

- Aggiornare regolarmente il software su tutti i dispositivi per evitare che gli attaccanti sfruttino le vulnerabilità e si infiltrino nella rete.

- Concentrare la strategia di difesa sul rilevamento di movimenti laterali e esfiltrazione dei dati verso internet. Prestare particolare attenzione al traffico in uscita per rilevare le connessioni dei criminali informatici alla rete aziendale.
- Creare backup offline che i criminali non possano manomettere e assicurarsi di potervi accedere rapidamente in caso di emergenza.
- Abilitare la protezione ransomware per tutti gli endpoint.
- Le aziende dovrebbero utilizzare soluzioni anti-APT e EDR in grado di scoprire e rilevare le minacce avanzate, indagare e rimediare tempestivamente agli incidenti e offrire l'accesso alle informazioni più recenti sulle minacce. Utilizzare un fornitore MDR in grado di rilevare in modo efficace agli attacchi ransomware avanzati.
- Mai pagare il riscatto. Non offre garanzie sul recupero dei dati e incoraggerà i criminali a continuare la loro attività. È necessario invece segnalare l'accaduto alle forze dell'ordine locali. È possibile trovare un decryptor all'indirizzo https://www.nomoreransom.org

**Redazione BitMAT**

*https://www.bitmat.it/*