Evoluzione ransomware: il riscatto si paga due (o tre) volte

Nov 05, 2020 Marco Schiaffino Attacchi, Gestione dati, In evidenza, Leaks, Malware, News, RSS, Scenario 0

Si moltiplicano i casi in cui gli estorsori, dopo aver incassato, minacciano di pubblicare i dati rubati se non ottengono ulteriori pagamenti.

Qualcuno ha davvero creduto che sia possibile di fidarsi di un criminale? Purtroppo la categoria degli ingenui (o dei disperati) è più ampia di quanto si possa credere, soprattutto quando si parla di estorsioni legate agli attacchi ransomware.

Come ripetono gli esperti di sicurezza, sono ancora troppe le vittime di questo genere di ricatti (soprattutto aziende) che decidono di cedere alle richieste dei pirati informatici e, sottolinea una nuova ricerca pubblicata su Internet da **Coveware**, la loro rimane una pessima idea.

I cyber criminali dediti a questo genere di attività, infatti, stanno diventando sempre più avidi e trovano il modo di "spremere" il più possibile le loro vittime, anche a costo di rompere quel "rapporto di fiducia" (se così possiamo definirlo) che lega vittima ed estorsore.

A cambiare le regole del gioco ci avevano pensato già i pirati del gruppo **Maze** (che ha annunciato una sorta di “addio alle scene” recentemente) modificando il loro modus operandi. Qualche mese fa.

Oltre a crittografare il contenuto dei computer compromessi, infatti, i membri di Maze hanno cominciato a esfiltrare i dati per poi minacciare di renderli pubblici nel caso in cui non venissero pagati.

Una tecnica che è stata prontamente adottata anche da altri cyber criminali, che hanno pensato bene di chiedere un doppio riscatto: uno per fornire la chiave di decodifica dei dati crittografati sui computer e uno per non divulgare i dati.

Tra questi anche il gruppo **Sodinokibi**, che in passato ha usato anche le multe del GDPR come “leva” per convincere le sue vittime a pagare.

Ora, però, i pirati hanno abbandonato ogni ritegno e non rispettano nemmeno più i patti. Nel report, infatti, vengono citati casi in cui l’estorsione è stata riproposta dopo poche settimane e altri in cui i dati oggetto della contrattazione

sono stati pubblicati nonostante il pagamento del “riscatto”.

Insomma: chi non ha preso sul serio gli avvertimenti degli esperti e delle forze di polizia, che ripetono da sempre quanto sia pericoloso cedere alle richieste dei criminali, lo ha pagato caro. Speriamo per lo meno che questi casi possano servire come esempio.

Condividi l’articolo

RegretLocker: ecco il ransomware specializzato in macchine virtuali

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/11/05/evoluzione-ransomware-il-riscatto-si-paga-due-o-tre-volte/?utm_source=rss&utm_medium=rss&utm_campaign=evoluzione-ransomware-il-riscatto-si-paga-due-o-tre-volte