PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 24 - numero 5163 di Venerdì 13 maggio 2022

# Dalle WMD alle WMI: i malviventi stanno cambiando gli strumenti di attacco

***Dalle armi di distruzione di massa alle armi di interruzione di massa: il numero crescente di attacchi per ransomware dimostra come i malviventi stiano modificando gli strumenti e le metodologie di attacco.***

Tutti ricordiamo come uno dei motivi principali per cui gli Stati Uniti invasero l'Iraq discendeva dal fatto che, sempre secondo gli Stati Uniti, esistevano prove certe del fatto che Saddam Hussein stesse mettendo a punto delle armi di distruzione di massa (WMD-weapons of mass destruction).

La progettazione e produzione di queste armi è cosa oltremodo complessa e solo pochi paesi al mondo hanno le competenze e le risorse per svilupparle.

Lo scenario però cambia in modo drammatico quando, invece di prendere in considerazione le WMD, si prendono in considerazione le WMI, vale a dire le armi di interruzione di massa.

Tra queste armi rientrano certamente tutti gli applicativi, alla base della richiesta di riscatti, per accedere ai dati, i cosiddetti ransomware.

Recentissima è la notizia che alcuni ospedali milanesi sono stati attaccati con questi applicativi, che hanno impedito l'accesso ai dati sanitari di molti pazienti, sia on-line sia con altre modalità.



Forse con un certo ritardo, gli esperti di sicurezza informatica sono riusciti a convincere i dirigenti aziendali dal fatto che lo strumento più efficace per proteggersi da queste nuove armi di interruzione di massa è attivazione di appropriati programmi di prevenzione e, soprattutto, di programmi di regolare backup di tutti i dati e programmi aziendali, in modo da neutralizzare le richieste di riscatto, motivate dalla impossibilità di accedere ai dati aziendali.

A conferma di questo atteggiamento, è stato recentemente pubblicato uno studio sull'incremento di vendite delle apparecchiature, su disco o nastro, di backup dei dati.

Secondo questa recentissima ricerca, il mercato del backup dei dati e degli strumenti di recovery è cresciuto dai 7, 3 miliardi di dollari nel 2017 agli 11, 59 miliardi di dollari nel 2022, con una crescita composita annuale del 10%.

Le situazioni che hanno portato a questo rapido incremento del mercato fanno riferimento alla crescente di quantità di dati raccolti dalle aziende, alla necessità di proteggersi da possibili attacchi e ad un costante miglioramento della qualità dei dati stessi. Al contempo, anche l'adozione di soluzioni di backup, ospitate nel cloud, contribuisce all'incremento di questo mercato.

Sembra che finalmente molte aziende si stiano convincendo che una politica di regolare e sicuro backup dei dati trattati rappresenti forse il più efficiente ed efficace strumento di prevenzione di attacchi per ransomware.

La disponibilità di copie di backup dei dati ed applicazioni, costantemente aggiornata, sia su supporto fisico, sia mediante archiviazione nel cloud, rappresenta oggi non solo un ragionevole atteggiamento di prevenzione, da parte delle aziende, ma soprattutto un indispensabile strumento di contrasto della criminalità informatica.

Non per nulla, un'analisi delle vittime di questi attacchi e delle richieste di riscatto mette in evidenza come una lacuna sul piano della effettuazione di regolari ed affidabili backup di dati e programmi rappresenta la debolezza principale, che sfruttano i malviventi per perpetrare i loro attacchi.

Il messaggio conclusivo è semplice: alcuni terabyte di prevenzione valgono bene, a fronte del pagamento di un ingente riscatto!

**Adalberto Biasiotti**



**www.puntosicuro.it**