ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4700 di Lunedì 18 maggio 2020

Gli attacchi con ransomware diventano sempre più sofisticati

Negli ultimi tempi si sono moltiplicati gli attacchi con ransomware e le tecnologie utilizzate dai malviventi hanno compiuto un salto di qualità. Ecco la situazione attuale.

I lettori sono certamente al corrente del funzionamento degli attacchi con ransomware, almeno fino a poco tempo fa.

Il malvivente informatico riesce a introdursi nel sistema informativo di un bersaglio e carica un applicativo, che cripta tutti i dati archiviati sull'hard disk, rendendo l'accesso impossibile a chi non dispone della chiave di decifratura.

Indi il malvivente invia un messaggio al proprietario del computer, informandolo che metterà a disposizione la chiave di decifratura solo se verrà pagata una certa somma, utilizzando la tecnica non tracciabile dei bitcoin. Chi scrive ha conosciuto diverse aziende che sono rimaste vittime di questa tipologia di attacchi, che trova la sua forza nel fatto che spesso le aziende non hanno provveduto ad effettuare una regolare duplicazione dei dati, su una copia di backup. Se infatti è disponibile una copia aggiornata di backup, il soggetto attaccato può rifiutarsi di pagare il riscatto, in quanto ha la possibilità di ricostruire comunque i dati bloccati.

Per dare un'idea dell'ordine di grandezza del riscatto che viene richiesto, stiamo parlando, in funzione della dimensione dell'azienda, di somme in bitcoin equivalenti a importi variabili da 100.000 fino a 2 milioni di euro. Questi attacchi sono presenti sulla scena del crimine informatico già da diverso tempo e molte aziende si sono finalmente attivate, adottando con misura precauzionale, d'altronde sacrosanta, una copia sistematica dei dati aziendali. Se poi vi sono due copie, tanto meglio!

A questo punto i malviventi informatici hanno compiuto un salto di qualità, perché, almeno nelle ultime versioni identificate dagli specialisti, gli attaccanti non solo possono rendere inaccessibili i dati con applicativi crittografici, ma provvedono anche a copiarli. Ad esempio, nel novembre 2019, un attacco ransomware contro una grande azienda americana di guardie particolari giurate, ha registrato una evoluzione di questa tipologia di attacco, che viene chiamata "doppia estorsione". Dopo che l'azienda è stata attaccata da un ransomware tipo Maze ed ha rifiutato di pagare un riscatto di 2, 3 milioni di dollari, gli attaccanti hanno minacciato di rendere pubblici dati particolari, che erano stati estratti dalla banca dati, nonché indirizzi di posta elettronica ed altri elementi, da utilizzare per avviare una campagna di spam apparentemente originata da questa stessa azienda. Per confermare la validità dell'attacco, i malviventi hanno diffuso 700 MB di dati, vale a dire circa il 10% di quelli effettivamente sottratti, contenenti tracce di contratti, anamnesi mediche, e altri dati oltremodo critici. In parallelo alla diffusione di questi dati, i malviventi hanno innalzato il livello del riscatto del 50%. Dopo questo primo attacco di nuova generazione, i malviventi si sono ulteriormente evoluti, perché hanno addirittura creato un sito Web dedicato, che elenca i nomi delle aziende che sono state attaccate e che hanno rifiutato di pagare il riscatto. Su questo sito vengono pubblicati dati, sottratti dagli attaccanti, a riprova del fatto che l'elenco pubblicato è realistico.

Accedendo a questo sito, si trovano i nomi di dozzine di aziende, studi legali, studi medici e compagnie di assicurazione, vittime di questa nuova tipologia di attacco informatico. Anche altri criminali informatici si sono allineati in questa strategia di aumento della pressione sul soggetto colpito, creando un altro sito, chiamato "Happy blog", dove sono stati pubblicati dettagli di 13 aziende attaccate, con un campionario di informazioni sottratte.

Tra i tanti soggetti attaccati, uno che ha rivelato pubblicamente quanto accaduto e l'azienda TXXX, che gestisce transazioni finanziarie legate a viaggi. L'azienda ha rivelato di aver pagato 2, 3 milioni di dollari in bitcoin per recuperare il pieno possesso dei dati ed evitare che essi venissero pubblicati abusivamente.

Tutti gli esperti sono convinti che questa tipologia di attacco, chiamata "doppio ricatto", continuerà a svilupparsi rapidamente nel 2020, colpendo in particolare le strutture sanitarie, che non solo raccolgono dati sensibili legati alla salute, ma che costituiscono anche bersaglio preferenziale in questa situazione pandemica.

A questo proposito, vi è da dire che purtroppo il mondo della sanità, già da decenni, ha dimostrato di essere assai poco preparato a fronteggiare situazioni di crisi informatica e quindi rappresenta un bersaglio particolarmente vulnerabile.

Ancora una volta, si ricordano alle aziende le principali misure da adottare per mitigare questo rischio:

- effettuare regolarmente e frequentemente copie di tutti i dati utilizzati,
- avviare un programma di educazione dei dipendenti nel gestire i messaggi di posta elettronica sospetti ed altri tentativi di intrusione dal Web,
- aggiornare tutte le protezioni informatiche esistenti all'ultima versione, ed infine
- utilizzare strategie di difesa a più livelli.

Adalberto Biasiotti