PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 18 - numero 3816 di martedì 05 luglio 2016

Ransomware: sapete cos'è?

Un nuovo temibile attacco dei criminali informatici sta ormai colpendo numerose aziende, con conseguenze potenzialmente assai gravi. Di Adalberto Biasiotti.

Cominciano ad essere ormai numerose le aziende ed altre entità, dotate di strutture informatiche, che vedono compromesso l'accesso alla propria base dei dati, perché i malviventi hanno messo a punto una tipologia di attacco informatico particolarmente sofisticata.

Con varie metodologie, ormai ben descritte nella letteratura di settore, i malviventi ottengono un accesso illecito al sistema informatico e scaricano un applicativo, che provvede a criptografare l'intera base dei dati, rendendola inaccessibile al soggetto colpito.

Uno dei più celebri applicativi fraudolenti di questo tipo si chiama appunto Cryptolocker. Il responsabile del sistema informativo, che si vede impedito l'accesso ai dati, riceve un messaggio di posta elettronica, nella quale il criminale informatico gli propone di pagare un riscatto, ricevuto il quale egli potrà avere una chiave, che permette di decifrare i dati criptografati.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[AP1002] ?#>

Il pagamento deve avvenire in bitcoin, vale a dire una moneta elettronica che non è tracciabile e protegge quindi l'identità dei malviventi informatici.

Un recente studio di mercato ha dimostrato come l'incremento di questi attacchi sia oltremodo elevato e le somme che vengono richieste e purtroppo ottenute dai malviventi continuano a crescere.

Ad esempio, un ente sanitario americano nel febbraio 2016 ha dovuto pagare 17.000 dollari di bitcoins per rendere nuovamente accessibile la propria banca dei dati.

Ormai i maggiori esperti mondiali dichiarano il 2016 come l'anno in cui l'estorsione digitale raggiungerà un picco.

Ebbene inoltre sottolineare che non sono le grandi aziende possono rimanere vittime di questo attacco, ma anche piccole e piccolissime aziende, cui si chiede un riscatto proporzionalmente più basso.

Ho avuto esperienza diretta di questa situazione, quando il sistema informatico di un libero professionista, a me noto, è stato infettato da questo virus e, su consiglio del suo esperto informatico, egli ha pagato 400 dollari di bitcoins per ottenere la chiave di decodifica.

Le esperienze raccolte in varie parti del mondo confermano inoltre che i criminali in questione sono "professionali", in quanto sino ad ora non si ha notizia di un riscatto pagato, che non abbia portato alla liberazione dell'accesso ai dati. Anzi, in qualche

caso i criminali informatici fungono anche da punto di assistenza e danno indicazioni non solo sulle modalità con cui è possibile effettuare pagamenti in bitcoin, ma anche sulle modalità con cui è possibile garantire lo sbocco del sistema.

Narrano le cronache che un malcapitato, che aveva pagato il riscatto, ma non era riuscito a convertire in chiaro la base dei dati, è stato assistito a distanza con molta professionalità, fino a portare a termine con successo l'operazione.

Vediamo adesso quali possono essere le conseguenze di un attacco di questo tipo.

Tanto per cominciare, l'attacco si porta a termine in un tempo brevissimo, perché bastano pochi minuti per cifrare una base dei dati di medie dimensioni, a partire dal momento in cui l'infezione è penetrata nel sistema.

I tempi tecnici necessari per riportare in chiaro i dati sono legati al tempo necessario perché il responsabile del sistema informatico capisca bene che cosa sia successo, ottenga l'approvazione della direzione al pagamento del riscatto, ammesso che la possa ottenere, analizzi possibili alternative, se ha a disposizione una base dei dati aggiornata e ancora non colpita dal virus, eventualmente metta a punto una procedura per il pagamento in bitcoin, concordata con il responsabile finanziario, ed infine riceva ed attivi il codice di decifrazione. Due o tre giorni passano assai rapidamente e durante tutto questo periodo il sistema informativo non è accessibile, con conseguenze che possono variare in maniera drammatica da azienda ad azienda.

Altro tempo si perde quando, anche se il sistema informatico è stato riportato in chiaro, il responsabile della sicurezza deve effettuare una bonifica e pulizia dell'intero sistema, per evitare che qualche traccia possa essere rimasta all'interno del sistema a sua insaputa.

Appare evidente che due giorni di fermo macchina per molte attività rappresentano un lasso di tempo del tutto inaccettabile: si pensi ai sistemi ospedalieri, ai sistemi di distribuzione dell'energia elettrica e controllo del traffico e simili.

Ma non è finita.

A tutti gli effetti, la violazione della base dei dati del sistema informativo è da considerare come un data breach, secondo la definizione che dà il nuovo regolamento europeo sulla protezione dei dati personali, regolamento 2016/679. Perché si verifichi un data breach infatti non è necessario che i dati vengono asportati o copiati all'esterno, ma è sufficiente che i dati vengano resi inaccessibili, anche per brevi periodi.

Poiché, con l'entrata in vigore del nuovo regolamento, la segnalazione al garante di una violazione dei dati è sempre obbligatoria, si crea un nuova problematica per il titolare del trattamento, che potrebbe avere riflessi non positivi sull'intera strategia di protezione dei dati dell'ente coinvolto.

Anche se i venditori di applicativi di protezione del software sono relativamente celeri nel mettere a punto applicativi aggiornati, non v'è alcun dubbio che la velocità di evoluzione degli strumenti di attacco, da parte di criminali informatici, è molto più elevata; ciò significa che gli applicativi antivirus sono sempre in ritardo, rispetto alle tecnologie di attacco.

Al momento, la migliore tecnica di protezione da questi attacchi è quella di sensibilizzare al massimo tutti i soggetti coinvolti sulla diligente chiusura di tutte le porte possibili di accesso del virus, prestando la massima attenzione a comunicazioni via posta elettronica, ad attacchi mediante tecniche di profiling ed altre procedure, che i malviventi conoscono assai meglio dei normali utenti.

Adalberto Biasiotti

 Questo articolo è pubblicato sotto una Licenza Creative Commons.

---

www.puntosicuro.it