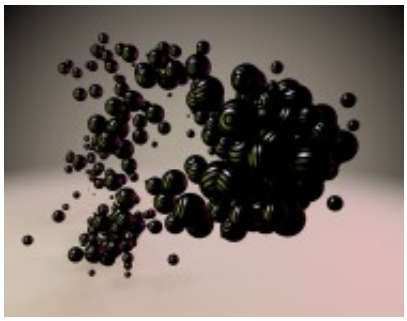
Ransomware: Come ti metto in scacco la PMI

Date : 21 gennaio 2016



> Il Cyber Crime è sempre in continua evoluzione ed è costantemente alla ricerca di nuovi vettori di attacco per poter ricavare denaro nel modo più facile possibile con i costi di gestione tendenti allo zero. Minima spesa massima resa!

Dopo le ondate di phishing bancario mediante siti di adescamento o mediante l'utilizzo di malware, l'imprenditore che investe in queste realtà criminali si è accorto che da un paio d'anni a questa parte vi è la necessità di diversificare il rischio, proprio perché banche ed utenti finali stanno iniziando a non abboccare più come una volta a questa tipologia di addescamenti, pertanto l'operatore che lavora nella Cyber Crime S.p.A. ha iniziato ad esplorare nuovi vettori di attacco, magari meno remunerativi rispetto a campagne di phishing massivo, ma con un mercato potenziale tutto da scoprire e da sfruttare; ispirandosi alle forme di malavita reale, qualcuno ha ben pensato di sviluppare un malware informatico che, opportunamente guidato da qualcuno, va a colpire dritto nel cuore del patrimonio dell'azienda, cioè i dati di produzione.

> Questa tipologia di malware prendono il nome di Ransomware.

Il Ransomware in realtà non è una invenzione degli ultimi tempi, già nel 1989 venivano distribuiti i primissimi Ransomware su floppy disk inviati per posta (non elettronica) adescando le vittime con promesse di software sofisticato contenente informazioni su HIV/AIDS ma, invece del software, una volta avviato l'eseguibile, il programma avviava la cifratura dell'- hard disk richiedendo il pagamento di 189 dollari per lo sblocco del sistema.

METODOLOGIA OPERATIVA DELL'ATTACCO

Ad oggi è letteralmente impossibile creare uno storco di tutte le versioni e le varianti di Ransomware ad oggi sviluppate. In passato i primi malware puntavano direttamente all'"utonto" finale ed avevano l'obiettivo di estorcere poche centinaia di dollari/euro a fronte di una schermata intimidatoria della Polizia di Stato o dell'FBI che minacciava ripercussioni legali se non si saldasse all'istante la multa telematica tramite un comodo pagamento via carta di credito o paypal; gli utili erano pochi e il gioco iniziava a non valer più la candela.

Con il passare del tempo si è capito che il modello di business del Ransomware poteva essere utilizzato anche sulle piccole e medie imprese, cioè quelle realtà che molto spesso non hanno un budget da investire nell'Information Security ma che in molti casi producono utili ed hanno a disposizione una eventuale liquidità economica da poter sottrarre; pertanto l'attaccante non dovrà far altro che unire tecniche di intrusione informatica con le tecniche di divulgazione di malware, con il solo obiettivo di entrare nella rete dell'azienda e bloccare la produttività della stessa, sbloccandola a patto del pagamento di un riscatto vero e proprio.

Come viene selezionata l'azienda da sottoporre all'infezione di un ransomware di questo tipo?

Nella maggior parte dei casi viene fatta una vera e propria pesca a strascico, cioè si parte da una scansione della rete su classi IP pubbliche individuando ipotetici servizi e applicazioni vulnerabili che permetterebbero l'accesso alla rete LAN di una qualsiasi azienda. Una volta ottenuto l'accesso si cerca di capire se l'azienda ha dei dati di importanza strategica e dove essi risiedano soprattutto quanto gli stessi possono essere fondamentali per la produzione di utili. Più i dati trovati rappresentano il patrimonio digitale dell'azienda, più la richiesta del riscatto sarà elevata; se solo ci pensate, anche la sola perdita dei dati contabili amministrativi porterebbe ad un parziale blocco di produttività di una qualsiasi realtà media, piccola o grande che essa sia.

Una volta fatta la "valutazione economica" parte la vera e propria attività di cifratura. Le metodologie utilizzate per la cifratura del dato possono essere svariate a seconda delle tecnologie che si intendono utilizzare e del tempo che si ha a disposizione per effettuare l'attività; i gruppi meglio organizzati scelgono con cura il giorno esatto per eseguire l'attività di infezione e di cifratura del dato, prediligendo i week end ad esempio, proprio perché nel caso di un quantitativo di dati molto elevato, il processo di cifratura risulterebbe molto lungo pertanto la variabile del tempo diventa fondamentale. La cifratura del dato può essere totale o parziale: • è totale quando il file risulta essere completamente cifrato mediante l'algoritmo scelto dall'attaccante • è parziale quando, per motivi di tempo, vengono cifrati soltanto header e footer del file, mantenendo nella maggior parte dei casi il copro del file in chiaro ma la coda e la testa cifrati.

Nella maggior parte dei casi i file cifrati avranno una estensione del file inusuale con all'interno del nome file un messaggio in lingua inglese che invita il lettore a mandare una e-mail ad un indirizzo di posta appositamente creato per il caso in questione per chiedere chiarimenti e delucidazioni su come poter ripristinare l'accesso al file. Solo dopo aver dato il denaro richiesto, l'attaccante invierà all'azienda il così detto decrypter, cioè l'applicativo che individuerà i file cifrati e ne ripristinerà il normale accesso come se nulla fosse mai accaduto. Gli attaccanti più furbi però, una volta classificata l'azienda come "ben pagante", lasceranno sempre una seconda via di ingresso (backdoor) per poter tornare una seconda volta in un futuro prossimo, cifrare di nuovo tutti i dati e richiedere la stessa cifra se non il doppio. Come dire, i migliori clienti bisogna tenerseli stretti!

UN CASO REALE

Nel 2013 una PMI italiana con circa 20 dipendenti operante nel settore della tipografia ha avuto la produzione completamente bloccata a causa di una infezione di un Ransomware che cifrò la bellezza di quasi 5 Terabyte di dati, il tutto durante le festività della pausa lavorativa dovuta al ponte del primo maggio.

La situazione era letteralmente disarmante. Tutto il file server aziendale era stato compromesso e cifrato, compresi i backup e i file di archivio dello storico dei lavori già eseguiti. L'unica cosa che si salvò fu il gestionale che, per pura coincidenza, non era stato ancora migrato nello storage aziendale oggetto della compromissione.

La richiesta di riscatto fu quotata 10.000 euro. L'azienda, che sino a quel momento non conosceva assolutamente cosa volesse dire la parola Information Security, non aveva la più pallida idea ne di come il malware fosse entrato nella loro rete, ne da dove fosse partita l'infezione; la persona che si occupa della parte informatica non aveva alcun background di Information Security, pertanto, qualsiasi tentativo di dialogo per ottenere informazioni come log di apparati di rete o dell'antivirus (antivirus con licenza gratuita per uso personale installato su tutte le postazioni), portava ad una unica risposta: "non so". L'obiettivo per il quale fummo chiamati non era il solo ripristino dell'ambiente di produzione, ma anche scoprire da dove sono entrati e da dove partì tutto il processo di cifratura.

Data la situazione fummo costretti ad eseguire una time line e una super time line degli eventi su tutti i sistemi, client e server, inizialmente solo Microsoft Windows; per time line e super time line si intende l'elaborazione di tutti i riferimenti temporali:

- residenti in un file system (data creazione, data modifica e ultimo accesso)
- dei log degli applicativi in uso
- dei log di sistema storicizzati localmente
- ordinati in ordine cronologico, così da poter ricostruire ogni singola azione avvenuta in quel determinato sistema.

La time line ci permise di capire esattamente quando il malware entrò in azione sulle workstation e da quale indirizzo IP partì la divulgazione; sbalorditi ed increduli le tracce puntavano il dito contro una workstation Mac che, per qualche motivo a tutti sconosciuto, aveva alcuni servizi, risultati poi essere vulnerabili, direttamente esposti sulla rete Internet. Individuato il vettore di ingresso, individuati i client coinvolti, partì immediatamente la bonifica dei sistemi e la rimozione delle backdoor riscontrate.

Ma i file cifrati? I file cifrati in realtà non erano completamente cifrati. Per nostra fortuna, soltanto header e footer erano stati manomessi pertanto è stato possibile evitare di pagare il riscatto, sviluppare internamente un decrypter ad hoc per la tipologia di file modificati e ripristinare la produttività aziendale in cinque giornate lavorative.

CONCLUDENDO

Nella maggior parte dei casi le vittime di questi attacchi sono realtà che non attuano alcun tipo

di investimento a tutela del proprio patrimonio digitale aziendale. Come nel caso citato poc'anzi, sarebbe bastato un investimento di poche migliaia di euro per un Endpoint Protection opportunamente configurato ed una gestione delle politiche di accesso remoto più responsabile e l'azienda, sicuramente, si sarebbe risparmiata questa brutta esperienza; ma è grazie a questa esperienza che una PMI ha capito che a fine anno bisogna riservare il budget per attuare investimenti, anche molto piccoli, volti a diminuire sempre di più il rischio della compromissione dei sistemi di produzione.

La morale quindi qual'è? Molto semplice: le PMI col tempo hanno capito che devono investire in sicurezza fisica (installando un allarme sonoro, una porta blindata o pagando un servizio di ronda notturna) per difendere i propri beni materiali da eventuali ladri di polli; nel 2014 le stesse PMI devono capire che bisogna investire anche in sicurezza logica per evitare che qualcuno, a fronte di una richiesta economica di poche migliaia di euro, provochi danni alla produzione aziendale per svariate centinaia di migliaia di euro.

A cura di **Stefano Fratepietro**, CISO in Tesla Consulting, DEFT Project Leader e Presidente Associazione DEFT

Articolo pubblicato sulla rivista ICT Security – Gennaio/Febbraio 2014