PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 4992 di Giovedì 05 agosto 2021

Parliamo ancora di ransomware

L'attacco al sistema sanitario informatico della regione Lazio ci impone di ritornare ancora una volta su questo delicatissimo tema: un documento con indicazioni utili.

Puntosicuro più volte si è occupato del tema del ransomware, mettendo in guardia tutti i lettori sul fatto che questo tipo di attacco viene perpetrato su una base sempre più allargata di bersagli e con tecniche sempre più sofisticate.

Più volte abbiamo messo in evidenza il fatto che una delle migliori difese è quella di avere a disposizione una copia di backup dei dati, in modo che un eventuale blocco dell'accesso ai dati in linea possa essere superato all'accesso ai dati di backup. Purtroppo, in data 4 agosto 2021 i quotidiani hanno dato notizia del fatto che l'assessore alla sanità della regione Lazio ha dichiarato che sono stati compromessi anche i dati di backup. Questa affermazione mette in evidenza il fatto che i dati di backup devono essere fisicamente isolati dai dati in linea, in modo che non sia possibile per un attaccante sofisticato riuscire a bloccare contemporaneamente in dati in linea ed i dati di backup.

Ecco il motivo per cui alcune grandi aziende provvedono ad un backup quotidiano su supporti fisici specifici, che vengono trasferiti, ad esempio, all'interno di un caveau di un istituto di vigilanza.

Viene quindi ribadito il principio che i dati di backup devono essere fisicamente separati e non devono costituire un backup on-line, che, come abbiamo appena visto, può essere a sua volta compromesso.

Un'analisi degli attacchi perpetrati nell'arco del 2020 ha messo in evidenza una evoluzione delle modalità operative degli attaccanti: invece di attaccare una moltitudine di piccoli clienti, oggi gli attaccanti si concentrano su pochi grossi clienti, che possono pagare delle cifre significative.

Abbiamo purtroppo già dato notizia di riscatti significativi che sono stati pagati da grandi aziende, crocifisse dagli attaccanti.

Inoltre, gli attaccanti hanno cominciato a scambiarsi gli strumenti di attacco, tant'è vero che gli esperti hanno potuto rilevare come la stessa tipologia di attacco venga perpetrata da attaccanti, che erano ubicati in paesi diversi. Pertanto, la considerazione che un particolare tipo di attacco proviene da un particolare paese non è più valida.

L'attacco al sistema sanitario della regione Lazio ha messo inoltre in evidenza un tema, sul quale più volte gli esperti di sicurezza hanno concentrato la loro attenzione. Il lavoro in smart Working, utilizzando apparati informatici talvolta privi di adeguate protezioni, ha indebolito il perimetro dei sistemi informativi, consentendo di inserire il ransomware, attaccando il terminale informatico di un dipendente che lavora da casa. Secondo le notizie di stampa, è proprio questo il caso che si è verificato nell'attacco a questo sistema sanitario.

L'evoluzione degli attaccanti si manifesta anche grazie al fatto che il software di attacco non è più inserito in un allegato di un messaggio di posta elettronica, ma spesso viene inserito in un pop-up, che appare sullo schermo, e che viene oggi chiamato "Trojan pop-up".

Nel corso della normale navigazione, soprattutto in mancanza di validi ed aggiornati filtri di ingresso, è del tutto possibile che un dipendente possa cliccare su un pop-up, che gli sembra particolarmente attraente, sia perché propone prodotti a prezzi allettanti, sia per altri motivi magari meno nobili.

Cliccando su questo pop-up, il software criminale entra nel sistema informativo di chi ha cliccato.

Un altro aspetto assai preoccupante e che aiuta a propagare il numero degli attaccanti viene chiamato con l'acronimo RAAS ? ransom as a service. In questo caso una banda specializzata mette a disposizione, anche di soggetti non particolarmente addestrati, tutti gli strumenti necessari per perpetrare un attacco di tipo ransomware, offrendo perfino un ufficio di consulenza tecnica, per insegnare all'acquirente di questo software come usarlo al meglio. Il costo di questa assistenza tecnica è normalmente legato ad una porzione del bottino che viene raccolto dal "cliente". Ad esempio, un applicativo, che viene venduto con la formula RAAS prevede una ripartizione del 60 e del 40% del bottino incassato fra il cliente ed il fornitore del servizio criminoso.

È bene ricordare lettori che fin dal settembre 2019 il dipartimento degli Stati Uniti della sicurezza interna aveva pubblicato un documento che dava tutt'una serie di preziose ed efficaci indicazioni sulle modalità di prevenzione di questo attacco. Questo documento è stato recentemente aggiornato.

Purtroppo, sia perché il documento è in inglese, sia perché alcuni esperti di informatica sono un poco pigri, queste notizie non sono state diffuse a sufficienza. Per assistere i nostri lettori, mettiamo a disposizione questo preziosissimo documento, in attesa che la nostra futura agenzia di cyber sicurezza possa fare qualcosa di simile anche in italiano per gli italiani!

Fact sheet - Ransomware Awareness Campaign (pdf)

Adalberto Biasiotti