PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 24 - numero 5292 di Mercoledì 07 dicembre 2022

Le quattro fasi di un attacco ransom

Questa tipologia di attacchi si sta diffondendo una velocità impressionante. Questo è il motivo per cui diverse agenzie nazionali, o federali, stanno cercando di sensibilizzare i soggetti potenzialmente a rischio, offrendo raccomandazioni specifiche.

Non solo cresce il numero di questi attacchi, ma cresce anche la gravità delle conseguenze. Ecco una sintetica tabella dei principali attacchi, condotti negli Stati Uniti, contro infrastrutture critiche.

Nel giugno 2021 la Casa Bianca ed il Dipartimento dell'agricoltura degli Stati Uniti annunciarono che una azienda, che trattava carni alimentari, era stata attaccata con un ransomware che aveva bloccato l'attività aziendale. L'azienda ha pagato 11 milioni di dollari per recuperare l'accesso ai dati.

Nel maggio 2021 la Colonial Pipeline Company ha annunciato che era rimasta vittima di un attacco ransomware, che ha temporaneamente bloccato la consegna di carburante ed altri prodotti petroliferi in quasi tutto il sud-est degli Stati Uniti. Il riscatto pagato ammontava a 4 milioni di euro.

Nel febbraio 2021 il Dipartimento di giustizia ha rivelato che tre soggetti nordcoreani sono stati imputati per la creazione di un ransomware, chiamato WannaCry, usato per numerosi tentativi di estorsione a varie aziende americane tra il 2017 ed il 2020. Questa tipologia di attacco, scoperta nel maggio 2017, colpiva i sistemi, operando a distanza; ha colpito ospedali, scuole e numerose altre organizzazioni. Questo applicativo ha infettato decine di migliaia di sistemi informativi in 150 paesi.

Nel Dicembre 2020, le agenzie federali hanno ricevuto numerosi rapporti di un attacco ransomware, diretto soprattutto alle istituzioni scolastiche.

Nell'ottobre 2020, il Dipartimento di giustizia ha annunciato che sei soggetti russi sono stati imputati per un attacco ransomware, che ha causato quasi 1 miliardo di perdite alle aziende colpite. Lo strumento di attacco, chiamato NorPetya, scoperto nel 2017, consentiva agli attaccanti di assumere il ruolo di controllore del sistema, cifrando file essenziali e rendendo inutilizzabile i sistemi Windows infettati. Le aziende coinvolte operavano nei settori della finanza, trasporto, energia e sanità.

Nel maggio 2019 il sindaco di Baltimora ha riferito che la città era rimasta vittima di un attacco per ransomware. Di conseguenza, i dipendenti della città non potevano accedere alla propria posta elettronica e la vendita di beni immobili e la fatturazione dei consumi di acqua sono state rallentate per molti mesi.

Per meglio inquadrare questa tipologia di attacco, la cui diffusione è apparentemente esponenziale, è bene analizzare le quattro fasi, grazie alle quali l'attacco viene portato a termine.

1. Intrusione iniziale-l 'attaccante riesce a entrare nel sistema informativo attaccato o nell'apparato informatico coinvolto, grazie ad infezione da parte di malware.

2. Fase di ricognizione ed infezione-l 'attaccante acquisisce una conoscenza approfondita del sistema attaccato ed è in grado di infettare con il ransomware l'intera rete.

3. Sottrazione o cifratura dei dati-l 'attaccante è in grado di estrarre i dati del sistema attaccato; è anche possibile che l'attaccante provveda a cifrare i dati presenti nel sistema, impedendo l'accesso ad essi, da parte del responsabile del sistema.

4. La richiesta di riscatto-l 'attaccante, fà apparire un messaggio con la richiesta di riscatto, indicando l'importo e le modalità di pagamento. Spesso vengono anche indicati dei termini ultimi per effettuarlo.

Negli Stati Uniti, gli organismi coinvolti nel fronteggiare questa tipologia di attacco sono sostanzialmente tre:

- la Cybersecurity and Infrastructure Security Agency ? CISA- del dipartimento della sicurezza interna,
- l'FBI,
- il servizio segreto.

Per contrastare la possibilità di questi attacchi è evidente che i responsabili della sicurezza informatica delle varie aziende, potenzialmente coinvolte, devono attuare tutta una serie di misure preventive, soprattutto provvedendo al tempestivo aggiornamento di misure esistenti.

Ma vi è anche un altro aspetto che il rapporto del General accounting Office ha messo in evidenza.

Un problema che potrebbe nascere, quando vi sono più enti abilitati ad intervenire, a fronte di attacchi con ransomware, è quello di identificare quale sia l'azienda coordinatrice principale che deve sviluppare le attività di risposta è messo sotto controllo dell'attacco.

Ecco il motivo per cui l'organo ispettivo ha sollecitato le tre entità sopra illustrate a mettere a punto una politica coordinata, che permetta di ridurre i tempi di intervento e migliorare in modo significativa l'assistenza che può essere offerta alle aziende

colpite.

Adalberto Biasiotti

www.puntosicuro.it