Proteggere i sistemi sanitari dal ransomware

Il ransomware è un malware che utilizza generalmente la crittografia asimmetrica per tenere sotto sequestro le informazioni di una vittima. La cifratura asimmetrica (pubblica-privata) è una crittografia che utilizza una coppia di chiavi per cifrare e decifrare un file. La coppia di chiavi pubblica-privata viene generata in modo univoco dall'aggressore per la specifica vittima. La chiave privata, necessaria per decifrare i file, viene memorizzata nel server dell'aggressore stesso. Quest'ultimo mette la chiave privata a disposizione della vittima solo dopo il pagamento del riscatto, anche se non è sempre così, come si è visto in recenti campagne di ransomware. Senza l'accesso alla chiave, decifrare i file tenuti in ostaggio è pressoché impossibile.

Negli ultimi anni il ransomware è stato in cima alle preoccupazioni di ogni professionista della sicurezza. Sfortunatamente, il ransomware è uno strumento di attacco informatico semplice ed efficace utilizzato per garantire un tornaconto economico. Nell'ultimo anno abbiamo osservato un cambiamento di obiettivi, dagli individui alle imprese, dato che quest'ultime sono in grado di pagare riscatti più ingenti. Di recente anche le strutture sanitarie sono diventate uno dei bersagli preferiti dagli autori del ransomware. Nel *Report McAfee Labs sulle Minacce: settembre 2016* abbiamo analizzato gli attacchi di ransomware del primo e secondo trimestre 2016 diretti contro gli ospedali e abbiamo scoperto che sono efficaci, correlati e mirati, benché relativamente poco sofisticati. Abbiamo inoltre spiegato le problematiche specifiche di alcuni ospedali relativamente al ransomware, compresi i sistemi legacy e i dispositivi medicali dotati di scarsa sicurezza, oltre al fatto che l'accesso immediato alle informazioni può essere una questione di vita o di morte.

Policy e procedure per proteggersi dal ransomware

La misura più importante da adottare per proteggere i sistemi dal ransomware è essere consapevoli del problema e dei relativi metodi di diffusione. Di seguito è riportato un elenco di policy e procedure a cui gli ospedali dovrebbero attenersi per contenere il successo degli attacchi di ransomware.

- Prevedere un piano d'azione da attuare in caso di attacco. Scoprire dove sono posizionati i dati di importanza critica e se esiste un metodo per infiltrarli. Eseguire esercitazioni di continuità operativa e disaster recovery con il team di gestione delle emergenze dell'ospedale per convalidare gli obiettivi RPO e RTO. Tali esercitazioni possono riuscire a mettere in luce impatti nascosti sulle operazioni degli ospedali che altrimenti non emergerebbero durante i normali test di backup. La maggior parte degli ospedali ha pagato il riscatto perché non disponeva di un piano di emergenza!
- Mantenere aggiornate le patch del sistema. Molte vulnerabilità comunemente sfruttate dal ransomware possono essere risolte da una patch. Mantenersi aggiornati con le patch per i sistemi operativi, Java, Adobe Reader e Flash e le applicazioni. Predisporre una procedura di applicazione delle patch e assicurarsi che le patch siano applicate correttamente.
- Per i sistemi e i dispositivi medici legacy degli ospedali a cui non è possibile applicare le patch, occorre mitigare il rischio sfruttando le whitelist delle applicazioni, che bloccano i sistemi e prevengono l'esecuzione di programmi non approvati. Segmentare sistemi e dispositivi da altre parti della rete con un firewall o un sistema di prevenzione delle intrusioni. Disattivare i servizi o le porte non indispensabili su questi sistemi per ridurre l'esposizione a possibili punti di accesso delle infezioni.
- Proteggere gli endpoint. Utilizzare la protezione degli endpoint e le relative funzionalità avanzate. In molti casi, il client viene installato con solo le funzionalità predefinite abilitate. Con l'implementazione di alcune funzionalità avanzate, come ad esempio “blocco di avviamento eseguibili dalla cartella Temp”, è possibile rilevare e bloccare più elementi malware.

- Se possibile, evitare l'archiviazione di dati sensibili sui dischi locali. Imporre agli utenti di archiviare i dati su unità di rete sicure. Si limita così il tempo di inattività perché è possibile ricreare semplicemente l'imaging dei sistemi infetti.
- Utilizzare l'antispam. La maggior parte delle campagne di ransomware inizia con un'email di phishing che contiene un collegamento o un determinato tipo di allegato. Per le campagne di phishing che impacchettano il ransomware in un file .scr o in un altro formato file non comune, è facile impostare una regola antispam che blocchi questi allegati. Se si consente il passaggio dei file .zip, occorre attivare la scansione di almeno due livelli nel file .zip per rilevare eventuali contenuti dannosi.
- Bloccare i programmi e il traffico indesiderati o non necessari. Se Tor non è necessario, bloccate l'applicazione e il relativo traffico sulla rete. Il blocco di Tor spesso consente di impedire al ransomware di ottenere la chiave RSA pubblica dal server di controllo, bloccando così il processo di crittografia ransomware.
- Aggiungere la segmentazione di rete per i dispositivi critici necessari per l'assistenza ai pazienti.
- Backup distanziati. Assicurarsi che i sistemi di backup, lo spazio di archiviazione e i nastri siano in una località non generalmente accessibile dai sistemi nelle reti produttive. Se i payload degli attacchi di ransomware si diffondono lateralmente, potrebbero potenzialmente intaccare i dati di backup.
- Sfruttare un'infrastruttura virtuale per i sistemi dei record medici elettronici di importanza critica che sono distanziati dal resto della rete produttiva.
- Educare continuamente gli utenti alla consapevolezza. Poiché la maggior parte degli attacchi di ransomware inizia con un'email di phishing, la sensibilizzazione degli utenti è estremamente importante. Per ogni 10 email inviate dagli aggressori, le statistiche hanno dimostrato che almeno una raggiungerà lo scopo. Non aprire le email o gli allegati inviati da mittenti non verificati o sconosciuti.

Cosa può fare la tecnologia di McAfee per proteggerti dal ransomware

McAfee VirusScan Enterprise e McAfee Endpoint Security 10

- Con McAfee VirusScan Enterprise (VSE) o McAfee Endpoint Security (ENS), prendere le seguenti misure:
  - Usare quotidianamente McAfee ePolicy Orchestrator (ePO) per distribuire i DAT aggiornati.
  - Assicurarsi che McAfee Global Threat Intelligence (McAfee GTI) sia attivato; McAfee GTI contiene oltre 7 milioni di firme di ransomware uniche.
  - Sviluppare regole di protezione degli accessi per bloccare l'installazione e i payload del ransomware; consultare gli articoli della knowledgebase sulle regole di protezione dell'accesso KB81095 e KB54812.
  - Usare il contenimento dinamico delle applicazioni per impedire alle applicazioni sconosciute di eseguire attività ostili.

McAfee Threat Intelligence Exchange

- Impostare con McAfee Threat Intelligence Exchange (TIE) le seguenti policy:
  - Iniziare con la modalità di osservazione.
  - Mano a mano che si scoprono endpoint con processi sospetti, usare i tag di sistema per applicare le policy di imposizione di McAfee TIE.
  - Rimuovi in base alla reputazione: file malevolo noto.
  - Blocca in base alla reputazione: molto probabilmente malevolo (il blocco in caso di file sconosciuto offrirebbe maggior protezione ma potrebbe anche aumentare il carico di lavoro amministrativo iniziale).
  - Invia i file a McAfee Advanced Threat Defense (ATD) in caso di livello di reputazione sconosciuto e inferiore.
  - Policy del server TIE: accetta le reputazioni McAfee ATD per i file non ancora osservati da McAfee TIE.
- Intervento manuale di McAfee Threat Intelligence Exchange:
  - imposizione della reputazione dei file (in modalità operativa).
  - Molto probabilmente dannoso: rimuovi/elimina.
  - Probabilmente dannoso: blocca.
  - La reputazione dell'impresa (organizzativa) può bypassare McAfee GTI. Si può scegliere di bloccare un processo indesiderato, per esempio un'applicazione non supportata o vulnerabile. Contrassegnare i file come Probabilmente malevoli.
  - Invia i dati di reputazione provenienti da terze parti in TIE tramite gli indicatori di compromissione.

McAfee Advanced Threat Defense

- McAfee Advanced Threat Defense presenta le seguenti funzioni di rilevamento integrate:
  - Rilevamento basato sulle firme: le firme mantenute da McAfee Labs sono attualmente oltre 150 milioni, comprese quelle di CTB-Locker, CryptoWall e delle loro varianti.
  - Rilevamento basato sulla reputazione: McAfee GTI.
  - Analisi statica ed emulazione in tempo reale: utilizzata per il rilevamento senza firme.
  - Personalizza le regole YARA.
  - Analisi completa del codice statico: esegue il reverse engineering del codice del file per valutarne tutti gli attributi e i gruppi di istruzioni, oltre che per analizzarne in modo completo il codice sorgente senza eseguirlo.
  - Analisi dinamica nella sandbox.
- Crea profili nell'analizzatore per capire dove è probabile che venga eseguito il ransomware:
  - Sistemi operativi comuni, Windows 7, Windows 8, Windows XP.
  - Installare applicazioni Windows (Word, Excel) e attivare le macro.
- Fornire profili unici nell'analizzatore per sistemi operativi separati con accesso a Internet:
  - Molti esempi eseguono uno script a partire da un documento di Microsoft Office che crea una connessione in uscita e attiva il malware. Fornire un profilo nell'analizzatore con una connessione a Internet aumenta le percentuali di rilevamento.

McAfee Application Control

- McAfee Application Control protegge con il whitelisting delle applicazioni. È ideale per proteggere tutti i tipi di dispositivo, soprattutto:
  - Dispositivi statici come le apparecchiature medicali.
  - Sistemi operativi legacy che non ricevono più gli aggiornamenti.
  - Server applicativi che offrono un limitato numero di servizi.
  - Sistemi che non vengono modificati frequentemente.
- Installazione iniziale
  - McAfee Application Control sottopone a scansione completa un sistema durante l'installazione, creando l'inventario degli endpoint e la whitelist delle applicazioni.
- Modalità osservazione
  - Consente agli amministratori di monitorare le nuove app installate e avviate, con l'opzione di unirle nella whitelist centralizzata se l'applicazione viene riconosciuta come autorizzata.
  - Assiste nella procedura di whitelisting identificando i nuovi programmi di aggiornamento affidabili per le applicazioni all'interno dell'ambiente.
  - Identifica i metodi di aggiornamento della whitelist, come processi, certificati, directory o utenti approvati.
- Modalità di autoapprovazione
  - Gli utenti possono approvare le applicazioni non incluse nella whitelist. Questo consente la flessibilità e il minimo impatto sull'azienda.
  - Gli amministratori sono così in grado di monitorare centralmente i contenuti approvati dagli utenti e di accettare o revocare l'autorizzazione di un'applicazione in base alla reputazione e alle policy dell'organizzazione.
- Imposizione della whitelist
  - Il sistema è completamente protetto dalle applicazioni sconosciute, comprese quelle ostili come il ransomware.
  - Notifica l'utente finale per la procedura di approvazione dei nuovi file eseguibili.

Ulteriori letture

Comunità McAfee Expert Center

- McAfee VirusScan Enterprise
- McAfee Endpoint Security
- McAfee Threat Intelligence Exchange
- McAfee Advanced Threat Defense
- McAfee Application Control

McAfee Together is power.

Via Fantoli, 7
20138 Milano
Italy
(+39) 02 554171
www.mcafee.com/it