Informazioni sulle minacce informatiche CTI) per la salute

CSP006

PRESENTAZIONE DA PARTE DI: STYLIANOS KARAGIANNIS (PDMFC, PORTOGALLO)

Example Cyberattack Pt.1

Attacco informatico a un'organizzazione sanitaria

Esempio per CTI Pt. 1

Un'organizzazione sanitaria è stata presa di mira da un attacco informatico volto a rubare i dati dei pazienti dal suo sistema di cartelle cliniche elettroniche (EHR). L'attacco, iniziato tramite un'e-mail di phishing contenente un allegato dannoso, ha portato alla compromissione di diversi account utente all'interno della rete dell'organizzazione.

1. Condivisione iniziale degli indicatori: Dopo aver scoperto l'e-mail di phishing e gli allegati sospetti, il team di sicurezza dell'organizzazione sanitaria carica gli indicatori di compromissione (IOC) pertinenti sulla propria istanza locale di MISP. Questi IOC includono: a) indirizzi del mittente dell'e-mail dannosa, b) oggetto e contenuto 'e-mail, c) nome del file e hash dell'allegato dannoso.
2. Analisi e correlazione delle minacce: La piattaforma MISP correla automaticamente gli IOC caricati con i feed e i database di intelligence sulle minacce esistenti. Questo processo aiuta a identificare le firme di malware note, i domini dannosi e gli indirizzi IP associati ad attacchi informatici simili rivolti alle organizzazioni sanitarie a livello globale.
3. Triage e prioritizzazione: In base alla gravità e all'impatto dell'attacco informatico, gli analisti della sicurezza dell'organizzazione sanitaria danno priorità agli IOC attivabili per ulteriori indagini e risposte. Ciò può comportare la segnalazione di indicatori ad alto rischio, come account utente compromessi o connessioni di rete a indirizzi IP noti come dannosi, per un'immediata riparazione.

Formazione CSP CSP001: Presentazione di S. Karagiannis, PDMFC, Portogallo

Attacco informatico alle organizzazioni sanitarie

Example Cyberattack Pt.2

4. Condivisione delle informazioni e collaborazione: Sfruttando le funzionalità di condivisione delle informazioni del MISP, l'organizzazione sanitaria condivide in modo sicuro i dati di intelligence sulle minacce, compresi gli IOC e i rapporti di analisi, con partner esterni fidati come altri fornitori di servizi sanitari, agenzie governative e gruppi industriali di cybersecurity. Questo approccio collaborativo migliora la consapevolezza della situazione e consente una risposta coordinata all'attacco informatico in tutto il settore sanitario.

5. Rilevamento e prevenzione migliorati: Integrando il MISP con la propria infrastruttura di sicurezza, l'organizzazione sanitaria implementa misure automatizzate di rilevamento e prevenzione delle minacce basate su informazioni condivise sulle minacce. Ciò include l'aggiornamento delle regole del firewall, dei sistemi di rilevamento delle intrusioni (IDS) e delle soluzioni di sicurezza degli endpoint per bloccare il traffico dannoso, mettere in quarantena i sistemi compromessi e prevenire l'ulteriore diffusione dell'attacco informatico all'interno della rete.

Risultato

Grazie alla condivisione proattiva delle informazioni sulle minacce e alla collaborazione abilitata dal MISP, l'organizzazione sanitaria attenua efficacemente l'attacco informatico, contenendone l'impatto e impedendo l'accesso non autorizzato ai dati dei pazienti. Sfruttando la condivisione delle informazioni sulle minacce, l'organizzazione rafforza la propria resilienza informatica e migliora la propria capacità di difesa contro le future minacce informatiche che colpiscono il settore sanitario.

Use Case #1: Analysis

Caso d'uso n. 1 - Analisi delle informazioni sulle minacce informatiche

MISP per analisti

- Utilizzate il MISP per raccogliere, analizzare e condividere le informazioni sulle minacce informatiche. Il MISP funge da repository centrale per la raccolta e la condivisione di informazioni tra organizzazioni e settori.
- Una volta completata l'analisi, gli analisti distribuiscono le informazioni utilizzando i sistema MISP.
  funzioni di condivisione avanzate.

- Nel settore sanitario: Gli analisti raccolgono informazioni sulle minacce manualmente o automaticamente utilizzando le funzionalità di ingestione di MISP. MISP offre integrazioni di arricchimento per fornire automaticamente un contesto aggiuntivo agli eventi.
- I CIO possono essere inviati alle soluzioni di sicurezza per essere bloccati.
- I rapporti possono essere generati e condivisi con i dirigenti.
- Gli eventi MISP possono essere condivisi automaticamente con il più ampio sistema di cybersecurity.
  comunità.

Use Case #2: Research

Caso d'uso n. 2 - Ricerca sulla sicurezza

MISP per i ricercatori

- I ricercatori di sicurezza utilizzano MISP per raccogliere e condividere informazioni su vulnerabilità, exploit e minacce. Le integrazioni di MISP e il supporto per le tassonomie/quadri CTI consentono ai ricercatori di utilizzare un linguaggio comune nella descrizione delle minacce.

- Nel settore sanitario: I ricercatori studiano nuove forme di malware ed elencano le IOC, le tecniche MITRE ATT&CK utilizzate e le CVE sfruttate.
- Le informazioni condivise aiutano le organizzazioni a bloccare gli IOC e i rilevamenti di scrittura per le tecniche specifiche di MITRE ATT&CK e dare priorità alle patch CVE.
- Gli IOC, come gli hash dei file, gli indirizzi IP e i nomi di dominio, sono essenziali per identificare e bloccare le attività dannose associate al ceppo di ransomware.

Use Case #3: Incident Response

Caso d'uso n. 3 - Risposta agli incidenti

MISP per la risposta

- I risponditori agli incidenti utilizzano MISP per condividere le informazioni sugli incidenti che hanno subito o che stanno risolvendo. Il motore di correlazione di MISP è ideale per la condivisione dei dati sugli incidenti, in quanto consente ai soccorritori di vedere rapidamente gli incidenti correlati.
- Nell'assistenza sanitaria: I soccorritori condividono le informazioni sui nuovi attor delle minacce,
  ceppi di malware, campagne di phishing, ecc.
- Il motore di correlazione aiuta i soccorritori a identificare rapidamente gli incidenti correlati e a intraprendere le azioni appropriate per ridurre al minimo l'impatto.
- I responsabili degli incidenti utilizzano il MISP per condividere i dettagli della campagna di phishing, compresi gli indirizzi dei mittenti delle e-mail, gli allegati dannosi e gli account utente compromessi.

Grazie

Presentatore: Stylianos Karagiannis (PDMFC, Portogallo) Si prega

di inviare tutte le domande a:
stylianos.karagiannis@pdmfc.com