Infrastrutture critiche e sicurezza per la salute

CSP008

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

Common Vulnerabilities

Settore sanitario

Vulnerabilità comuni

CVE-2021-34527: nota anche come "PrintNightmare", questa vulnerabilità interessa il servizio Print Spooler di Windows, consentendo potenzialmente agli aggressori remoti di eseguire codice arbitrario con i privilegi del sistema. Le organizzazioni sanitarie possono essere soggette allo sfruttamento se utilizzano sistemi Windows per la stampa di cartelle cliniche o altri documenti.

CVE-2021-44228: Denominata "Log4Shell", questa vulnerabilità critica riguarda la libreria di log Apache Log4j, comunemente utilizzata nelle applicazioni basate su Java. Lo sfruttamento di questa vulnerabilità potrebbe portare all'esecuzione di codice in modalità remota, esponendo potenzialmente dati sensibili dei pazienti nelle applicazioni sanitarie che utilizzano Log4j.

CVE-2019-0708: comunemente chiamata "BlueKeep", questa vulnerabilità riguarda l'implementazione del protocollo Remote Desktop Protocol (RDP) nelle versioni precedenti di Microsoft Windows. Se sfruttata, gli aggressori potrebbero eseguire codice arbitrario sui sistemi vulnerabili, compromettendo potenzialmente le reti e i sistemi sanitari.

Threat Groups

Settore sanitario

Gruppi di minacce nella sicurezza informatica

APT41: l'APT41 può condurre attacchi mirati contro le organizzazioni sanitarie utilizzando tecniche sofisticate, tra cui e-mail di spear-phishing contenenti allegati o link dannosi progettati per sfruttare le vulnerabilità dei sistemi sanitari.

- APT41 prende di mira la rete di un ospedale con e-mail di spear-phishing camuffate da comunicazioni legittime provenienti dalle autorità sanitarie. L'e-mail contiene malware che, se aperto da personale ignaro, compromette i sistemi dell'ospedale, consentendo all'APT41 di esfiltrare dati sensibili dei pazienti a scopo di spionaggio o di guadagno finanziario.

Deep Panda: Deep Panda può sfruttare le vulnerabilità dei sistemi sanitari per ottenere un accesso non autorizzato o condurre attività di spionaggio. Può utilizzare tattiche come gli exploit zero-day o gli attacchi alla catena di approvvigionamento per infiltrarsi nelle reti sanitarie.

- Deep Panda sfrutta una vulnerabilità zero-day in un software di gestione dei dispositivi medici ampiamente utilizzato e installato negli ospedali. Sfruttando questa vulnerabilità, ottiene l'accesso alle cartelle cliniche dei pazienti, ai dispositivi medici e ad altre informazioni sensibili, che utilizza a scopo di spionaggio.

Threat Groups Pt.2

Settore sanitario

Gruppi di minacce nella sicurezza informatica Pt.2

FIN4: FIN4 può prendere di mira i dipendenti del settore sanitario con sofisticate e-mail di phishing per rubare le credenziali di accesso alla posta elettronica e ad altre informazioni sensibili. Può anche sfruttare le vulnerabilità dei sistemi di posta elettronica per ottenere un accesso non autorizzato.

- FIN4 invia e-mail di phishing a dirigenti sanitari e personale finanziario, spacciandole per richieste legittime di informazioni finanziarie o opportunità di investimento. Quando i destinatari forniscono inconsapevolmente le loro credenziali, FIN4 ottiene l'accesso a dati finanziari riservati, che utilizza per l'insider trading o altri reati finanziari.

menuPass: menuPass può utilizzare varie tecniche, tra cui social engineering, malware e strumenti di accesso remoto, per compromettere le reti sanitarie e rubare informazioni sensibili.

- menuPass conduce una campagna di spear-phishing rivolta ai ricercatori sanitari che lavorano su trattamenti medici innovativi. Con l'inganno, i ricercatori scaricano allegati infettati da malware, che forniscono a menuPass l'accesso a preziosi dati di ricerca, proprietà intellettuale e informazioni sui pazienti.

Grazie

Presentatore: Stylianos Karagiannis (PDMFC, Portogallo)

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