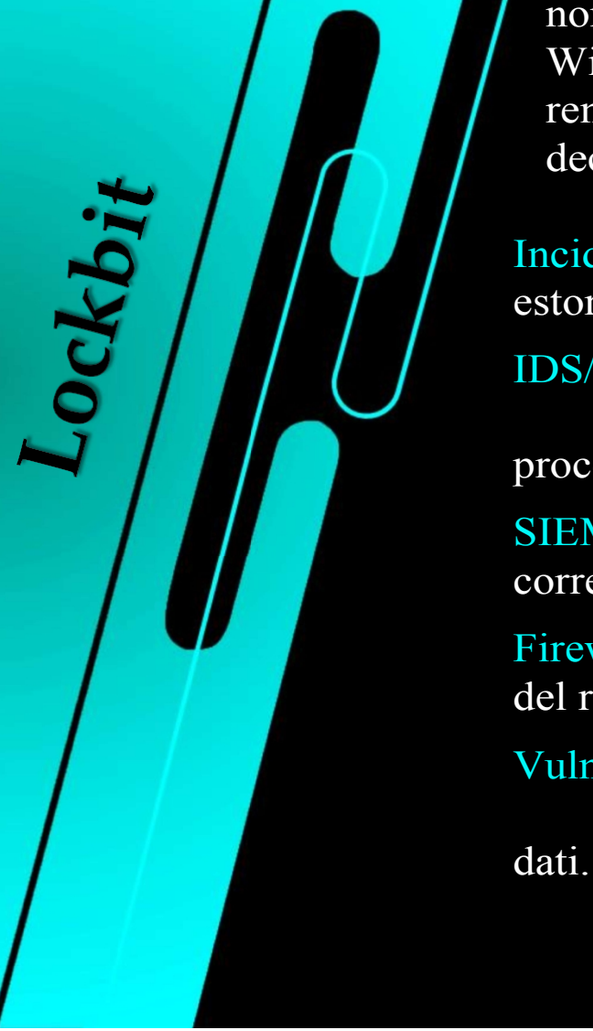
Infrastrutture critiche e sicurezza per la salute

CSP008

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

Scenari di attacco informatico

Lockbit



Il ransomware Lockbit si infiltra nella rete sanitaria attraverso e-mail di phishing o sistemi non patchati, prendendo di mira risorse critiche come il controller di dominio (DC) di Windows e gli host di Windows. Una volta all'interno, Lockbit cripta i dati sensibili, rendendoli inaccessibili, e richiede il pagamento di un riscatto per le chiavi di decriptazione.

Incidenti: Cifratura dei dati, interruzione dei servizi, potenziale perdita di dati, richieste di estorsione.

IDS/IPS: Rileva anomalo rete attività di rete associate con ransomware
processi di crittografia, attivando avvisi per indagini e risposte immediate.

SIEM: Centralizza i log e gli avvisi dai sistemi interessati, consentendo ai team di sicurezza di correlare gli eventi e rispondere rapidamente all'incidente.

Firewall: Blocca le connessioni di rete non autorizzate e impedisce gli spostamenti laterali. del ransomware all'interno della rete, contenendo la diffusione dell'infezione.

Vulnerabilità Valutazione: Identifica e patch vulnerabilità sfruttate dal ransomware, riducendo il rischio di future infezioni e violazioni dei dati.

Scenari di attacco informatico Pt.2

Negazione del servizio

Attori malintenzionati lanciano un attacco DDoS (Distributed Denial of Service) contro il sistema PACS Picture Archiving and Communication System), inondandolo con un volume di traffico spropositato. Ciò comporta l'indisponibilità dei dati di imaging medico e l'interruzione dei servizi sanitari.

Incidenti: Interruzione del servizio, negazione dell'accesso ai dati di imaging medico, potenziale impatto sulla cura del paziente.

IDS/IPS: Rileva e attenua i modelli di traffico anomalo indicativi di un DoS.
attacco, evitando che il sistema venga sopraffatto.

Firewall: Filtra e blocca il traffico dannoso diretto al PACS, garantendone la disponibilità e l'integrità.

Valutazione della vulnerabilità: Identifica le vulnerabilità dei PACS che potrebbero essere sfruttate in attacchi DoS, consentendo di adottare misure preventive per rafforzare la resilienza.

Grazie

Presentatore: Stylianos Karagiannis (PDMFC, Portogallo)

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