laboratorio SANITÀ 2030™
14-15 GIUGNO 2023 LOMBARDIA
FIERA DI BERGAMO

Sistema Socio Sanitario

Regione Lombardia

ASST Fatebenefratelli Sacco

# Contesto degli incidenti

## Response


Totale isolamento dell'azienda dalla rete pubblica
Isolamento datacenter da rete client


- Valutazione del danno
  - Cosa è stato colpito
  - Elenco e schema dei servizi aziendali
- Ricostruzione del patrimonio informativo
  - Elenco dei sistemi prioritari
  - Ordine di ripristino

Analisi incidente

# Contesto degli incidenti

## Analisi dell'incidente

Le analisi sugli incident si sono svolte in maniera congiunta tra:

- **S.I.A.** dell'ASST Fatebenefratelli Sacco
- CyberSecurity **ARIA**
- **Polizia Postale** e delle Telecomunicazioni (in raccordo con EUROPOL)
- **Agenzia per la CyberSicurezza Nazionale**

L'analisi è stata svolta seguendo metodologie di analisi forense analizzando artefatti rinvenuti su vari EndPoint degli Enti Sanitari.
Ha principalmente interessato EndPoint (Server e PDL) con S.O. Windows le cui credenziali esfiltrate sono state utilizzate per attaccare l'infrastruttura VmWare ESX

laboratorio SANITÀ 2030™
14-15 GIUGNO 2023 LOMBARDIA
FIERA DI BERGAMO

# Contesto degli incidenti

## Esito analisi

Nell'attacco si sono identificate tre macro fasi, molto comuni in attacchi sofisticati di questo tipo:

1. Una prima fase, nella quale un IAB (Initial Access Broker) ha ottenuto l'accesso all'infrastruttura attraverso attacchi sofisticati che hanno contemplato meccanismi complessi di offuscamento del codice per eludere la verifica di eventuali IOC noti.

2. Una ipotetica seconda fase in cui l'IAB ha messo all'asta e/o ceduto gratuitamente l'accesso al gruppo che ha portato avanti l'attacco RansomWare vero a proprio.

3. Una terza ed ultima fase nella quale l'attaccante ha portato a termine l'attacco, cifrando l'infrastruttura per renderla inutilizzabile.

# Contesto degli incidenti

## Conclusioni

### Impatto sui cittadini

- Impossibilità di accedere ai servizi non essenziali (Visite ambulatoriali, gestioni amministrative, cure secondarie, ecc..)

### Impatto sugli utenti aziendali

- Cambio di paradigma lavorativo
- Limitazione dei canali di comunicazione esterni (siti non correlato all'ambito lavorativo, mail personali, piattaforme di scambio files, ecc.)

### Impatto sui sistemi informativi

- Response team in grado di reagire ad incidenti (preparazione tecnica, conoscenza delle procedure d'emergenza, **capacità di lavorare sotto stress**)
- Rivoluzione della metodologia lavorativa

**Delitti in materia di violazione del diritto d'autore (Art. 25-novies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009]**

- Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, legge n.633/1941 comma 1 lett. a) bis)
- Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, legge n.633/1941 comma 3)
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis legge n.633/1941 comma 1)
- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis legge n.633/1941 comma 2)
- Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter legge n.633/1941)
- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies legge n.633/1941)
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies legge n.633/1941).

**Torna all'inizio**