UNIVERSITA’ DEGLI STUDI DI PADOVA
Dipartimento di Ingegneria dell’Informazione

Corso di Laurea in Ingegneria Informatica

Relazione per la prova finale

Ransomware: evoluzione, cicli di attacco e meccanismi di difesa

Relatore: Prof. Mauro Migliardi

Laureando: Carotta Stefano

Matricola n.: 2154272

ANNO ACCADEMICO 2025/2026

INTRODUZIONE

Questo lavoro nasce dalla volontà di analizzare una delle minacce informatiche più diffuse e dannose degli ultimi anni: il ransomware.

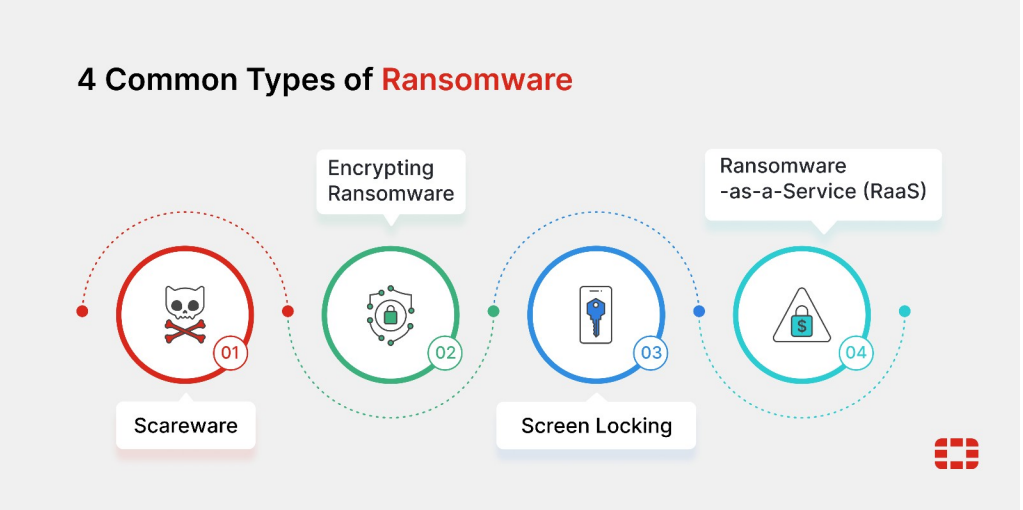
L’obbiettivo è quello di ricostruirne l’evoluzione storica ed analizzare i principali modelli teorici che ne descrivono il ciclo di attacco e le relative strategie di difesa.

COS'È UN RANSOMWARE?

Il ransomware è una tipologia di malware progettata per impedire l'accesso ai dati o ai sistemi della vittima, con l'obbiettivo di ottenere un riscatto.

TIPOLOGIE

- Crypto-ransomware → cifratura dei dati
- Locker ransomware → blocco dell'accesso al sistema
- Scareware → falsa minaccia
- Doxware/Leakware → minaccia di divulgazione
- RaaS → modello organizzativo ed economico
- Doppia estorsione → cifratura + esfiltrazione



EVOLUZIONE STORICA E SVOLTE DECISIVE

- 1989 – AIDS Trojan
- 2000-2010 – Ascesa ransomware moderni e nascita locker ransomware
- 2013 – CryptoLocker → crittografia forte + pagamento in criptovalute
- Affermazione modello RaaS → abbassa la barriera d'ingresso + maggiore diffusione
- 2017 – WannaCry e NotPetya → propagazione automatica su scala globale
- 2019/20 – Maze e introduzione della doppia estorsione
- Big Game Hunting → obbiettivi ad alto valore, riscatti più consistenti
- Oggi – Ransom Bazaar → modello più "imprenditoriale", trattative con le vittime

I MODELLI

Modelli lineari

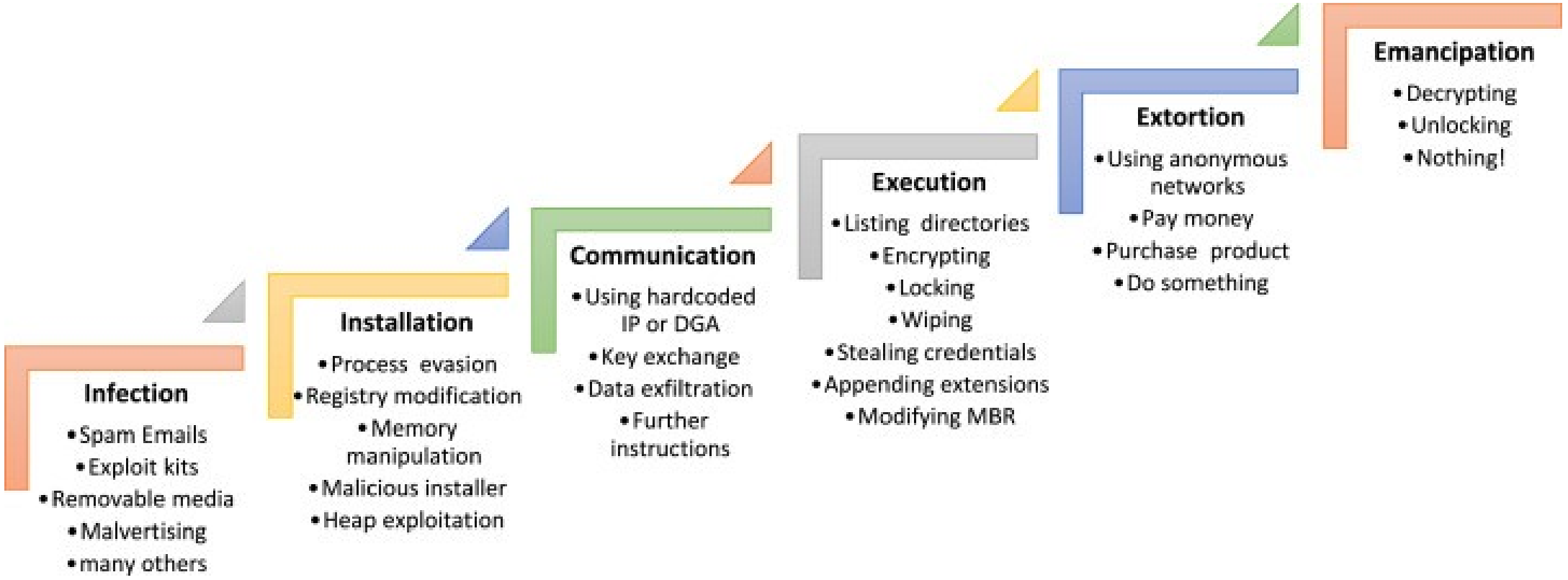
- I2CE3 (6 fasi)
- Cyber Kill Chain (6 fasi)
- Windows-based (4 fasi)
- Randep (8 fasi)

Modelli non lineari

- Crime script (prospettiva criminologica)
- Framework relazionale (dipendenza tra categorie di attacco)

IL MODELLO DI RIFERIMENTO: I2CE3

6 fasi: Infezione, Installazione, Comunicazione, Esecuzione, Estorsione, Emancipazione



FASI DI UN ATTACCO: ACCESSO E INSEDIAMENTO

FASE 1
Infezione

Infezione: il payload raggiunge la vittima attraverso vettori d'infezione, principalmente mail di phishing e exploit kit

Difese: filtri email, patch tempestive, formazione degli utenti

FASE 2
Installazione

Installazione: radicamento del malware nel sistema: code injection, strumenti di amministrazione remota, caricamento librerie, movimento laterale.

Difese: analisi statica e dinamica dei file, monitoraggio chiamate API

FASE 3
Comunicazione

Comunicazione: contatto con il server di comando e controllo, scambio chiave di cifratura e istruzioni

Difese: rilevamento traffico anomalo, blacklist indirizzi IP, honeypot di rete

FASI DI UN ATTACCO: ESECUZIONE E ESTORSIONE

FASE 4

Esecuzione

Esecuzione: cifratura, blocco o cancellazione delle risorse, esfiltrazione

Difese: monitoraggio attività I/O sul file system, backup isolati

FASE 5

Estorsione

Estorsione: richiesta di riscatto, solitamente in criptovalute, sfruttando tecniche di ingegneria sociale, ad esempio scadenze temporali

Difese: tracciamento delle transazioni

FASI DI UN ATTACCO: EMANCIPAZIONE

Emancipazione: liberazione (o no) delle risorse dopo il pagamento, logica “commerciale” in cui l’attaccante deve mantenere la sua reputazione e continuare a guadagnare

Difese: identificazione della famiglia per sfruttare eventuali strumenti noti

CONCLUSIONI

Comprendere le fasi di un attacco non è soltanto un esercizio teorico, ma la base per difese realmente efficaci

Nessuna singola contromisura è sufficiente, serve la combinazione di diverse difese calibrate su ogni fase