W19D4 – Pratica
Epic Education Srl

Analisi di rete
CSIRT ITALIA (ACN)
Campagna phishing Trenitalia

Simone Giordano

19/11/2025

Contatti:
Tel: 3280063044
Email: mynameisimone@gmail.com
Linkedin: https://www.linkedin.com/in/simone-giordano-91290652/

Sommario

Analisi di rete
Esercizio 1

Traccia

Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto. Trovate in allegato una cattura di rete effettuata con Wireshark. Analizzate la cattura attentamente e rispondere ai seguenti quesiti:
Identificare eventuali IOC, ovvero evidenze di attacchi in corso
In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
Consigliate un'azione per ridurre gli impatti dell'attacco

Esercizio

Dall'analisi è possibile rilevare molteplici richieste TCP, il Syan-Ack viene completato su alcune porte, in questi casi le porte sono aperte. Questo comportamento fa pensare a una scansione.

IOC: molteplici richieste TCP da 192.168.200.100 verso 192.168.200.150
Potenziali vettori di attacco: scansioni di rete per rilevare le porte aperte.
Per **limitare i rischi** si potrebbe impostare una policy del firewall bloccando le richieste provenienti dall'IP 192.168.200.100.

Di seguito i risultati che rilevano appunto le porte aperte e quelle chiuse o filtrate.

IP sorgente	IP destinazione	Porta sorgente	Porta destinazione	Risposta	Stato porta
192.168.200.100	192.168.200.150	53060	**80**	SYN-ACK (#4)	**APERTA**
192.168.200.100	192.168.200.150	33876	**443**	**RST-ACK** (#5)	**CHIUSA**
192.168.200.100	192.168.200.150	41304	**23 (Telnet)**	SYN-ACK (#19)	**APERTA**
192.168.200.100	192.168.200.150	56120	**111 (RPCbind)**	SYN-ACK (#20)	**APERTA**
192.168.200.100	192.168.200.150	33878	**443**	RST-ACK (nessun SYN-ACK)	**CHIUSA**
192.168.200.100	192.168.200.150	58636	**554 (RTSP)**	Nessuna risposta → no SYN-ACK	**CHIUSA / FILTRATA**
192.168.200.100	192.168.200.150	52358	**135 (RPC/DCOM)**	Nessuna risposta → no SYN-ACK	**CHIUSA / FILTRATA**
192.168.200.100	192.168.200.150	46138	**993 (IMAPS)**	Nessuna risposta → no SYN-ACK	**CHIUSA / FILTRATA**
192.168.200.100	192.168.200.150	41182	**21 (FTP)**	Nessuna risposta → no SYN-ACK	**CHIUSA / FILTRATA**

CSIRT ITALIA (ACN)
Facoltativo parte 1

Traccia

Cos'è il CSIRT Italia (ACN)?
Quali sono i suoi compiti?

Esercizio

Il **CSIRT Italia (Computer Security Incident Response Team)** è la struttura nazionale che si occupa di prevenire, monitorare e gestire gli incidenti di sicurezza informatica che riguardano il Paese.
Fa parte dell'**Agenzia per la Cybersicurezza Nazionale (ACN)**.
È il punto di riferimento nazionale per la risposta agli incidenti cyber.
Coordina attività di prevenzione, gestione e comunicazione degli eventi di sicurezza che possono colpire:

- Pubbliche Amministrazioni
- Infrastrutture critiche
- Aziende strategiche
- Operatori di servizi essenziali (energia, trasporti, telecomunicazioni, ecc.)
- Cittadini e imprese, tramite avvisi e comunicazioni ufficiali

Compiti principali del CSIRT Italia

1. Monitoraggio e allerta

- Raccoglie informazioni sulle minacce informatiche emergenti.
- Pubblica **alert**, bollettini e indicatori di compromissione (IoC).
- Avverte tempestivamente enti e organizzazioni quando individua vulnerabilità critiche.

2. Gestione e risposta agli incidenti

- Supporta le organizzazioni italiane nella gestione di attacchi informatici.
- Coordina la risposta durante incidenti rilevanti o su larga scala.
- Fornisce assistenza tecnica e operativa nei casi più gravi.

3. Analisi degli attacchi e threat intelligence

- Analizza malware, campagne di phishing, ransomware, DDoS, e altre minacce.
- Produce report di intelligence e raccomandazioni operative.

4. Coordinamento nazionale e internazionale

- Collabora con:
  - CSIRT degli altri Paesi UE
  - ENISA
  - CERT e organismi internazionali
- È coinvolto nel **Network CSIRTs europeo** previsto dalla direttiva **NIS2**.

5. Prevenzione e supporto alla sicurezza

- Supporta le organizzazioni nel rafforzare le proprie difese.
- Diffonde buone pratiche di sicurezza e aggiornamenti su vulnerabilità.
- Gestisce la piattaforma nazionale di condivisione di informazioni sulle minacce.

6. Comunicazione al pubblico

- Pubblica avvisi per cittadini e imprese su:
  - campagne di phishing in corso,
  - vulnerabilità critiche,
  - truffe online,
  - consigli di prevenzione.

Campagna phishing Trenitalia

Facoltativo parte 2

Traccia

Esamina l'allerta: https://www.csirt.gov.it/contenuti/campagna-phishing-a-tema-sondaggio-trenitalia-al03-2403 22-csirt-ita

Come puoi proteggere la tua organizzazione da questa campagna phishing?

Esercizio

Gli utenti e le organizzazioni possono far fronte a questa tipologia di attacchi verificando scrupolosamente le e-mail ricevute e attivando le seguenti misure aggiuntive:

- fornire periodiche sessioni di formazione finalizzate a riconoscere il phishing diffidando da comunicazioni inattese;
- verificare il dominio delle e-mail ricevute: eventuali mail legittime di Trenitalia provengono dai domini ufficiali quali @trenitalia.it o @fsitaliane.it;
- non accedere a collegamenti internet o a relativi contenuti esterni se non si è certi dell'affidabilità della risorsa: eventuali sondaggi legittimi, oltre ad essere sponsorizzati anche tramite canali social, dovrebbero portare l'utenza verso il sito ufficiale di Trenitalia;
- accertarsi della legittimità dei siti che richiedono l'inserimento dei propri dati personali: organizzazioni come Trenitalia non richiedono l'inserimento di dati sensibili, come i dati delle carte di credito, tramite sondaggi.

Infine, si raccomanda di valutare la verifica e l'implementazione - sui propri apparati di sicurezza - degli Indicatori di Compromissione (IoC[1]) forniti di seguito.

url	hxxps://fancymeshop[.]com/l/G7b9787S8a4a6tGWLKDzkxiPT/payment?token=eyJpdiI6ImczOHRjaGtsOGVGUW5Da2dFcG90TUE9PSIsInZhbHVlIjoiZEpRR 2e08e2fe516e&_sid=eyJpdiI6IkxKQmFwazA4Z3JrdG0rTHFReitDMVE9PSIsInZhbHVlIjoidHEvelBxMnN1RDAxWEUzWW56T0N2N1dSUUVoNDJNQlozN2x4d L1FYOGl1VVA2ZWZ0RnBoRDIxZzVxMUxFckpRNiIsIm1hYyI6IjkzMTY0MjM4Yzk4YTMwNjlmNjc0OTcyYzUxNTU1NzAyMDdiZGI4ZGI4MTViNmNkNDg0MTgz
url	hxxps://accessstoffersdirect[.]sbs/l/G7b9787S8a4a6tGWLKDzkxiPT?offer_id=10616&s1=102fe395854025aa8882f92d698258&s2=1029&s3=1377&s4=#r
url	hxxps://pelagiancampanile[.]shop/?encoded_value=279768Q&sub1=5f82724c80e843338d4907622dcf5279&sub2=&sub3=&sub4=&sub5=12990&sourc
url	hxxp://travell[.]store/#cl/15651_md/4/110108/94/210/18460

url	hxxps://link[.]mail[.]beehiiv[.]com/ls/click?upn=QQCcmWuavKz0lTcVCvz5s53FxcZVR-2BTUi-2FSz1fz4RL4-3DLfZX_WhZ1LpnDLanQed5Yrjccsa790MLhXkJe 2Bzvu0md0rCV1fFLXjqGpG0AJeU1p9TOGefymXNjQYCtQoXhpsZUiqH3Yzdrctixpz1KRLKiGIp4gCuWUbYRJ0ORlMyjGn3kx6dfvQISQs3RJob354b1966Mn5Kk
domain	fancymeshop[.]com
domain	accessstoffersdirect[.]sbs
domain	pelagiancampanile[.]shop
domain	travell[.]store
domain	link[.]mail[.]beehiiv[.]com