mercoledì 20 novembre 2024 15:22

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

Dalla cattura notiamo che ci sono un numero elevato di richieste TCP (SYN) su porte sempre diverse in destinazione, questo ci fa pensare ad una potenziale scansione in corso da parte dell'host 192.168.200.100 verso l'host target 192.168.200.150.

Questa ipotesi è supportata dal fatto che per alcune righe della cattura vediamo risposte positive del target [SYN+ACK] ad indicare che la porta è aperta. Per altre, invece, notiamo la risposta [RST+ACK] ad indicare che la porta è chiusa. Lato target, si potrebbero configurare delle policy firewall per bloccare accesso a tutte le porta da parte di quel determinato attaccante, in modo tale da evitare che informazioni circa porta / servizi in ascolto finiscano nella mani dell'attaccante

o.	Time	Source	Destination	Protocol	Length	Info
118	36.779605648	192.168.200.150	192.168.200.100	TCP	60	214 → 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
119	36.779605750	192.168.200.150	192.168.200.100	TCP	60	106 → 46886 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
120	36.779605798	192.168.200.150	192.168.200.100	TCP	60	138 → 50204 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
121	36.779605843	192.168.200.150	192.168.200.100	TCP	60	884 → 51262 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
122	36.779637573	192.168.200.100	192.168.200.150	TCP	74	44244 → 699 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
123	36.779776288	192.168.200.100	192.168.200.150	TCP	74	43630 → 703 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
124	36.779856041	192.168.200.150	192.168.200.100	TCP	60	699 → 44244 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
125	36.779911109	192.168.200.100	192.168.200.150	TCP	74	55136 → 274 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
126	36.779946174	192.168.200.100	192.168.200.150	TCP	74	40522 → 42 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
127	36.780035851	192.168.200.150	192.168.200.100	TCP	60	703 → 43630 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
128	36.780121127	192.168.200.150	192.168.200.100	TCP	60	274 → 55136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
129	36.780149473	192.168.200.100	192.168.200.150	TCP	74	57552 → 58 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
130	36.780170333	192.168.200.100	192.168.200.150	TCP	74	40822 → 266 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
131	36.780215176	192.168.200.150	192.168.200.100	TCP	60	42 → 40522 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
132	36.780301750	192.168.200.150	192.168.200.100	TCP	60	58 → 57552 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
133	36.780325837	192.168.200.100	192.168.200.150	TCP	74	37252 → 11 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
134	36.780346429	192.168.200.100	192.168.200.150	TCP	74	40648 → 235 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
135	36.780409818	192.168.200.100	192.168.200.150	TCP	74	36548 → 739 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
136	36.780427899	192.168.200.100	192.168.200.150	TCP	74	38866 → 55 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
137	36.780472830	192.168.200.100	192.168.200.150	TCP	74	52136 → 999 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
138	36.780490897	192.168.200.100	192.168.200.150	TCP	74	38022 → 317 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
139	36.780577880	192.168.200.150	192.168.200.100	TCP	60	266 → 40822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
140	36.780577981	192.168.200.150	192.168.200.100	TCP	60	11 → 37252 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
141	36.780578026	192.168.200.150	192.168.200.100	TCP	60	235 → 40648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
142	36.780578074	192.168.200.150	192.168.200.100	TCP	60	739 → 36548 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
143	36.780578119	192.168.200.150	192.168.200.100	TCP	60	55 → 38866 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
144	36.780578158	192.168.200.150	192.168.200.100	TCP	60	999 → 52136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
145	36.780578198	192.168.200.150	192.168.200.100	TCP	60	317 → 38022 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
146	36.780617671	192.168.200.100	192.168.200.150	TCP	74	49446 → 961 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
147	36.780701625	192.168.200.100	192.168.200.150	TCP	74	51192 → 241 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
148	36.780805705	192.168.200.150	192.168.200.100	TCP	60	961 → 49446 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
149	36.780824718	192.168.200.100	192.168.200.150	TCP	74	42642 → 293 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
150	36.780889399	192.168.200.150	192.168.200.100	TCP	60	241 → 51192 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
151	36.780906540	192.168.200.100	192.168.200.150	TCP	74	41828 → 974 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK

Facoltativo:

● Cos'è il CSIRT Italia (ACN)?

Il CSIRT Italia è un'unità dell'ACN (Agenzia per la Cybersicurezza Nazionale) che aiuta a proteggere le organizzazioni dai cyberattacchi. Forniscono informazioni e consigli su come stare al sicuro online, aiutando le organizzazioni a rispondere agli incidenti informatici e collaborando con altre organizzazioni per combattere la cybercriminalità.

● Quali sono i suoi compiti?

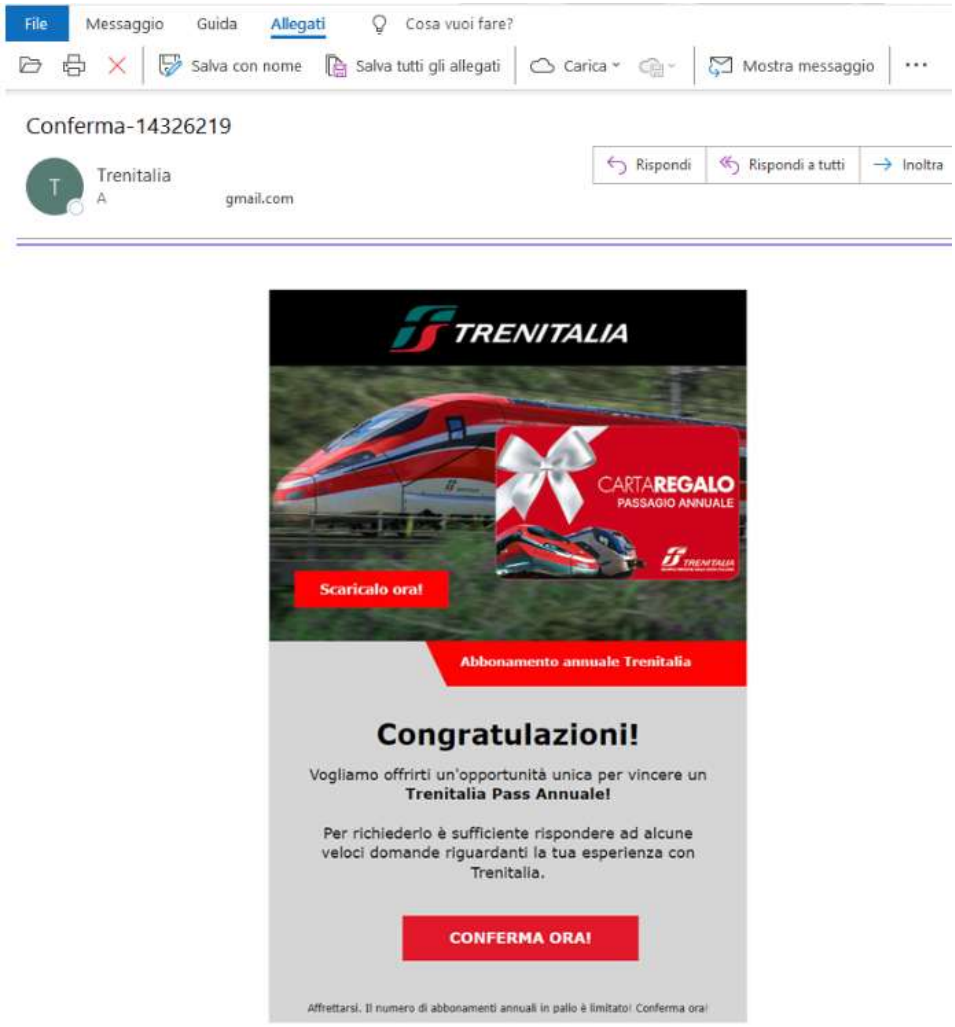
I compiti del CSIRT sono definiti dal Decreto Legislativo 18 maggio 2018, n. 65 e dal Decreto del Presidente del Consiglio dei ministri 8 agosto 2019 art. 4. Essi includono:

- il monitoraggio degli incidenti a livello nazionale;
- l'emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti;
- l'intervento in caso di incidente;
- l'analisi dinamica dei rischi e degli incidenti;
- la sensibilizzazione situazionale;
- la partecipazione alla rete dei CSIRT.

Il CSIRT stabilisce relazioni di cooperazione con il settore privato.
Per facilitare la cooperazione, il CSIRT promuove l'adozione e l'uso di prassi

comuni o standardizzate nei settori delle procedure di trattamento degli incidenti e dei rischi e sistemi di classificazione degli incidenti, dei rischi e delle informazioni.

● Esamina l'allerta: ○ https://www.csirt.gov.it/contenuti/campagna-phishing-a-tema-sondaggio-trenitalia-al03-240322-csirt-ita



● Come puoi proteggere la tua organizzazione da questa campagna phishing?

Azioni di mitigazione

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 le azioni di mitigazione e implementando gli IoC suggeriti.