La cattura di rete che ho analizzato presenta una serie di anomalie che suggeriscono la presenza di attività sospette o malintenzionate. Nello specifico, si notano **numerosi pacchetti TCP con il flag "RST" (Reset)**. Questo potrebbe indicare che una delle parti coinvolte nella comunicazione sta **terminando le connessioni in modo inaspettato**, il che è tipico di attacchi come il Denial of Service (DoS) o di una scansione di rete aggressiva. Gli attacchi DoS, come il **SYN flood**, sono progettati per sopraffare un server con richieste di connessione, bloccando o rallentando il servizio.

In aggiunta, la cattura mostra **un numero elevato di pacchetti SYN**, inviati a breve distanza temporale l'uno dall'altro. Questo è un comportamento classico di un **tentativo di SYN flood**, un attacco che mira a esaurire le risorse di un server saturando le connessioni aperte. La presenza di questi pacchetti senza un corretto completamento del **Three-Way Handshake** conferma la natura sospetta del traffico.

Un altro aspetto rilevante è l'uso del flag TCP **SACK_PERM**, che si riferisce alla funzionalità Selective Acknowledgment. Anche se questa opzione è legittima, in passato è stata sfruttata per vulnerabilità come **CVE-2019-11477**, nota come "SACK Panic". Sebbene non vi siano prove concrete che questo attacco sia in corso, la sua presenza nella cattura, insieme agli altri segnali, suggerisce che potrebbero essere in atto tentativi di sfruttare questa vulnerabilità.

Inoltre, si osserva una sequenza di pacchetti **ACK inviati senza risposta adeguata dall'altro host**. Questo comportamento può indicare una **scansione di rete** o un tentativo di brute force contro un servizio specifico, dato che l'attaccante potrebbe cercare di verificare quali porte o servizi sono aperti sul sistema vittima.

Alla luce di queste osservazioni, è possibile ipotizzare che siano in corso **tentativi di attacco di tipo DoS o una scansione aggressiva della rete**. Gli **Indicatori di Compromissione (IOC)**

rilevati sono chiari segnali che l'attaccante sta cercando di individuare punti deboli o di sopraffare i servizi di rete.

Per mitigare l'attacco e ridurre l'impatto, consiglio diverse azioni. Prima di tutto, è necessario **implementare un sistema di prevenzione contro attacchi DoS**, ad esempio con firewall configurati per rilevare e bloccare traffico anomalo come i pacchetti SYN flood. In aggiunta, si potrebbe utilizzare **rate-limiting** per limitare il numero di richieste di connessione simultanee, prevenendo così il sovraccarico del server.

Un'altra azione importante è **identificare e bloccare gli indirizzi IP** da cui proviene il traffico sospetto. Questo blocco tempestivo può ridurre la superficie d'attacco e limitare ulteriori tentativi di connessione malevola. Inoltre, è raccomandabile applicare **patch di sicurezza aggiornate** per mitigare vulnerabilità note nel protocollo TCP, come la già menzionata vulnerabilità **CVE-2019-11477**, che sfrutta proprio il TCP SACK.

Infine, per garantire una protezione a lungo termine, consiglio di **attivare un monitoraggio continuo del traffico di rete**. Un sistema di intrusion detection può rilevare comportamenti anomali in tempo reale, consentendo di intervenire prontamente e bloccare eventuali attacchi futuri prima che possano causare danni significativi.

FACOLTATIVO

1. Cos’è il CSIRT Italia (ACN)?

Il **CSIRT Italia**, che fa parte dell'Agenzia per la Cybersicurezza Nazionale (ACN), è il principale team nazionale incaricato di gestire e rispondere agli incidenti di sicurezza informatica in Italia. Il suo ruolo è essenziale per la difesa delle infrastrutture critiche e del cyberspazio italiano. Mi occupo della gestione e del monitoraggio

degli incidenti informatici, fornendo assistenza e supporto a enti pubblici e privati per garantire la sicurezza informatica nazionale.

2. Quali sono i suoi compiti?

I principali compiti del **CSIRT Italia** includono:

- **Monitoraggio delle minacce**: mi occupo della sorveglianza costante delle attività malevole nel cyberspazio italiano e dell'analisi di minacce emergenti. Questo ci permette di rilevare rapidamente attacchi informatici, come campagne di phishing, malware e altre attività malevole.
- **Coordinamento delle risposte**: quando si verifica un incidente di sicurezza informatica, coordino le risposte operative e tecniche tra organizzazioni diverse, garantendo che le misure adottate siano efficienti ed efficaci. Questo implica contattare le organizzazioni colpite, proporre misure di contenimento e mitigazione e, ove necessario, cooperare con le forze dell'ordine.
- **Diffusione di avvisi di sicurezza**: io e il mio team pubblichiamo regolarmente avvisi e allarmi su nuove vulnerabilità o attacchi in corso, come la campagna di phishing su Trenitalia. Questi avvisi sono fondamentali per avvertire e informare le aziende e i cittadini sui pericoli imminenti.
- **Formazione e prevenzione**: forniamo linee guida e suggerimenti per aiutare le organizzazioni a rafforzare le loro difese informatiche. Mi occupo di promuovere le buone pratiche di sicurezza e di incentivare l'adozione di soluzioni tecnologiche sicure.

3. Esamina l’allerta di phishing "Sondaggio Trenitalia"

L’allerta pubblicata dal **CSIRT Italia** riguarda una campagna di phishing a tema **Trenitalia**. L'attacco sfrutta il nome del noto servizio ferroviario per ingannare gli utenti. In questa campagna, gli attaccanti inviano email che sembrano provenire da Trenitalia, contenenti un invito a partecipare a un sondaggio fittizio. Il fine è quello di indurre le vittime a cliccare su link malevoli che li portano a siti truffaldini, progettati per raccogliere dati sensibili, come credenziali di accesso o informazioni finanziarie. Le email sono costruite per sembrare legittime, sfruttando loghi e linguaggio tipico di Trenitalia, ma il loro obiettivo è l'acquisizione fraudolenta di informazioni personali.

Come operatore di sicurezza informatica, mi assicuro che tutti i dettagli di queste campagne vengano analizzati a fondo, verificando gli indicatori di compromissione (IOC) e allertando le organizzazioni e i cittadini. Questi tipi di attacchi mirano spesso a sfruttare la fiducia delle persone nei confronti di marchi riconosciuti, come Trenitalia, rendendo fondamentale la tempestiva comunicazione dell'allerta.

4. Come posso proteggere la mia organizzazione da questa campagna phishing?

Per proteggere la mia organizzazione da questa campagna di phishing specifica, adotto una serie di misure preventive e reattive.

- **Formazione del personale**: Il primo passo che adotto è educare i dipendenti su come riconoscere le email di phishing. Organizzo corsi e seminari per spiegare le tecniche usate dagli attaccanti, come l'uso di link sospetti o richieste insolite di informazioni personali. Attraverso esempi pratici, aiuto il personale a sviluppare l'abilità di individuare email malevole, evitando così di cadere nella trappola.
- **Filtri anti-phishing e monitoraggio del traffico**: Implemento soluzioni tecnologiche avanzate, come filtri anti-phishing a

livello di server email. Questi sistemi bloccano preventivamente i messaggi sospetti prima che raggiungano le caselle di posta degli utenti. Allo stesso tempo, monitoro il traffico di rete alla ricerca di comportamenti anomali o tentativi di collegamento a siti noti per essere associati a campagne di phishing.

- **Autenticazione a due fattori (2FA)**: Un'altra misura chiave che adotto è l'implementazione dell'autenticazione a due fattori per tutti gli accessi ai sistemi critici. Questo garantisce che, anche nel caso in cui le credenziali venissero compromesse attraverso una campagna di phishing, l'attaccante non sarebbe in grado di accedere ai sistemi senza il secondo fattore di autenticazione, che spesso è un token fisico o una notifica inviata a un dispositivo sicuro.
- **Patch di sicurezza regolari**: Mi assicuro che tutti i software e i sistemi operativi utilizzati nell'organizzazione siano aggiornati con le ultime patch di sicurezza. Gli attaccanti spesso sfruttano vulnerabilità note in software non aggiornati per lanciare attacchi più sofisticati dopo una campagna di phishing.
- **Simulazioni di phishing**: per mantenere alta la vigilanza, organizzo regolari simulazioni di phishing all'interno dell'organizzazione. Inviamo email finte per valutare le reazioni del personale e forniamo feedback formativo immediato a chi cade nella simulazione, in modo che possano imparare dai propri errori in un ambiente sicuro.
- **Monitoraggio continuo e risposta agli incidenti**: infine, implemento un sistema di monitoraggio continuo e risposta agli incidenti (SOC), che analizza in tempo reale i flussi di dati in entrata e in uscita, rilevando tempestivamente attività anomale e segnalando potenziali compromissioni. Quando un sospetto incidente viene rilevato, attivo le procedure di risposta immediata, bloccando i contatti malevoli e avviando un'analisi forense per valutare i danni e mitigare ulteriori rischi.

Adottando queste misure, riesco a garantire una protezione efficace contro le campagne di phishing, come quella segnalata dal **CSIRT Italia** legata a **Trenitalia**, minimizzando i rischi e mantenendo l'integrità dei sistemi e delle informazioni aziendali.