Raul Pastor

IoC

È stata rilevata una potenziale scansione di rete originata dall'host 192.168.200.100 verso il 192.168.200.150, caratterizzata da numerose richieste TCP su porte variabili. La presenza di risposte differenziate ([SYN+ACK] per porte aperte e [RST+ACK] per porte chiuse) convalida il tentativo di enumerazione dei servizi. Si consiglia di procedere tempestivamente con l'inibizione dell'IP attaccante tramite regole di filtraggio sul firewall del target.

Compito facoltativo:

Il CSIRT Italia è istituito presso l'Agenzia per la cybersicurezza nazionale.

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;
- servizio di monitoraggio delle potenziali vulnerabilità sugli asset esposti.

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.