ESERCIZIO W19D1

L’esercizio si concentra sul creare un elenco di minacce comuni che possono colpire un’azienda. La traccia espone questi punti:

- Inizia raccogliendo informazioni sulle minacce alla sicurezza informatica, utilizzando fonti aperte, i siti web di sicurezza informatica e i forum di discussione.
- Analizza ciascuna minaccia in dettaglio, cercando di comprendere il modo in cui può essere utilizzata per compromettere la sicurezza informatica e i danni che può causare.
- Utilizza queste informazioni per creare un elenco delle minacce più comuni, tra cui malware, attacchi di phishing e attacchi DDoS aggiungendo tutte le informazioni raccolte dall’analisi.

OSINT

Procediamo con la raccolta di informazioni. Un ente pubblico ideale, che rilascia un report contenente le maggiori minacce dell’anno, prende il nome di ENISA. Da qui ricaviamo le news pertinenti vari vettori di attacco.

Analisi vettori

Ransomware: un attacco che consente agli attaccanti di prendere il controllo del client, ponendo al proprietario la richiesta di riscatto. Gli elementi principali che costituiscono un ransomware sono:

- Assets
- Azioni
- Blackmail

Il ransomware adopera differenti metodi di estorsione e si concentra a volte anche su obiettivi diversi dal guadagno. Lockbit, alphv e bian sono senz'altro i ransomware più attuali di questi anni.

Malware: Spesso anche definito codice malevolo, il malware è un software o un firmware che effettua azioni non autorizzate, in grado di avere un impatto serio sulla confidenzialità, l'integrità e la disponibilità di un dato sistema. Possono essere virus, worms, trojan o altre entità di codice.

L'obiettivo di un attaccante che usa il malware può essere il controllo del sistema o network attaccato, rubare informazioni o rendere certi servizi inutilizzabili. In questo periodo cresce l'uso di spyware commerciali, cosi come wiper Sandworm distruttivi messi in campo dai gruppi APT della Russia.

Social Enginnering: Include un range di attività che punta a ottenere informazioni sensibili andando a sfruttare il fattore umano. Gli utenti possono essere invogliati ad aprire documenti, file, e-mail, oppure link infetti che conducono a siti non affidabili.

I vettori che interessano il Social Enginnering sono il Phishing, Spear Fishing, Whaling, Smishing, Vishing e Watering hole attack.

Data breach: Consiste nell'accesso non autorizzato ai dati, che può portare alla distruzione, alla perdita o alla distribuzione di informazione sensibili degli stessi. Parliamo di Data breach, Data leak e Data manipulation.

Denial of Service: Un attacco web che punta all'annullamento di un sistema o del servizio di un sistema, spesso avviati tramite bot. Il vettore non è nuovo, ma si è evoluto nel corso degli anni. Di recente si utilizza molto una variazione del Dos, ovvero l'RDos. Si prende di mira un sistema vulnerabile e poi si invia una lettera di estorsione alle vittime, per rilasciare il bersaglio preso in ostaggio.

Internet threat: Un intenzionale distruzione dei servizi di networking di una certa locazione o popolazione, per la ritenzione delle informazioni. Access Now ha constatato che non solo i servizi stanno riemergendo dopo il Covid, ma stanno diventando sempre più lunghi. L'annullamento di internet privano le popolazioni della connessione durante periodi critici, come crisi umanitarie, proteste oppure conflitti armati.