W19D1 – threat intelligence

Esercizio obbligatorio

Il sistema di valutazione di ThreatConnect permette di valutare il grado di affidabilità di una informazione per la valutazione e l'identificazione di una minaccia su una scala di 6 o 7 livelli e di classificare la criticità di una minaccia su una scala di 6 livelli. Per quanto riguarda l'affidabilità dell'informazione, al livello più basso c'è un'informazione "unassessed" che ha uno score pari a 0 per informazioni non ancora verificate. Al livello successivo vi sono le minacce "screditate", per cui una minaccia è stata screditata dalle informazioni e non è quindi reale. Lo score in questo è caso è di 1. Al livello successivo, con uno score da 2 a 29, il livello è "improbabile", per cui è possibile valutare un'informazione circa una minaccia, anche se non conviene farlo a causa di informazioni discordanti. Nel livello successivo, con un punteggio da 30 a 49, la minaccia è "incerta", perché si possono valutare le informazioni, ma non sono sufficienti per identificare e comprendere la possibile minaccia. La minaccia è "possibile" con un punteggio da 50 a 69, per cui ci sono delle evidenze concrete di avere a che fare con una minaccia, ma non è ancora possibile confermare questa minaccia. La minaccia è "probabile" quando ottiene un punteggio tra 70 e 89 e ci sono stati vari segnali ed informazioni che sembrano confermare che la minaccia sia reale, anche se serve effettuare ancora delle verifiche. La minaccia è "confermata" con uno score da 90 a 100, che dimostra come la minaccia sia concreta e reale sulla base di più informazioni raccolte da più fonti. ThreatConnect permette di classificare una minaccia anche in base alla sua gravità con il Threat Rating, che assegna da 0 a 5 teschi in base alla severità della minaccia. Se non vi sono informazioni per valutarla, la minaccia è "sconosciuta" e non viene assegnato nessun teschio. Con un teschio si contrassegnano le minacce "sospette", per cui non è stata ancora rilevata con certezza un'attività malevola, anche se sono presenti delle anomalie che possono ricollegarsi ad un'attività malevola. Si ha una "low threat" con due teschi se si affronta un avversario non troppo esperto che compie attività non sofisticate, mentre con tre teschi si parla di una "moderate threat", per cui l'avversario è capace e sa portare avanti delle azioni in modo diretto e mirato. Quattro teschi indicano una "high threat", per cui l'avversario ha competenze avanzate, è già entrato in un sistema e sa mantenere gli accessi sui sistemi compromessi. Si parla di "critical threat" con cinque teschi, quando l'attaccante è estremamente competente e riesce ad arrecare danni in ogni fase del suo attacco.

Esercizio facoltativo

Ci sono numerose minacce che possono colpire le aziende e in questo report intendo analizzare le più comuni minacce in ambito internazionale per poi concentrarmi sulle minacce che hanno colpito specificamente l'Italia. Una delle minacce più diffuse in ambito internazionale è quella del phishing, che rimane molto diffuso e causa da solo il 36% dei casi di data breach, come si legge nel rapporto di Verizon 's data breach investigations report (DBIR). Con il phishing è molto facile imitare quasi perfettamente email o altri messaggi legittimi e indurre le vittime a farsi consegnare dati sensibili come dati bancari o di login. Il

rapporto 2023 ENISIA Threat Landscape report riporta che il phishing è ancora molto diffuso tra gli attacchi di social engineering e spesso rappresenta il primo passo in attacchi cyber strutturati, ad esempio con dei ransomware o altri tipi di malware. Tra le principali minacce cyber contro le aziende figurano proprio i ransomware, che risultano la tipologia di malware più utilizzata contro le aziende secondo le ricerche di IBM X-Force Threat Intelligence Index 2023. Criptano i dati delle aziende per ottenere un riscatto e stanno diventando sempre più distruttivi, puntando spesso anche su infrastrutture critiche ed IBM stima che il costo totale nel mondo dei danni causati da attacchi ransomware sia stato pari a 4,5 milioni di dollari. I ransomware sono particolarmente minacciosi perché possono portare a lunghi periodi di blocco delle attività, a costi anche elevati per i riscatti e a danni anche in termini di reputazione per le aziende colpite. Sono così temibili che secondo il rapporto Global Cybersecurity Outlook 2023 del World Economic Forum sono tra le principali preoccupazioni per le aziende, con una crescita dell'85% tra il 2020 e il 2022 degli attacchi ransomware. Sono sempre più diffusi gli attacchi BEC, ossia Business Email Compromise, per cui un malintenzionato riesce ad accedere ad una email ufficiale in ambito business, magari tramite il phishing, e la utilizza per delle attività malevole, ad esempio per delle transazioni o per inviare delle fatture fraudolente e autorizzare pagamenti di vario tipo. Vengono spesso bersagliati dirigenti o dipartimenti finanziari e l'impatto economico di questa minaccia cyber è molto grave, tanto che si stima che il 75% delle aziende abbia subito almeno un episodio di questo tipo e secondo FBI's Internet Crime Complaint Center è il tipo di crimine informatico con il maggiore impatto economico nel 2022, pari a 2.4 miliardi di dollari. Da attenzionare anche gli attacchi DDoS, ossia Distributed Denial of Service, che implicano la saturazione delle risorse di un sito, di una applicazione o un server con un traffico di rete massiccio. Secondo il Threat Intelligence Report di NETSCOUT del 2023 gli attacchi crescono ad un ritmo di circa il 15% ogni anno, diventando sempre più complessi e duraturi. Secondo il report di ENISA del 2023, spesso le campagne di DDoS sono accompagnate anche da attacchi ransomware, rendendo gli attacchi ancora più impattanti dal punto di vista economico e reputazionale, allungando il downtime di un servizio o di una rete. Non bisogna abbassare la guardia nemmeno contro quelle che si definiscono "insider threats", causate da sabotatori interni come dipendenti scontenti o partner che cercano di rubare dati e causare danni finanziari, legati anche a diritti di proprietà intellettuale. Secondo IBM il costo medio delle insider threats nel 2023 era di 11,45 milioni per ogni incidente e richiede circa 85 giorni per essere contenuto e scoperto, essendo molto più complesso individuare una minaccia interna. Secondo il Ponemon Institute Insider Threat Report del 2023, negli ultimi due anni questa tipologia di attacchi è cresciuta del 44% ed il costo associato è cresciuto del 31% nello stesso periodo. Sono sempre più diffusi e pericolosi anche gli attacchi alla supply chain, per cui un malintenzionato attacca un'azienda sfruttando vulnerabilità nella catena di approvvigionamento e nei partner e fornitori. Il rapporto ENISA Threat Landscape 2023 indica che nell'ultimo anno questa tipologia di attacchi è cresciuta del 50%, riuscendo a danneggiare più aziende con un solo attacco e creando notevoli danni economici e reputazionali. Questa tipologia di attacchi va attenzionata, anche perché nel 40% di tutti i

data breach è stato causato da attacchi alla supply chain, come certifica il report Accenture 's 2023 State of Cybersecurity Resilience Report.

Per quanto riguarda la situazione italiana, i dati del rapporto Clusit 2024 dimostrano che le aziende italiane sono purtroppo bersagliate dai criminali informatici, con una crescita degli attacchi informatici nel 2023 del 65% contro la crescita mondiale dell'11%. È peggiorata anche la severity degli attacchi, per cui l'81% degli attacchi ha una severità critica o grave, con enormi perdite economiche associate. Guardando solo ai dati del 2023, la tecnica di attacco più utilizzata è stata quella degli attacchi DDoS, che passano dal 4% del 2022 al 36% del 2023, superando i malware come primo vettore di attacco. Questo è legato alla crescita in generale dell'hacktivism, ovvero dell'utilizzo di tecniche di hackeraggio per fini politici o sociali. Al secondo posto vi sono gli attacchi basati su malware, che scendono dal 53% del 2022 al 33% del 2023, lasciando il primo posto nella classifica dei vettori di attacco al DDoS. Al terzo posto vi è la categoria di attacchi "unknown", quelli per i quali le tecniche utilizzate non sono rese note e sono in calo dal 27% al 17% proprio perché è obbligatorio segnalare la tipologia di incidenti che si sono verificati. Al quarto posto si trova il phishing, in crescita da 8% a 9%, al quinto vi sono gli attacchi che sfruttano delle vulnerabilità stabili al 2% ed infine entrano nella classifica gli attacchi basati sul web, che si attestano all'1,6% del totale. Analizzando i diversi tipi di attacchi in termini di valore assoluto, si comprende appieno la gravità degli attacchi subiti da aziende ed enti italiani. Gli attacchi DDoS hanno avuto una crescita del 1486% rispetto al 2022, mentre gli attacchi con malware, benché al secondo posto tra gli attacchi più frequenti, segnano una crescita del 4% come valore assoluto. Il valore assoluto del phishing e in generale degli attacchi di social engineering è cresciuto dell'87% e questo dimostra chiaramente la necessità di investire nella formazione del personale per evitare che diventi vittima del phishing. Sono in calo invece gli attacchi basati sul furto di identità o sul cracking di account, che in Italia si attestano solamente all'1% contro il 3% su scala mondiale. Il dato più preoccupante è proprio la crescita degli attacchi DDoS, cresciuti non solo per motivi politici, ma anche grazie alla vulnerabilità di moltissimi IoT, la cui sicurezza sarà una sfida sempre più importante in futuro. In base ai dati elaborati dal SOC di Fastweb, la famiglia più utilizzata di malware è stata ADload, ossia un adware al quale è riconducibile ben il 27% degli attacchi con malware. I dati di Fastweb evidenziano anche la gravità del fenomeno degli attacchi DDoS, alimentati anche dal mercato delle botnet, che rispetto al 2022 hanno fatto registrare una crescita del 32% degli eventi a grave impatto, mentre gli incidenti a basso impatto sono scesi del 40%. Se gli attacchi DDoS richiedono uno sforzo maggiore per essere contenuti, vi sono dei miglioramenti per quanto riguarda gli attacchi a servizi critici esposti sul web, per i quali continua il trend in calo che evidenzia la maggiore consapevolezza da parte di aziende ed enti che espongono servizi sensibili sulla rete. La diminuzione nel 2022 è stata dell'8%. Da queste analisi si può dunque comprendere come in Italia sia necessario concentrarsi sull'arginare gli attacchi DDoS, senza però dimenticare l'impatto degli attacchi basati sul malware e continuando a lavorare sulla formazione e sulla consapevolezza per proteggersi dal phishing e per consolidare politiche di aggiornamento e di patching responsabili. Anche a livello globale gli attacchi DDoS sono sempre più frequenti e gravi, anche se resta alta la minaccia soprattutto dei ransomware,

che hanno avuto un impatto minore in Italia rispetto al resto del mondo. Infine, il phishing rappresenta sempre un pericolo sia in Italia che nel mondo e serve quindi portare avanti azioni di formazione e sensibilizzazione per arginare questa tipologia di attacco.