THREAT INTELLIGENCE (1)

Elenco possibili minacce

TRACCIA:

Creare un elenco di minacce comuni che possono colpire un'azienda, ad esempio phishing, malware, attacchi DDoS, furto di dati.

- 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.

PHISHING

Negli attacchi di phishing di base, i criminali informatici inviano un'e-mail che sembra essere legale, invitando la vittima ad aprire un allegato o a fare clic su un collegamento. Questo clic potrebbe comportare il caricamento di malware sul computer della vittima o potrebbe portare la vittima a un sito Web dall'aspetto realistico. In diversi casi, l'obiettivo è quello di acquisire le credenziali dell'utente all'insaputa della vittima.

ESEMPIO DI ATTACCO DI PHISHING:

E-mail:
Un'e-mail di phishing è un'e-mail falsa che sembra essere una comunicazione cruciale ed emette un tono di urgenza e quindi riesce a indurre a scaricare un allegato o a fare clic su un collegamento.

La vittima verrà poi indirizzata a un sito Web falso. Questo sito Web potrebbe semplicemente rilasciare un virus sul tuo dispositivo o potrebbe chiederti di condividere informazioni personali ed in molti casi, il download di un allegato infetterà il computer con un virus. Prima di inviare queste e-mail fraudolente, i truffatori imparano a conoscere il più possibile le strutture aziendali, le immagini, il linguaggio, ecc. di un'impresa, per rendere l'e-mail di phishing quasi indistinguibile da quella autentica.

Alcune di queste e-mail si rivolgono specificamente ai dipendenti responsabili della gestione dei contanti e delle questioni finanziarie. Fingono di essere l'amministratore delegato o un altro superiore autorizzato a ordinare un trasferimento monetario e chiedono alla vittima di inviare fondi a un conto specifico, presumibilmente quello dell'amministratore delegato o forse dell'azienda.

COME PROTEGGERSI DALLE E-MAIL DI PHISHING

- Controllate se l'indirizzo e-mail corrisponde al dominio ufficiale.
- Fare attenzione anche ai numerosi errori grammaticali, di ortografia e di battitura, i quali rappresentano dei segnali di allarme.
- Confrontate l'URL allegato con il rispettivo dominio di un'azienda o organizzazione legittima. Se notate qualcosa di sospetto, non cliccateci sopra.
- Non inviate denaro frettolosamente. Se il vostro superiore vi chiede improvvisamente un trasferimento di questo tipo, rivolgetevi direttamente a lui.
- Utilizza software antivirus
- Utilizzare una firewall
- Usa password complesse
- Mantieni aggiornato il tuo sistema operativo
- Utilizza l'autenticazione a due fattori

MALWARE

Malware è un termine generico usato per descrivere virus, ransomware, spyware, trojan e qualsiasi altro tipo di codice o software creato con intenti dannosi.

È questo intento dannoso che caratterizza la definizione di malware: il significato di malware è il danno che può infliggere a un computer, a un sistema informatico, a un server o a una rete.

COSA PUO' FARE IL MALWARE E QUANTO E' PERICOLOSO

Gli attacchi malware possono decifrare password deboli, penetrare in profondità nei sistemi, diffondersi attraverso le reti e interrompere le operazioni quotidiane di un'organizzazione o di un'azienda. Altri tipi di malware possono bloccare file importanti, inviarti spam con annunci, rallentare il tuo computer o reindirizzarti a siti Web dannosi. Gli hacker puntano gli attacchi malware contro individui, aziende e persino governi.

A QUALE SCOPO VENGONO USATI I MALWARE?

- ***Furto di dati***: pericolosi criminali informatici possono rubare dati e utilizzarli per commettere furti di identità o venderli sul dark web ad altri criminali informatici.
- ***Spionaggio aziendale***: Il furto di dati su scala aziendale è noto come spionaggio aziendale. Le aziende possono rubare segreti ai loro concorrenti e i governi spesso prendono di mira anche le grandi aziende.
- ***Sabotaggio***: A volte, l'obiettivo è il danno. Gli aggressori possono eliminare file, cancellare record o arrestare intere organizzazioni per causare milioni di dollari di danni.

- ***Estorsione***: Il ransomware crittografa i file o il dispositivo di una vittima e richiede il pagamento della chiave di decriptazione. Lo scopo è quello di convincere la vittima – una persona, un'istituzione o un governo – a pagare il riscatto.
- ***Attacchi DDoS:*** Gli hacker possono utilizzare software dannoso per creare botnet, reti collegate di "computer zombie" sotto il controllo dell'aggressore. La botnet viene quindi utilizzata per sovraccaricare un server in un attacco DDoS (Distributed Denial of Service).

COME RILEVARE, RIMUOVERE E PREVENIRE IL MALWARE

- Non fidarti di strane e-mail, avvisi improvvisi, profili falsi e altre truffe sono i metodi più comuni per distribuire malware. Se non sai esattamente cos'è qualcosa, non cliccarci sopra.
- Ricontrolla i tuoi download. Prima di scaricare, ricontrolla sempre che il provider sia affidabile.
- Procurati un ad blocker. Contrastalo bloccando gli annunci con un ad blocker affidabile. Alcuni annunci infetti possono scaricare malware non appena vengono caricati sullo schermo, senza che sia necessario fare clic su di essi.
- Fai attenzione a dove navighi. Il malware può essere trovato ovunque, ma si trova più comunemente su siti Web con scarsa sicurezza del back-end. Se stai visitando un sito grande e affidabile, il rischio di imbatterti in malware è minimo.
- Aggiorna sempre il tuo software. Il software obsoleto può presentare vulnerabilità di sicurezza, che gli sviluppatori correggono regolarmente con gli aggiornamenti software. Installare sempre gli aggiornamenti per il sistema operativo e altri software non appena diventano disponibili.
- Proteggi i tuoi dispositivi con un'app antivirus. Anche se segui tutti i consigli di cui sopra, il tuo dispositivo potrebbe comunque essere infettato da malware. Per una protezione ottimale, combina abitudini online intelligenti con potenti software anti-malware come AVG AntiVirus Free, che rileva e blocca il malware prima che possa infettare il tuo PC, Mac o dispositivo mobile.

COME INDIVIDUARE SE SI E' STATI COMPROMESSI DA UN MALWARE

- Improvvisi cali di prestazioni: Il malware può occupare gran parte della potenza di elaborazione del dispositivo, causando gravi rallentamenti. Ecco perché rimuovere il malware è un modo per velocizzare il tuo PC.
- Arresti anomali: Alcuni malware causeranno il blocco o l'arresto anomalo del computer, mentre altri tipi causeranno arresti anomali consumando troppa RAM o aumentando le temperature della CPU. Un utilizzo elevato e prolungato della CPU può essere un segno di malware.
- File eliminati o danneggiati: Il malware spesso elimina o corrompe i file come parte del suo piano per causare il maggior caos possibile.

- Molti annunci pop-up: Il compito dell'adware è quello di inviarti spam con pop-up. Anche altri tipi di malware possono causare annunci pop-up e avvisi.
- Reindirizzamenti del browser: Se il tuo browser continua a indirizzarti a siti che non stai tentando di visitare, un attacco malware potrebbe aver apportato modifiche alle tue impostazioni DNS.
- I tuoi contatti ricevono strani messaggi da te: Alcuni malware si diffondono inviando e-mail o messaggi ai contatti delle vittime. Le app di messaggistica sicure possono aiutarti a proteggere le tue comunicazioni dalle intercettazioni.

ESEMPI DI MALWARE NELLA VITA REALE:

Alcuni degli esempi di malware più noti:

Virus di Vienna
Alla fine degli anni '1980 il virus Vienna ha corrotto i dati e distrutto i file, portando alla creazione del primo strumento antivirus al mondo.

WannaCry
Nel 2017, WannaCry è diventato rapidamente il più grande attacco ransomware della storia. Ha paralizzato governi, ospedali e università di tutto il mondo e ha causato danni per circa 4 miliardi di dollari.

Petya e NotPetya
Questi due ceppi di ransomware sono arrivati entrambi nel 2017, diffondendosi in lungo e in largo, anche nella banca nazionale ucraina. Gli attacchi malware Petya e NotPetya hanno provocato circa 10 miliardi di dollari di danni in tutto il mondo.

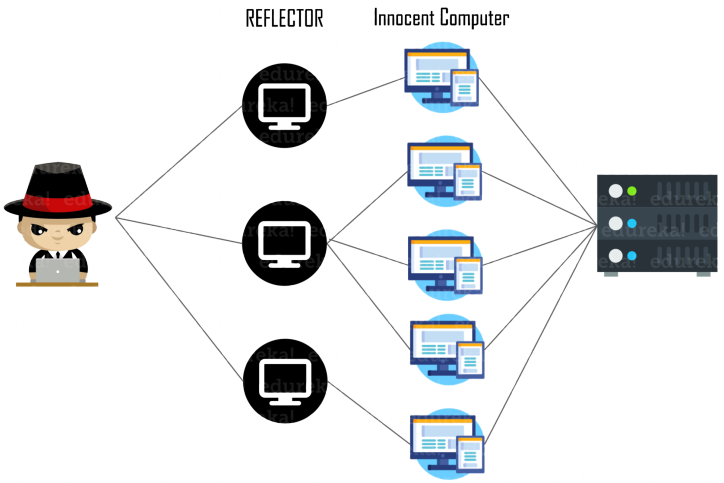
Violazione dei dati di Equifax
Gli hacker hanno messo a segno una delle violazioni dei dati più devastanti della storia quando sono riusciti a violare l'agenzia di credito statunitense Equifax nel 2017, accedendo ai dati personali sensibili di 147 milioni di persone.

Truffe di phishing relative al COVID-19
Nel 2020, molti criminali informatici hanno approfittato dei timori legati al COVID-19 in una serie di attacchi di phishing e malware. Dallo sfoofing dell'Organizzazione Mondiale della Sanità all'offerta di falsi lavori a distanza, gli hacker hanno utilizzato attacchi di phishing per distribuire malware e dirottare dati personali sensibili.

ATTACCHI DDoS

Un attacco DDoS (Distributed Denial of Service) è un tentativo dannoso di interrompere o sovraccaricare un server o un'infrastruttura di rete inondandola di traffico falso. L'obiettivo di un attacco DDoS è quello di interrompere o negare i servizi da parte di utenti legittimi, che possono essere qualsiasi cosa, compresi i siti Web che forniscono informazioni, servizi online come siti di e-commerce o servizi di back-end come l'elaborazione dei pagamenti, la comunicazione tra organizzazioni e applicazioni cloud.

Attacchi DDoS: Gli hacker possono utilizzare software dannoso per creare botnet, reti collegate di "computer zombie" sotto il controllo dell'aggressore. La botnet viene quindi utilizzata per sovraccaricare un server in un attacco DDoS (Distributed Denial of Service).



TIPOLOGIE PIU' COMUNI DI ATTACCHI DDoS:

- Attacco DDoS volumetrico:
  Gli attacchi volumetrici inondano la larghezza di banda di una macchina o di una rete con false richieste di dati su ogni porta disponibile. Ciò sovraccarica la rete, impedendole di accettare il traffico regolare. Esistono anche sottocategorie di attacchi volumetrici. Il tipo più comune di attacco volumetrico è un flood UDP (User Datagram Protocol), che viene spesso utilizzato per inviare pacchetti UDP contraffatti con indirizzi falsi, come l'indirizzo IP della vittima, ai server per le applicazioni basate su UDP, generando un flusso di traffico di risposta.

- Attacco DDoS del protocollo:
  Gli attacchi DDoS di protocollo prendono di mira i protocolli utilizzati nel trasferimento dei dati per arrestare in modo anomalo un sistema. Uno dei più comuni è un SYN flood, che attacca il processo di creazione di una connessione TCP/IP inviando un flusso di pacchetti SYN chiedendo alla vittima di sincronizzarsi invece di riconoscere una connessione, bloccando il sistema mentre attende una connessione che non avviene mai.

- Attacco DDoS dell'applicazione:
  Analogamente agli attacchi al protocollo, gli attacchi alle applicazioni prendono di mira i punti deboli di un'applicazione. Questi attacchi si concentrano principalmente sul traffico Web diretto.

QUALI SONO I POSSIBILI DANNI

***Reazione a catena*:**
Il malfunzionamento di diversi siti, possono conseguentemente mancare la disponibilità del sito per un periodo di tempo.

***Downtime del sito*:**
Un DDoS che colpisce un Web Server, rende la pagina irraggiungibile e compromette la reputazione del marchio colpito.

FURTO DI DATI

Questa forma di furto aziendale è un rischio significativo per le aziende di tutte le dimensioni e può avere origine sia all'interno che all'esterno di un'organizzazione.

Il furto doloso dei dati dei dipendenti spesso si verifica senza che le vittime ne siano mai a conoscenza, a causa della compromissione dei loro account o dispositivi personali da parte di hacker che sfruttano una cattiva gestione delle password o reti non sicure. I malintenzionati che ottengono l'accesso ai sistemi delle aziende possono nascondersi all'interno delle reti, fingendo di essere un utente legittimo per giorni, settimane o anni.

CONSEGUENZE DEL FURTO DI DATI:

Richieste di ransomware da parte degli aggressori: le organizzazioni possono avere le proprie informazioni tenute in ostaggio dai criminali informatici e pagare per recuperarle non è una soluzione garantita.

Costi di ripristino elevati: il costo del recupero dei dati può variare a seconda del sistema originariamente utilizzato per archiviare un backup e l'applicazione di patch ai sistemi dopo una violazione può far aumentare ulteriormente la fattura.

Danni reputazionali e logoramento dei clienti: i clienti esistenti possono andarsene e se ne andranno in caso di furto di dati e può essere difficile per i marchi con una storia di violazioni attirare nuovi affari.
Azioni legali da parte di clienti i cui dati sono stati esposti: nel caso in cui i dati siano stati gestiti in modo improprio, le aziende sono esposte alla possibilità di azioni legali da parte degli utenti interessati.

Tempi di inattività durante il recupero dei dati: il furto di dati può comportare l'impossibilità per le aziende di utilizzare i sistemi esistenti mentre la violazione viene corretta e una perdita di produttività dei dipendenti può colpire le organizzazioni con la stessa durezza di un furto.

Multe da parte degli organismi di regolamentazione: a seconda del settore, un'azienda può subire forti ripercussioni finanziarie per non aver rispettato i requisiti di sicurezza.
Poiché molti furti di dati si verificano a causa della semplice negligenza dei dipendenti, le aziende devono proteggersi dalla perdita e dallo sfruttamento delle informazioni.

COME AVVIENE IL FURTO DI DATI

Gli aggressori utilizzano molti metodi per rubare dati dalle organizzazioni.

Password inefficaci: gli aggressori mirano a rubare le password in gran parte perché si tratta di una tecnica semplice ed economica che raccoglie enormi ricompense.

Server senza patch: c'è sempre spazio per ulteriori miglioramenti nei processi di sicurezza e gli sviluppatori pubblicano spesso correzioni di bug esistenti nelle applicazioni server. Ma spetta agli amministratori implementare queste patch: le aziende che non controllano e non distribuiscono gli aggiornamenti dei server lasciano i loro sistemi aperti allo sfruttamento.

Informazioni disponibili pubblicamente: non è solo la tecnologia che gli hacker utilizzano per commettere furti aziendali. I social network e le informazioni pubblicamente disponibili sono sempre più importanti per aiutare i criminali informatici non solo a prendere di mira le persone, ma anche a raccogliere i dettagli di cui hanno bisogno per accedere ai sistemi aziendali ed eseguire il furto di dati dei dipendenti.

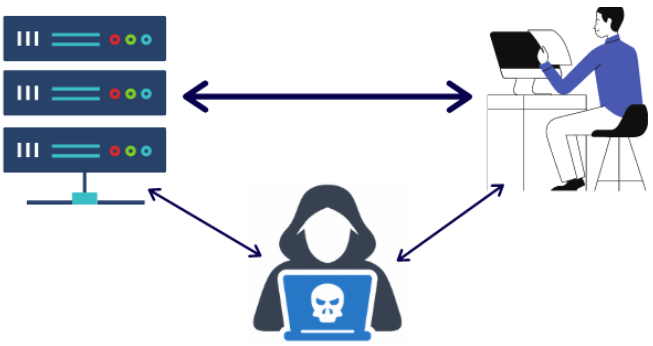
Minacce interne: gli utenti che se ne vanno sono un rischio importante per le aziende: il 69% delle organizzazioni subisce una perdita di dati quando i dipendenti lasciano la propria attività. Questi dati sono spesso altamente sensibili, come le informazioni su clienti e potenziali clienti o codice proprietario. Ma anche i dipendenti interni rappresentano una minaccia: gli utenti scontenti potrebbero essere inclini a rubare i dati aziendali per guadagno personale o finanziario.

ATTACCO MAN-IN-THE-MIDDLE

Un attacco man-in-the-middle (MitM) è un tipo di attacco informatico in cui le comunicazioni tra due parti vengono intercettate, spesso per rubare credenziali di accesso o informazioni personali, spiare le vittime, sabotare le comunicazioni o corrompere i dati.

Gli attacchi MitM sono attacchi in cui l'aggressore si trova effettivamente tra la vittima e un host legittimo a cui la vittima sta cercando di connettersi..quindi, o ascoltano passivamente la connessione o la intercettano, la terminano e impostano una nuova connessione verso la destinazione.

Sebbene gli attacchi MitM possano essere protetti con la crittografia, gli aggressori di successo reindirizzeranno il traffico verso siti di phishing progettati per sembrare legittimi o semplicemente passeranno il traffico alla destinazione prevista una volta raccolto o registrato, rendendo incredibilmente difficile il rilevamento di tali attacchi.



COME FUNZIONA MITM?

Gli attaccanti stabiliscono una connessione HTTPS tra loro e il server, ma utilizzano una connessione HTTP non protetta con la vittima, il che significa che le informazioni vengono inviate in testo normale senza crittografia. Gli attacchi Evil Twin rispecchiano i punti di accesso Wi-Fi legittimi, ma sono interamente controllati da attori malintenzionati, che ora possono monitorare, raccogliere o manipolare tutte le informazioni inviate dall'utente.

In uno scenario bancario, un utente malintenzionato potrebbe vedere che un utente sta effettuando un trasferimento e modificare il numero di conto di destinazione o l'importo inviato. Gli autori delle minacce potrebbero utilizzare attacchi man-in-the-middle per raccogliere informazioni personali o credenziali di accesso. Se gli utenti malintenzionati rilevano che le applicazioni vengono scaricate o aggiornate, è possibile inviare aggiornamenti compromessi che installano malware al posto di quelli legittimi.

COME PREVENIRE GLI ATTACCHI MITM

- ***Utilizzare la crittografia:***
  La crittografia è uno strumento cruciale per prevenire gli attacchi MITM perché codifica i dati in modo che possano essere letti solo dal destinatario previsto. Un esempio di crittografia è HTTPS, che viene utilizzato per proteggere il traffico web. HTTPS crittografa i dati inviati tra un browser Web e un server Web, impedendo agli aggressori di intercettare e leggere i dati.

- ***Prestare attenzione alle reti pubbliche:***
  Le reti Wi-Fi pubbliche, come quelle che si trovano nei bar o negli aeroporti, sono spesso non protette e possono essere facilmente intercettate dagli aggressori. Per proteggersi dagli attacchi MITM alle reti pubbliche, è importante utilizzare una rete privata virtuale (VPN) o evitare del tutto di utilizzare reti pubbliche per comunicazioni sensibili.

- ***Mantenere aggiornati software e sistemi:***
  Le vulnerabilità del software e del sistema possono essere sfruttate dagli aggressori per eseguire attacchi MITM. Per evitare che ciò accada, è importante mantenere tutti i software e i sistemi aggiornati con le patch e gli aggiornamenti di sicurezza più recenti. Ciò include browser Web, sistemi operativi e applicazioni mobili. Le organizzazioni dovrebbero anche disporre di un processo per il monitoraggio e l'aggiornamento regolare di software e sistemi per garantire che siano sempre protetti dalle minacce più recenti.

- ***Usare l'autenticazione a due fattori:***
  L'autenticazione a due fattori (2FA) aggiunge un ulteriore livello di sicurezza agli account online, richiedendo agli utenti di fornire due forme di identificazione prima di accedere ai propri account. Questo può includere qualcosa che conoscono, come una password, e qualcosa che hanno, come un'impronta digitale o un token di sicurezza. Utilizzando la 2FA, gli utenti possono assicurarsi che, anche se le loro credenziali di accesso sono compromesse, gli aggressori non possano accedere ai loro account senza la forma aggiuntiva di identificazione.