Attacchi informatici

Cosa sono?

- Azioni e manovre malevole messe in atto da:
  - ✓ Singole persone;
  - ✓ Organizzazioni criminali

COLPISCONO:

Creare un danno per colpire e violare i sistemi IT che possono essere infrastrutture, applicazioni, reti e/o dispositivi elettronici, app e servizi digitali online.

Obbiettivo di un attacco:

- Furto dei dati o delle identità digitali
- Blocco delle attività
- Malfunzionamento di un servizio
- Furto delle credenziali degli utenti
- Accesso alle informazioni

Cosa si viola?

- **Integrità**
- **Riservatezza**
- **La disponibilità dei dati**

Chi sono i veri autori?

- **Hacker;**
- **Cracker**

Chi sono gli Hacker?

- Esperti di informatica e programmazione, legati all'idea del "software libero"
- Attivisti e informatici che lavorano nell'ambito della sicurezza e che si servono delle tecniche di hacking per individuare le debolezze di un sistema e che vengono definiti:

White Hat Hacker

Chi sono gli Cracker?

- **Pirata** informatico in grado di penetrare all'interno di reti di computer senza autorizzazione
- Ha un obiettivo preciso ossia:
  - ✓ Danneggiare il sistema
  - ✓ Sottrarre dati personali
  - ✓ Sottrarre informazioni finanziarie

Quali sono i più diffusi?

- Attacco per motivi politici (per esempio l'attuale guerra in Ucraina e gli attacchi filo Russi all'Italia)

OBBIETTIVO:

- ✓ Diffondere allarmi e malcontenti;
- ✓ Protesta nei confronti di azioni portate avanti da governi
- ✓ Dirigere verso cambiamenti sociali

Attacco con scopo politico più diffuso(1/2)

Distributed Denial of Service (DDoS)

- Implica l'utilizzo di un insieme di computer/dispositivi, precedentemente dirottati per dirigere il traffico verso un singolo sito web di destinazione
- lo scopo è saturare la rete rendendo il sito non raggiungibile.

Attacco con scopo politico più diffuso (2/2)

Defacement:

- Modifica del contenuto di una pagina o di un sito web mediante l'introduzione illecita di testi critici o sarcastici.

Quali sono i diversi tipi di attacchi esistenti?:

- Malware
- Phishing
- Attacco man-in-the-middle
- Attacco DoS – Denial-of-Service
- SQL injection
- Attacchi informatici zero-day
- Tunneling DNS

Attacco Malware:

Malware è la contrazione di “malicious” e “software” ossia **programma malvagio**

- E’ in grado di danneggiare il funzionamento e la sicurezza del sistema operativo
- Si trasmette attraverso Internet, spesso tramite la posta elettronica o la semplice navigazione(virus, trojan horse, keylogger, worm e backdoor)

Come capisco che è un Malware?

- Particolarmente difficili da individuare;
- Non danneggiano gli hardware fisici di un sistema, né le apparecchiature di rete
- Sono capaci di rubare, criptare o eliminare i dati, alterare o compromettere le funzioni fondamentali di un computer e spiare le attività degli utenti, senza che questi se ne accorgano o forniscano alcuna autorizzazione al riguardo.

Attacco Phishing:

- Significa “pescare” ossia utilizzare tecniche per “pescare” dati finanziari e password di un utente.
- Si finge di essere un istituto finanziario o un ente accreditato per:
  - ingannare la vittima convincendola a fornire informazioni personali e riservate
  - Recuperare dati finanziari o codici di accesso a carte di credito

Come agisce un attacco Phishing?:

- Nel messaggio inviato all'utente, viene indicato un collegamento link che rimanda **solo apparentemente** al sito web dell'Istituto di credito o del servizio a cui si è registrati.
- Qualora l'utente inserisca i propri dati riservati, questi cadranno nelle mani dei criminali.
- Con la stessa finalità di carpire dati di accesso a servizi finanziari on-line o ad altri servizi che richiedono una registrazione, un altro pericolo arriva dall'utilizzo dei virus informatici, con le stesse modalità di infezione.

Esempio di Phishing attuale:

- Messaggio che arriva sul telefonino con scritto: ”Ciao, il tuo pacco è stato consegnato il 3/04 al punto di consegna. Vedi dove puoi ritirare il tuo pacco qui ”con un link sospetto
- Se non rispondiamo potrebbe arrivare un secondo sms con scritto:
- ‘’Secondo avviso. Il tuo pacco è stato consegnato al punto di consegna .Vedi dove puoi ritirare il tuo pacco qui” e un altro link strano

NON CLICCARE MAI SUL LINK

Attacco Man-in-the-middle:

- ”Uomo nel mezzo”;
- si verifica quando qualcuno, in segreto, ritrasmette o altera la comunicazione tra due parti che credono di comunicare direttamente tra loro, senza interferenze di terzi
- si serve di una rete Wi-Fi per intercettare le comunicazioni dell’utente, intaccando la connessione del router apparentemente senza falle o sfruttando un punto debole nel setup del router, con il fine di intercettare le sessioni degli utenti

Nuona variante di Attacco Man-in-the-middle è il Man-in-the- browser:

- il cyber criminale, riuscendo a installare un malware nei computer delle vittime, è in grado di registrare i dati scambiati tra il browser e i siti target in cui ha inserito il codice malware
- Questo tipo di attacco permette di colpire più persone allo stesso tempo e ha, inoltre, il vantaggio di poter essere realizzato in modalità remota.
- Questi attacchi bloccano la fruizione del servizio obbligando l'utente ad installare nuove versioni dell'applicazione contenenti il codice malevolo.

Esempio di attacco Man-in-the-browser (1/2)

- Nel 2015 in Russia venne scoperto nel **Facebook** locale un malware chiamato **EKO**. Questo malware è riuscito a diffondersi attraverso il sistema di messaggistica di Facebook.
- La vittima riceveva un messaggio da un suo contatto contenente un link ad un video **YouTube**. Se si fosse cliccato sul link si sarebbe atterrati su una pagina fake di YouTube, l'apertura della pagina inviava all'utente un messaggio nel quale gli si diceva di installare un'estensione per poter riprodurre il video. Ovviamente il malware era contenuto nell'estensione e dopo la sua installazione entrava in circolo sul **browser**.

Esempio di attacco Man-in-the-browser (2/2)

- Quello che succedeva dopo l'installazione dell'estensione era la ricezione da parte della vittima di numerosi messaggi o pubblicità indesiderata.
- Un aspetto sicuramente più preoccupante era la capacità di EKO di controllare le azioni dell'utente e avere accesso ai suoi dati personali (inclusi i dati bancari). Infine, l'utente infetto diventava il veicolo per la diffusione del malware.
- È molto difficile riuscire a identificare la presenza del Man-in-the-Browser a causa della sua capacità di **auto-contenersi** nel browser e non lasciare ulteriori tracce sul pc della vittima.

Come ci difendiamo da un attacco man-in-the-browser?:

- Mantenere il proprio browser sempre aggiornato e controllare periodicamente le estensioni e gli **add-on** installati.
- Adottare un browser specifico da usare solamente per operazioni sensibili e un secondo per tutte le altre attività di navigazione.

Anche per quanto riguarda le misure server-side gli accorgimenti per evitare l'infezione sono:

- Utilizzare un'autenticazione a due fattori
- Portare avanti un'analisi comportamentale, capace di identificare un comportamento anomalo del cliente

Attacco DoS – Denial-of-Service:

- ”Negazione del servizio”;
- Malfunzionamento causato da un attacco in cui vengono fatte deliberatamente esaurire le risorse di un sistema informatico che fornisce un servizio ai clienti, fino a renderlo non più in grado di funzionare
- L’aggressore provoca una “negazione del servizio”, sovraccaricando, con una miriade di richieste, le connessioni di rete di un sistema responsabile dello scambio di dati esterni: se la quantità di richieste supera il **limite di capacità**, il sistema rallenta o collassa.

Bersagli di un attacco DoS – Denial-of-Service:

- Siti di shopping online, casinò online e qualsiasi azienda e organizzazione che fornisce servizi online.
- L'autore può, infine, anche richiedere un pagamento per interrompere l'attacco.
- Esempi attuali attacco hacker filo-russi di **Killnet** nel 2023 che hanno reso inaccessibili il sito della Nato, il sito del Ministero dell'interno Italiano ecc…

Come difendersi da un attacco DoS – Denial-of-Service (1/2)

- Non si può da semplice utente;

Da amministratori di sistema:

- Deviare il traffico verso in vicolo cieco in modo da preservare la stabilità e la piena funzionalità delle risorse informatiche
- arginare il traffico in arrivo da protocolli non essenziali e da indirizzi IP non validi applicando dei filtri a livello di router e firewall (misura poco efficace);

Come difendersi da un attacco DoS – Denial-of-Service (2/2)

- L'adeguata configurazione del server e dei servizi che ospita è uno dei migliori antidoti
- **Sovrastimare** le necessità l'unica misura funzionante ossia una stima in eccesso delle risorse che saranno necessarie a un determinato sistema informatico.
- Facendo ricorso a una ampia rete di distribuzione che si estende in diversi Stati si sarà in grado di fronteggiare un attacco diretto verso uno dei server o una sezione della rete, semplicemente deviando il traffico in eccesso verso altri server "**gemelli**" posti anche a grande distanza e non sottoposti all'attacco.

Attacco SQL injection

- L'aggressore prende di mira le vulnerabilità tipiche di quei database che si avvalgono del linguaggio SQL;
- l'immissione non autorizzata di codici di richiesta o di query nei sistemi di database.
- SQL injection è una delle tecniche hacking utilizzate per l'inserimento e l'esecuzione di codice SQL non previsto all'interno di applicazioni web basate su database.
- Ciò che rende l'SQL injection particolarmente pericoloso è che non richiede l'uso di strumenti particolari, ma solo di un PC e di un qualsiasi browser tra quelli comunemente adoperati per la navigazione sul web.

Attacco SQL injection

- Un criminale esperto di sintassi SQL, infatti, può inviare particolari istruzioni attraverso le pagine del sito che prevedano un dialogo con il DB, con l'obiettivo di ottenere un accesso non autorizzato all'applicazione stessa, per recuperare informazioni, dati sensibili e modificarli o eliminarli.

Query Mysql vulnerabile

```
SELECT * FROM utenti WHERE username = '$_POST["nominativo"]' AND
password='$_POST["password"]'
```

Query Mysql contraffatta

```
SELECT * FROM utenti WHERE nome = '1' OR '1' = '1' AND password='1' OR '1' =
'1'
```

- Tale query può causare quindi la restituzione del primo o di più valori della tabella utenti, perché la clausola WHERE viene ora soddisfatta da ogni voce della tabella utenti, in quanto la parte introdotta dall'istruzione logica OR è sempre verificata.

Attacco informatici zero-day

- Minacce informatiche di ultima generazione
- È molto difficile capire da dove provengano - cyber criminale che ha scoperto determinate vulnerabilità e ha iniziato a sfruttarle (servizi browser e delle applicazioni per email).
- “zero-day” – o “zero giorni” – significa che, trattandosi di falle di sicurezza appena scoperte, “zero” è il tempo a disposizione degli sviluppatori per riuscire a sistemarle prima che si possa sfruttarle
- attacco che sfrutta tali vulnerabilità per installare software dannosi su un dispositivo.

Esempi di attacco informatici zero-day

2021: vulnerabilità zero-day di Chrome.

2020: Zoom.

2020: Apple iOS.

Attacco Tunneling DNS

- Attacco informatico datato ma ancora oggi la più concreta per le organizzazioni.
- Gli aggressori nascondono i dati all'interno delle query DNS (il **Domain Name System** è **il protocollo che mantiene in funzione la rete,** mappando i nomi di dominio e abbinandoli ai relativi indirizzi IP) e, inviandole, riescono a trasferire o ad attivare malware all'interno di un server compromesso.
- Questo genere di attacco viene utilizzato in diversi modi, ma l'approccio più comune vede protagonisti i server e una volta che un dispositivo interno è stato compromesso – ad esempio, attraverso azioni di **phishing** o con il rilascio di un malware – l'aggressore manterrà il contatto con tale dispositivo per eseguire i comandi.

Come avviene un Attacco Tunneling DNS (1/2)

- Il cyber criminale registra un dominio.
- Il server DNS indirizza a quello malevolo, dove appunto è installato il software di tunneling malware.
- Il delinquente infetta un computer con il **malware**, che penetra nel firewall dell'organizzazione. Le richieste DNS sono sempre autorizzate a entrare e uscire dal firewall, quindi il computer infetto è autorizzato a inviare query al **resolver DNS**, ovvero la prima fase della ricerca DNS.
- Quest'ultimo invia quindi le richieste di indirizzi IP ai server di dominio di primo livello.

Come avviene un Attacco Tunneling DNS (2/2)

- Il resolver DNS instrada le query al server del criminale, dove viene implementato il programma di tunneling. In questo modo viene creata una connessione tra il criminale informatico e la vittima attraverso il resolver DNS.
- L'aggressore può utilizzare questo tunnel per scopi malevoli, come l'esfiltrazione di informazioni.
- Non esiste una connessione diretta tra il criminale informatico e la vittima, quindi è difficile rintracciare il computer del cyber offender.