Le minacce alla sicurezza cibernetica: strumenti, strategie e categorie

Author : Salvatore Lombardo

Date : 17 dicembre 2018

In questo articolo, per meglio comprendere le insidie che minacciano la sicurezza cibernetica, cercherò di descrivere come avviene un attacco informatico e quali siano gli strumenti e le strategie adottate, anche se risulta difficile fornire una descrizione esaustiva a causa della continua evoluzione del fenomeno.

L’evoluzione di un attacco informatico

Un attacco informatico, in base al bersaglio scelto, può colpire le reti, i sistemi connessi oppure semplicemente le applicazioni, sfruttando spesso, ma non solo, una non adeguata protezione hardware e software.

Gli attacchi informatici possono essere distinti in attacchi passivi, qualora mirino solo all'acquisizione delle informazioni, e in quelli attivi, se mirano alla manipolazione dei dati informativi. Pertanto, una corretta politica di sicurezza dovrebbe garantire la ***protezione dagli attacchi passivi*** e la ***segnalazione immediata degli attacchi attivi***.

Sulla base di questa distinzione l’evoluzione di un attacco cibernetico può essere suddivisa in due fasi:

- La fase passiva, in cui si cerca di reperire più informazioni possibili dal target, ad esempio, tramite scansione della rete e sfruttamento delle vulnerabilità individuate.
- La fase attiva in cui si attacca l’obiettivo e si cerca un accesso al sistema con permessi amministrativi. Dopo la violazione, l’attaccante di solito procede alla cancellazione di ogni traccia che possa insospettire il gestore del servizio o il proprietario del sistema.

Modello strutturale dei codici malevoli

Nonostante ogni tipologia di codice virale usi metodiche diverse, si può ritenere che il modello strutturale di base sia grossomodo uguale per tutti. Si può con buona approssimazione

affermare che un codice malevolo segua le seguenti quattro fasi:

Il contagio: in questa prima fase, il codice virale s’installa all'interno del sistema, raggirando le eventuali protezioni. Successivamente, procede alla modifica delle impostazioni del sistema spianandosi la strada;

L’attesa: Il codice virale resta in attesa che si realizzi una determinata condizione, a seguito della quale si attiva, replicandosi oppure agendo secondo l’algoritmo di programmazione;

La reiterazione e la diffusione: al determinarsi di certi eventi o condizioni, il codice malevolo si riproduce e/o individua i bersagli verso cui propagarsi, infettando altri sistemi;

L’attacco: al verificarsi di certe condizioni, il codice virale esegue i compiti per i quali è stato programmato, come il danneggiamento o il furto dei dati del sistema, ritornando nella fase di inattività e replicandosi, fino alla possibile compromissione definitiva del sistema ospitante.

Strumenti d’attacco cibernetico

Lo strumento usato negli attacchi informatici generalmente viene definito malware. Con questo termine, che deriva dalla contrazione di due termini inglesi “malicious” e “software”, ovvero codice malevolo, si identificano una serie di entità software che in base alle caratteristiche specifiche di azione, possono essere così classificate:

- **Virus:** nel caso in cui una volta eseguito, infetti altri file in modo da riprodursi facendo copie di se stesso;
- **Worm:** nel caso in cui si autoreplichi e si diffonda senza la necessità di contagiare altri file;
- **Trojan Horse**: qualora al momento dell’esecuzione si camuffi in modo da sembrare qualcos'altro;
- **Hijacker:** qualora prenda il controllo di un browser al fine di modificarne la pagina iniziale o farlo accedere automaticamente a siti indesiderati;
- **Keylogger:** nel caso in cui registri tutte le informazioni digitate su tastiera, le memorizzi su un file e poi le trasmetta ad un server remoto;
- **Spyware:** qualora raccolga informazioni riguardanti le attività di rete dell’utente, trasmettendole ad un server remoto in ascolto;
- **Criptolocker:** qualora l’azione del codice si traduca nel criptare i dati del sistema colpito. Se a seguito di ciò si richiede un pagamento di riscatto per la decriptazione si parla di **Ransomware**;
- **Exploit:** se l’azione del codice sfrutta una vulnerabilità del sistema informatico. In tal caso tale vulnerabilità di sicurezza prende il nome di **0-day**, perché il realizzatore del sistema ha zero giorni di tempo per rimuovere l’anomalia del programma;
- **Malware Fileless:** nel caso risieda in memoria o nel registro di sistema. I malware senza file sono in genere avviati sfruttando programmi legittimi esistenti e/o integrati nel sistema operativo. Sono difficili da rilevare;
- **Malware Ibrido:** nel caso possa assumere caratteristiche diverse nelle varie fasi evolutive dell’infezione. Ad esempio Wannacry [1] ha sfruttato un exploit per il contagio,

si è diffuso come un worm, ed ha colpito come un ransomware.

Strategie di attacco cibernetico

Anche per le tattiche di attacco è difficile essere esaustivi nella descrizione delle tipologie, ma di seguito si elencano alcune delle principali tecniche note:

- **Il phishing** è una tecnica rivolta a carpire in maniera ingannevole dati sensibili, ad esempio cercando, attraverso delle comunicazioni ingannevoli, di invogliare gli utenti a visitare una pagina web, allestita ad hoc per assomigliare ad un sito ufficiale di una banca o altro istituto simile, per fornire credenziali e/o pin dispositivi. I dati così memorizzati vengono successivamente utilizzati illecitamente;
- **Il vishing** è una tecnica simile alla precedente, con la differenza che il raggiro avviene attraverso una comunicazione telefonica. Il recente tentativo di furto di credenziali relativi ai sistemi informativi comunali [2] ne è un esempio;
- **L'ingegneria sociale** è una strategia con la quale i criminali informatici raccolgono innumerevoli informazioni sulle organizzazioni, i loro dipendenti ed i privati, ad esempio, attraverso il web e i social network, oppure inviando messaggi assolutamente credibili per carpire dati utili;
- **L'IP Spoofing** è un tipo di attacco informatico che consiste nel falsificare l'indirizzo IP del computer da cui viene eseguito l'attacco;
- **Il Denial of Service** è una tecnica usata per rendere fuori uso i sistemi informativi di una organizzazione. Le tecniche di DoS mirano quindi ad interrompere il servizio sovraccaricando la rete ed i server. Nel caso di attacchi di questo tipo multipli si parla di **Distributed DoS**;
- **Il Web Defacement** è una tecnica che altera i dati di un determinato sito web per creare disinformazione e/o cambiare l'aspetto di una home page;
- **Il Backdoor** permette ad un attaccante di accedere a un computer remoto, eludendo le procedure di sicurezza per l'autenticazione;
- **Il Rootkit** è un attacco realizzato per violare i sistemi informatici e modificarne i file di sistema, mascherando opportunamente l'azione malevola;
- **L'SQL Injection** è una tecnica usata per violare applicazioni di gestione dati, con la quale viene eseguito del codice SQL per inviare il contenuto del database ad un server remoto;
- **Il Malvertising** è una tecnica di diffusione di malware attraverso la contaminazione di annunci pubblicitari legittimi di siti web stimabili.

Categorie degli attacchi cibernetici

È possibile classificare le tipologia di minacce cibernetiche in quattro categorie definite in base alle loro finalità:

- **Criminalità cibernetica:** attività criminali quali la truffa o la frode telematica, il furto d'identità, la sottrazione di informazioni e/o di proprietà intellettuali;
- **Spionaggio cibernetico:** azioni per acquisizione illecita di informazioni sensibili;

- **Terrorismo cibernetico:** azioni a scopo ideologico e volte a condizionare stati o organizzazioni internazionali;
- **Guerra cibernetica:** insieme di quelle attività e azioni militari cibernetiche organizzate per conseguire determinati effetti;
- **Hacktivismo:** attività motivate ideologicamente, con intento di solito dimostrativo, che mirano principalmente a creare un danno d'immagine e alla funzionalità temporanea di sistemi e infrastrutture di reti. A tale scopo si possono usare attacchi di tipo DDoS e Web Defacement.

Considerazioni finali

Gli attacchi informatici sono causa ogni anno di ingenti danni economici e reputazionali e di frequenti episodi di violazione privacy come dimostrano i recenti casi di data breach di cui il nostro paese è stato vittima [3][4].

È preoccupante apprendere dal Rapporto Clusit 2018 che quasi i 2/3 degli attacchi totali contro obiettivi teoricamente ben strutturati siano stati realizzati attraverso le strategie più semplici, tra quelle menzionate in questo articolo, e prodotte a basso costo (*phishing, SQL Injection, DDoS*).

Purtroppo, tutti gli indicatori ed il trend degli ultimi anni fanno ragionevolmente pensare che l'entità di questo impatto sia destinata a crescere e che non debba assolutamente essere sottovalutata.

Come rimarcato ancora una volta dagli esperti del Clusit, investire nell'Information Security e diffondere efficacemente una cultura della sicurezza informatica sono due must che non possono più essere rinviati.

Note

[1] https://www.ictsecuritymagazine.com/articoli/wcrypt-cosa-abbiamo-imparato-dallo-spauracchio-degli-ultimi-anni

[2] http://www.sogei.it/flex/cm/pages/ServeBLOB.php/L/IT/IDPagina/1848

[3] https://www.repubblica.it/tecnologia/sicurezza/2018/11/05/news/nuovo_attacco_di_anonymous_italia_diffusi_i_dati_di_ministeri_e_polizia-210845817/

[4] https://www.wired.it/internet/web/2018/11/20/italia-attacco-hacker-account-mail-pec/

Riferimenti Bibliografici

- https://iris.polito.it/retrieve/handle/11583/2517684/60956/Mezzalama_Lioy_Metwalley_A

natomia_del_malware.pdf
- https://www.uscybersecurity.net/malware/
- https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/quadro-strategico-nazionale-cyber.pdf
- https://clusit.it/
- https://www.zerounoweb.it/techtarget/searchsecurity/cybercrime/rapporto-clusit-2018-in-forte-crescita-gli-attacchi-informatici-nel-primo-semestre/
- https://www.eurosystem.it/approfondimenti/rapporto-clusit-2018/

Articolo a cura di **Salvatore Lombardo**