



OPEN INNOVATION

Cybersecurity: gli attacchi

Quali possono essere e quali i potenziali rischi



DI VINCENZO GERMANO*

I MALWARE

Considerando i flussi di dati che ogni giorno vengono trasmessi attraverso le reti da tutti i dispositivi connessi, la **Cybersecurity** è diventata una disciplina fondamentale per la loro protezione e non solo, anche per la sicurezza dei sistemi, dei dispositivi, dei servizi utilizzati per elaborarli e archiviarli, avendo come *focus* principale quello di metterli al sicuro da criminali informatici, garantendo l'integrità, la riservatezza e la disponibilità delle informazioni. Come analizzato negli approfondimenti dei mesi precedenti (*si veda Il Giornale dell'Ingegnere n. 4 e 5/2022, ndr.*) la **Cybersecurity** comprende un insieme di strumenti, approcci di gestione del rischio, tecnologie, formazione e *best practice* progettate per proteggere reti, dispositivi, programmi e dati da attacchi o accessi non autorizzati; si è visto come gli ambiti di applicazione possano essere molteplici, dalla sicurezza delle applicazioni alla sicurezza *in cloud* e delle reti, passando anche dagli aspetti di *disaster recovery* e *business continuity planning*, e in tutto ciò si è sottolineato come la sensibilizzazione dell'utente finale giochi un ruolo fondamentale in questo processo; a tal proposito si continua l'approfondimento e la sensibilizzazione riguardo quelli che possono essere alcuni degli attacchi informatici maggiormente diffusi, descrivendone a grandi linee il loro funzionamento.

A questo punto cerchiamo di comprendere meglio in che modo gli attori malintenzionati (*cyber-criminal* o *cyber-criminali*) ottengano il controllo dei sistemi informatici e riescano a condurre attacchi descrivendo alcuni metodi comuni utilizzati per minacciare la sicurezza informatica. Di sicuro uno degli attacchi maggiormente diffusi in questo ambito è legato ai **malware**, termine coniato considerando la fusione di due parole anglosassoni "*malicious*" e "*software*", ossia "software dannoso", espressione generica che descrive qualsiasi programma o codice dannoso, realizzato *ad hoc* per interrompere, danneggiare o disabilitare computer, sistemi informatici, reti, *tablet* e dispositivi mobili, spesso assumendo il controllo parziale o totale delle operazioni di un dispositivo. I motivi per i quali viene realizzato un *malware* possono essere i più disparati: dall'estorsione di denaro al sabotare la capacità di portare a termine il lavoro, o anche per dichiarazioni politiche. Per quanto un *malware* non possa danneggiare l'*hardware* fisico dei sistemi o delle apparecchiature di rete, si tenga presente che può rubare, crittografare o eliminare dati, alterare o dirottare le funzioni principali del computer e spiare la loro attività all'insaputa dell'utente finale. Con il termine "*malware*" però si identificano in maniera generica tutta una serie di tipologie di *software* dannosi riconducibili a sette principali categorie. Partendo da uno dei più innocui,

l'**adware** (*advertising software* o *software pubblicitari*) è un *software* indesiderato progettato per raccogliere dati sull'utilizzo del dispositivo sotto attacco e fornire annunci pubblicitari appropriati sullo schermo (il più delle volte all'interno di un *browser web*); in genere utilizza un metodo per camuffarsi come legittimo mediante l'installazione di un altro programma. Sebbene non sia sempre pericoloso, in alcuni casi può causare problemi al sistema, reindirizzare il *browser Internet* su altri siti non sicuri per condurre ulteriori attacchi; inoltre, livelli significativi di *adware* possono rallentare notevolmente i sistemi. Lo **spyware** è un *malware* che osserva segretamente le attività del computer dell'utente e le segnala all'autore del *software*; piuttosto che interrompere semplicemente le operazioni di un dispositivo, prende di mira informazioni sensibili, garantendo persino l'accesso remoto. Spesso è utilizzato per rubare informazioni finanziarie o personali, infatti una tipologia specifica di *spyware* è il *keylogger*, che registra le sequenze di tasti premuti sulla tastiera per rivelare *password* e informazioni personali. Il **virus** è un *software* dannoso, generalmente allegato a un documento o un *file* che tenta di diffondersi da un dispositivo all'altro, una volta scaricato, il *virus* rimane inattivo fino a quando il *file* non viene aperto ed eseguito. Vengono progettati per interrompere la capacità di funzionamento di un sistema, causano notevoli

li problemi operativi e potenziali perdite di dati.

I **worm** sono *software* dannosi che si replicano rapidamente e si diffondono su qualsiasi dispositivo all'interno della rete e, a differenza dei *virus*, non hanno bisogno di programmi a cui appoggiarsi per diffondersi, per questo si moltiplicano a una velocità esponenziale. I *worm* (come i *virus*) possono interrompere gravemente le operazioni di un dispositivo, causando la perdita di dati.

I **trojan**, come il suo omonimo "il cavallo di Troia" (del poema epico *l'Odissea*), nell'informatica sono definiti come un tipo di *malware* (e non un *virus*) che sfrutta l'inganno e l'ingegneria sociale per indurre utenti ignari a eseguire programmi per computer apparentemente benigni che nascondono secondi fini dannosi, perciò sono mascherati da utili programmi *software*, ma una volta che l'utente lo avvia, il *trojan* ha accesso al sistema; tuttavia, a differenza dei normali *virus* e *worm*, non sono progettati per replicarsi automaticamente.

La penultima categoria di *malware* riguarda i **ransomware** (*ransom malware* - *malware a riscatto*), ovvero una tipologia di *malware* che impedisce agli utenti di accedere al proprio sistema o ai *file* personali e richiede il pagamento di un riscatto per riottenere l'accesso. Il *ransomware* ha fatto notizia negli ultimi anni perché sono state attaccate aziende, privati, organizzazioni ma anche agenzie governative, che si sono trovati i *file* cifrati e in "ostaggio" fintanto che non è avvenuta una tran-

sazione economica di "riscatto". Le prime varianti di *ransomware* furono sviluppate alla fine degli anni '80, con una richiesta di pagamento da inviare tramite posta ordinaria, oggi gli autori di *ransomware* ordinano che il pagamento venga inviato tramite criptovaluta o affini. Infine, l'ultima categoria di *malware* diffusasi ultimamente è la **fileless malware** (*malware* in assenza di *file*): come suggerisce il termine, è una tipologia di *malware* residente nella memoria dei dispositivi della vittima e non su *file* sul disco rigido; poiché non ci sono *file* da scansionare, è più difficile da rilevare rispetto al *malware* tradizionale. Inoltre, rende più difficile l'analisi forense perché il *malware* scompare quando il computer della vittima viene spento o riavviato.

ALTRI TIPI DI MINACCE DI CYBERSECURITY

Purtroppo, per gli utenti finali, con i *malware* non si esaurisce la lista, molto più estesa, di attacchi informatici possibili, infatti tra le macro categorie ve ne sono altre, per citarne alcune, gli attacchi di tipo *phishing*, ovvero quando i criminali informatici prendono di mira le vittime con *e-mail* che sembrano provenire da un'azienda legittima che richiede informazioni sensibili; spesso vengono utilizzati per indurre le persone a cedere i dati delle carte di credito e altre informazioni personali o per installare *malware* sui dispositivi utente.

Un'altra tipologia di attacco è il *man-in-the-middle*, un tipo di minaccia informatica in cui un criminale informatico intercetta la comunicazione digitale tra due individui per rubarne dati; un esempio può essere quello di una rete *wi-fi* non protetta in cui un utente malintenzionato potrebbe intercettare i dati trasmessi dal dispositivo della vittima e dalla rete. Oppure *denial of service* ("negazione del servizio") o *DoS*, un attacco informatico che inonda una rete o un computer/server con un'enorme quantità di "richieste", sovraccaricando efficacemente il sistema e rendendolo incapace di rispondere alle richieste degli altri utenti.

CONCLUSIONI

Quanto appena illustrato non vuol essere una guida onnicomprensiva, ma semplicemente una carrellata di tipologie di attacchi per comprendere come essi possono nascondersi potenzialmente dietro ogni *link*, *file*, allegato delle *mail*, programma o applicazione, e come essi possono operare in modo tale da aumentando la consapevolezza dell'utente sulle minacce informatiche, preziosa in tutti gli ambiti della sicurezza.

* INGEGNERE ELETTRONICO E COMPONENTE COMMISSIONI INNOVAZIONE E INGEGNERIA FORENSE ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI TORINO