PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 27 - numero 5886 di Martedì 08 luglio 2025

Attacchi ransomware in aumento: come proteggersi dai cybercriminali?

Il numero di attacchi ransomware cresce esponenzialmente: scopri le principali tecniche usate dagli hacker e impara a difenderti contro i rischi cyber.

Negli ultimi anni, **le minacce informatiche sono aumentate in modo esponenziale**, colpendo aziende, enti pubblici e privati. Gli hacker utilizzano tecniche sempre più sofisticate per infiltrarsi nei sistemi informatici, rubare dati sensibili e causare danni economici. Tra i principali pericoli ci sono malware, trojan, spyware e, soprattutto, i ransomware. Le organizzazioni criminali operano a livello globale sfruttando falle nei software, debolezze umane e tecnologie avanzate per compromettere interi sistemi.

Le conseguenze di un attacco cyber possono essere devastanti: furto di dati, paralisi delle attività aziendali, danni alla reputazione e, nei casi più gravi, richieste di riscatto per il ripristino dei sistemi. Le vittime si trovano spesso a dover scegliere tra pagare ingenti somme di denaro o subire la perdita irreversibile dei propri file. **La prevenzione e la consapevolezza sui pericoli informatici** sono dunque fondamentali per proteggere l'azienda e sé stessi.

I ransomware: cosa sono?

Tra tutte le minacce informatiche, il **ransomware** è una delle più insidiose e dannose. Questo tipo di malware **blocca l'accesso ai dati di un sistema infetto e richiede un pagamento per sbloccarli**.

Il ransomware può prendere di mira sia grandi aziende sia piccoli imprenditori e utenti privati e ha conosciuto un'evoluzione preoccupante negli ultimi anni. Le organizzazioni criminali si sono specializzate nella creazione di malware sempre più sofisticati, capaci di eludere gli antivirus e propagarsi rapidamente all'interno delle reti aziendali. Alcuni attacchi mirano a cifrare i file e impedire alle vittime di accedervi, mentre altri puntano al furto e alla diffusione di dati sensibili, minacciando di renderli pubblici se il riscatto non viene pagato.

Un aspetto inquietante è che, anche in caso di pagamento, non vi è alcuna garanzia che i dati vengano restituiti. Molte aziende hanno subito attacchi che hanno compromesso irreparabilmente i loro archivi digitali, nonostante abbiano seguito le richieste degli hacker. Per questo motivo, **la miglior strategia contro il ransomware è la prevenzione**.

Di seguito, analizziamo le principali modalità con cui il ransomware viene diffuso, illustrando esempi concreti per comprendere la portata della minaccia.

1. Phishing (e-mail malevole)

Una delle tecniche più comuni per diffondere il ransomware è il **phishing**, ovvero l'invio di **e-mail fraudolente** che contengono link dannosi o allegati infetti. Queste sembrano apparentemente provenire da fonti affidabili, come banche, aziende o colleghi, e spesso includono un messaggio urgente per spingere la vittima ad aprire immediatamente l'allegato.

- **Esempio:** un impiegato riceve un'e-mail che sembra arrivare dall'ufficio risorse umane della sua azienda, con un file Excel allegato chiamato "Aggiornamento stipendi 2024". Il documento richiede di abilitare le macro per visualizzare i dati. Appena l'utente attiva le macro, un ransomware si installa e inizia a cifrare tutti i documenti dell'azienda, bloccando l'accesso ai file e paralizzando l'attività lavorativa.

2. Exploit di vulnerabilità software

Gli hacker sfruttano **falle nei software non aggiornati** per infiltrarsi nei dispositivi e installare ransomware. Sistemi operativi, server e applicazioni obsolete rappresentano una porta d'accesso ideale per i criminali, che possono iniettare codice malevolo senza che l'utente se ne accorga.

- **Esempio:** **L'attacco WannaCry del 2017** ha colpito migliaia di aziende nel mondo sfruttando una vulnerabilità in Windows che Microsoft aveva già corretto con un aggiornamento. Tuttavia, molte aziende non avevano installato la patch di sicurezza in tempo e sono state infettate, subendo danni multimilionari e interruzioni prolungate.

3. Drive-by download

Questa tecnica prevede l'infezione automatica del dispositivo quando un utente visita un **sito compromesso**. Non è necessario alcun clic: basta accedere alla pagina per scaricare il ransomware.

- **Esempio:** un dipendente cerca immagini gratuite su internet e accede a un sito di wallpaper che è stato compromesso dagli hacker. Senza accorgersene, il suo browser scarica ed esegue un malware che crittografa i file aziendali.

4. Accesso remoto compromesso (RDP)

L'uso di **password deboli** o rubate consente agli hacker di entrare nei sistemi aziendali tramite il protocollo Remote Desktop (RDP) e installare il ransomware manualmente.

- **Esempio:** un'azienda utilizza RDP per consentire ai dipendenti di lavorare da remoto. Un criminale trova le credenziali di accesso su un forum hacker e accede alla rete interna, lanciando un ransomware che blocca tutti i server.

Leggi anche: **Cybersecurity: come impostare una password sicura**

5. Malvertising (pubblicità malevola)

Gli hacker iniettano codice dannoso in **annunci pubblicitari** su siti web legittimi. Quando un utente visualizza o interagisce con la pubblicità, il ransomware viene scaricato.

- **Esempio:** un utente visita un noto sito di notizie e vede un annuncio per un concorso. Cliccandoci sopra, il suo browser viene reindirizzato a un sito malevolo che scarica un ransomware in background.

6. USB e dispositivi rimovibili

I criminali possono diffondere ransomware anche attraverso **dispositivi USB infetti**, lasciati intenzionalmente in luoghi pubblici per indurre le vittime a raccoglierli e collegarli ai propri computer. Una volta collegato, il malware si installa automaticamente e compromette i file.

- **Esempio:** un impiegato trova una chiavetta USB abbandonata nel parcheggio aziendale. La collega al suo PC per curiosità e il ransomware contenuto al suo interno si attiva, crittografando tutti i file aziendali e propagandosi alla rete interna.

7. Catene di fornitura (supply chain attacks)

Gli attaccanti compromettono software o servizi legittimi, infettando gli utenti finali tramite **aggiornamenti software manomessi** o servizi cloud violati.

- **Esempio: l'attacco al software di Kaseya** da parte del gruppo cybercrime REvil nel 2021 ha sfruttato una vulnerabilità per distribuire ransomware a centinaia di aziende tramite un aggiornamento software infetto.

8. Infezioni a catena (worm-like behavior)

Alcuni ransomware sono progettati per **diffondersi automaticamente tra i dispositivi di una rete** senza bisogno di intervento umano, sfruttando vulnerabilità di sistema o credenziali compromesse.

- **Esempio:** il ransomware **NotPetya** nel 2017 ha infettato intere aziende propagandosi automaticamente da un dispositivo all'altro, sfruttando exploit non corretti tempestivamente.

9. Attacchi fileless

Questi attacchi utilizzano strumenti legittimi del sistema operativo, come PowerShell o WMI, per eseguire il ransomware direttamente in memoria, **evitando di lasciare tracce evidenti sul disco** e rendendo più difficile il rilevamento.

- **Esempio:** un hacker sfrutta una vulnerabilità in PowerShell per lanciare un ransomware senza salvare alcun file sul disco, eludendo i tradizionali sistemi antivirus.

10. Social engineering avanzato

I criminali informatici utilizzano tecniche di **ingegneria sociale** per ingannare le vittime, convincendole a scaricare file dannosi o a fornire credenziali di accesso.

- **Esempio:** un dirigente riceve un'email che sembra provenire dal suo amministratore IT, chiedendo di scaricare un aggiornamento di sicurezza. In realtà, il file contiene un ransomware che blocca l'intero sistema aziendale.

11. Attacchi a sistemi backup

Per impedire alle vittime di ripristinare i propri dati, gli attaccanti cercano di **eliminare o corrompere i backup** prima di attivare il ransomware.

- **Esempio:** gli hacker accedono ai server di backup aziendali, cancellano i salvataggi recenti e poi rilasciano il ransomware, lasciando l'azienda senza possibilità di ripristino.

I ransomware rappresentano una minaccia concreta e in continua evoluzione. Proteggersi significa non solo adottare soluzioni di sicurezza avanzate, ma anche **formarsi** per riconoscere i segnali di un possibile attacco.

Alice Gugliotta

Fonte: eLearningNews