aderente a Confartigianato Imprese

Milano, 27 gennaio 2025
Prot.: LEG/71/rp/2025

La parola all'esperto

Strategie di difesa e risposta agli attacchi ransomware

Il Servizio Operazioni e gestione delle crisi cyber di ACN (l'Agenzia per la Agenzia per la cybersicurezza nazionale) ha recentemente pubblicato un rapporto sullo stato dell'arte della minaccia ransomware in Italia e nel mondo.

Quello che emerge è che, negli ultimi anni, il ransomware si è affermato come una delle minacce prevalenti a livello nazionale. **L'Italia si colloca** tendenzialmente **al quarto posto** fra le nazioni europee maggiormente colpite **(con il 12% dei casi in Europa).**

Le vittime appartengono prevalentemente al settore privato, **con le piccole imprese che risultano essere la tipologia di target principale degli attaccanti**. Analizzando la loro distribuzione in base ai settori di attività economica di appartenenza, **il manifatturiero emerge come il settore maggiormente colpito**. Da un punto di vista geografico, le zone più interessate dal fenomeno risultano essere i grandi **distretti industriali del Nord Italia.**

Al riguardo, il Servizio Legale segnala **l'approfondimento dell'Avv. Gian Paolo Valcavi**, partner di freebly società benefit tra avvocati s.r.l., il quale, dopo averci aiutato a meglio comprendere le tecniche di attacco del ransomware, ci ricorda che **ogni PMI ha uno strumento a sua disposizione per affrontare le sfide portate dalle crescenti abilità dei criminali informatici: il proprio sistema privacy**.

Il Servizio Legale resta a disposizione ai consueti recapiti.

Il ransomware è una tipologia di minaccia che ha lo scopo di cifrare i dati del bene informatico per richiedere alla vittima un riscatto per riottenere l'accesso ai propri dati

L'impatto degli attacchi sulle vittime di ransomware può essere di tipo economico, operativo, reputazionale, con esposizione anche a rischi di natura legale

CONTATTI
Servizio Legale Appalti
tel. 02.671401
mail: legale@apmi.it

Gli **attacchi ransomware** costituiscono una **minaccia sempre più complessa e pervasiva**, sviluppandosi secondo schemi ben organizzati e sfruttando la vulnerabilità, sia tecnologica, che umana.

Il documento dell'**Agenzia per la Cybersicurezza Nazionale (ACN)** ci guida nell'analisi delle principali tecniche di attacco e nell'individuazione di misure mirate per supportare le nostre organizzazioni nella mitigazione di tali rischi.

Tecniche di Attacco

Gli attacchi ransomware seguono un processo articolato in più fasi, comunemente definito ***"killchain"***. Ogni step è ottimizzato per aumentare l'efficacia complessiva ed assicurare il successo delle azioni degli aggressori.

Vediamo lo schema normalmente seguito:

I) Compromissione Iniziale (Initial Access)

La compromissione iniziale è ottenuta tramite svariati vettori a seconda delle vulnerabilità del target, tra i quali:

- **Phishing**: e-mail ingannevoli dalle apparenze convincenti per sottrarre credenziali o installare malware;
- **Sfruttamento di vulnerabilità**: attacco a falle di sicurezza conosciute o nuove (0-day), prima che vengano applicate eventuali patch;
- **Credenziali sottratte**: utilizzo di password rubate o accessi deboli per entrare nei sistemi critici;
- **Uso dell'intelligenza artificiale (AI)**: l'impiego dell'AI nell'ambito del phishing produce campagne sempre più realistiche e difficilmente individuabili, come accade con i deep-fake, cioè messaggi video, chiamate telefoniche o videochiamate, che riproducono perfettamente la voce, le movenze e le sembianze della persona che ci chiede di effettuare operazioni anomale (es: pagamenti, comunicazioni di password, …), la cui efficacia è spesso basata sulla credibilità del messaggio (es: il video riproduce la mia immagine mentre parla) e sulla fretta che crea pressione nella vittima dell'azione malevola.

II) Elevazione dei Privilegi (Privilege Escalation)

Dopo il primo accesso, gli attaccanti mirano ad ampliare il controllo utilizzando le seguenti modalità:

- **Persistenza**, cioè la creazione di backdoor e meccanismi per mantenere l'accesso nonostante riavvii od operazioni correttive iniziali;
- **Movimenti laterali** e, quindi, l'espansione orizzontale nella rete per colpire dispositivi aggiuntivi;
- **Tecniche "*Living-off-the-land*"**, tramite l'utilizzo di strumenti già esistenti all'interno dell'infrastruttura della vittima (come software di accesso remoto) per eludere il rilevamento.

Prosegue →

- ***Tool* specializzati**, come Cobalt Strike (software progettato per il red teaming e i test di penetrazione, nato per gestire la sicurezza informatica e diventato, suo malgrado, uno degli strumenti più utilizzati dai criminali informatici per simulare comportamenti legittimi e neutralizzare i sistemi di sicurezza).

III) Esfiltrazione e blocco dei dati (Data Exfiltration & Encryption)

Nella fase critica finale, gli aggressori sfruttano queste modalità (in modo congiunto o separato):

- **Esfiltrazione**, cioè copia e spostamento dei dati della vittima verso server controllati dagli attaccanti, servendosi di software come Rclone o MEGASync;
- **Crittografia**, ovvero l'Impiego di avanzati algoritmi per bloccare completamente i dati e renderli inaccessibili;
- **Estorsioni "senza crittografia"**, tendenza emergente che prevede la minaccia di pubblicare informazioni sottratte senza procedere alla crittografia dei dati sottratti, così da agire sul lato reputazionale della vittima.

Le prime cose da fare

La protezione efficace dai ransomware richiede l'implementazione congiunta di linee guida strategiche tecniche e organizzative identificate su tre pilastri cruciali, che vedono il modello privacy quale filo conduttore di tutte le varie azioni di protezione.

I) Processi organizzativi

- **Piano per la gestione degli incidenti**, cioè, controllare ed eventualmente rivedere le politiche di gestione dei *data breach* che dovrebbero far parte del modello privacy adottato, così da avere procedure operative per reagire rapidamente;
- **Backup e ripristino**, che vede l'esecuzione periodica di backup sicuri, testati regolarmente per garantire un recupero efficace in tempi rapidi, fatti non solo online (quindi più facilmente aggredibili), ma anche off-line e in modo asincrono (non è la prima volta che si rivalutano vecchie abitudini);
- **Politiche aziendali di sicurezza**, tramite l'adozione di standard e best practice per limitare i punti deboli esistenti;
- **Formazione del personale**, punto fondamentale e centrale perché l'attacco richiede sempre la collaborazione (involontaria e spesso inconsapevole) di una persona interna all'organizzazione e, quindi, un percorso di costante aggiornamento e consapevolezza per tutto il personale facilita la cultura del sospetto e, quindi, della protezione dai principali vettori d'attacco, in particolare il phishing.

II) Tecnologie a supporto

- **Sistemi di monitoraggio** tramite la configurazione di sistemi di logging e rilevamento in tempo reale per identificare attività sospette;

Prosegue →

- **Backup offline**, cioè, come si scriveva, la conservazione sicura delle copie di backup in repository isolati e non collegato in rete, così da essere isolati da quanto accade sulla rete aziendale.
- **Threat intelligence** e, quindi, integrazione di feed informativi aggiornati sulle minacce per anticipare schemi noti d'attacco;
- **Difese perimetrali**, tramite sistemi di filtraggio avanzati destinati a prevenire intrusioni dall'esterno della rete.

Alcuni suggerimenti: aggiorna sempre il tuo sistema privacy

Per cercare di gestire l'ansia che il messaggio potrebbe aver creato, basta pensare che **hai uno strumento a tua disposizione per affrontare le sfide che le crescenti abilità dei criminali informatici ti impongono: il tuo sistema privacy.**

Questo è il punto di partenza: **il modello privacy adottato deve essere il punto di riferimento** per l'analisi su come proteggere i dati riservati aziendali e la tua reputazione dagli attacchi hacker.

Si tratta di **continuare con quell'attività di miglioramento continuo** del modello privacy adottato: insomma, la parola d'ordine è **non stare mai fermi**, perché gli attacchi informatici sono sempre più sofisticati e realizzati con strategie sempre nuove. **Grazie alla tua proattività tu saprai prevenirli e, nel caso più sfortunato, gestirli**.

Informando e formando costantemente le persone che collaborano con te avrai fatto una buona parte del lavoro.

Avv. Gian Paolo Valcavi