

# Supply Chain Attack: minaccia invisibile alla sicurezza informatica



## Cos'è un Supply Chain Attack?

Un supply chain attack è un attacco informatico che sfrutta la debolezza o la compromissione di uno o più fornitori all'interno della catena di approvvigionamento di un'azienda. Questi fornitori possono essere partner commerciali, produttori di software o hardware, terze parti che gestiscono servizi critici o qualsiasi altro ente coinvolto nel processo di fornitura dei prodotti o dei servizi di un'azienda.

La caratteristica distintiva di questo tipo di attacco è la sua capacità di colpire molteplici obiettivi attraverso un singolo punto di ingresso. Gli attaccanti possono sfruttare la fiducia tra l'azienda bersaglio e i suoi fornitori per introdursi e danneggiare i sistemi, rubare dati sensibili, compromettere la privacy dei clienti, interrompere la produzione industriale.

## Come individuare un Supply Chain Attack?

Rilevare gli attacchi alla supply chain è un compito complesso che richiede un'approfondita analisi e una vigilanza costante da parte degli esperti di sicurezza informatica. Ecco alcune metodologie e strumenti che possono essere utilizzati per identificare questa minaccia:

- **Monitoraggio degli Accessi:** tracciare e monitorare gli accessi ai sistemi e alle reti aziendali è fondamentale per individuare eventuali attività sospette o inconsuete.

- **Anomalie nei Dati di Fornitori:** analizzare i dati provenienti dai fornitori per individuare eventuali variazioni o anomalie nei pattern di comportamento, nei tempi di consegna o nelle prestazioni.
- **Verifica della Firma Digitale:** verificare l'autenticità delle firme digitali dei software e dei firmware utilizzati all'interno della catena di fornitura, in modo da rilevare eventuali modifiche non autorizzate.
- **Auditing dei Fornitori:** condurre regolari audit di sicurezza sui fornitori, verificando le loro misure di protezione dei dati e delle informazioni sensibili.
- **Indagini Forensi:** in caso di sospetta supply chain attack, condurre indagini forensi approfondite per identificare la causa e mitigare il danno.

## Risposta ai Supply Chain Attack

I supply chain attack possono causare danni significativi alle organizzazioni coinvolte. Pertanto, è essenziale avere un piano di risposta dettagliato in caso di cyber attacco. Alcuni passi chiave da seguire includono:

- **Isolamento e Mitigazione:** isolare immediatamente il punto compromesso e prendere misure per limitare la diffusione dell'attacco.
- **Allerta e Comunicazione:** informare tempestivamente tutte le parti coinvolte, inclusi i fornitori e i clienti, sull'incidente e fornire istruzioni dettagliate su come proteggersi.
- **Indagine Forense:** condurre un'indagine forense approfondita per comprendere l'entità dell'attacco e identificare eventuali altre vulnerabilità nel sistema.
- **Miglioramenti della Sicurezza:** implementare le pratiche di sicurezza, come autenticazione multi-fattore, crittografia dei dati e controlli di accesso più rigorosi, per ridurre il rischio di futuri attacchi.
- **Pianificazione della Continuità Operativa:** avere un

piano di continuità operativa per garantire la continuità dei servizi critici anche in caso di attacco.

## Come Proteggersi dai Supply Chain Attack?

La prevenzione è il primo passo per proteggersi da questa tipologia di cyber attacchi. Si possono adottare diverse misure preventive per mitigare i rischi:

- **Due Diligence sui Fornitori:** eseguire una rigorosa due diligence sui fornitori prima di stabilire partnership o accordi contrattuali.
- **Test e Valutazione dei Software:** valutare regolarmente i software e i firmware utilizzati dai fornitori, garantendo che siano privi di vulnerabilità note.
- **Controlli di Sicurezza:** richiedere ai fornitori di implementare rigorosi controlli di sicurezza, tra cui autenticazione robusta, crittografia e logging dettagliato.
- **Monitoraggio Costante:** mantenere una costante vigilanza sulle attività dei fornitori e dei sistemi interni per rilevare tempestivamente eventuali attività sospette.
- **Formazione del Personale:** sensibilizzare il personale aziendale riguardo le minacce di supply chain attack e fornire una adeguata formazione.

## Recenti Attacchi alla Supply Chain

- **SolarWinds** (Dicembre 2020): Uno degli attacchi alla supply chain più significativi della storia. Gli attaccanti hanno infiltrato il sistema di aggiornamento software di SolarWinds, un'azienda specializzata in strumenti di monitoraggio e gestione delle reti. I file di aggiornamento compromessi sono stati distribuiti a migliaia di clienti, inclusi numerose agenzie governative e aziende di livello enterprise. Il malware introdotto ha consentito agli aggressori di ottenere l'accesso ai sistemi delle vittime e compromettere la

sicurezza dei dati.

- **Kaseya VSA** (Luglio 2021): Un attacco ransomware ha sfruttato una vulnerabilità zero-day nel software di gestione remota Kaseya VSA per colpire centinaia di aziende di tutto il mondo. Gli aggressori hanno utilizzato Kaseya VSA per diffondere il ransomware REvil, richiedendo ingenti somme di denaro per il rilascio dei dati rubati.
- **Codecov** (Aprile 2021): Codecov, una popolare piattaforma di testing del codice, è stata compromessa da un attacco supply chain. Gli aggressori hanno alterato lo script di Codecov utilizzato dai clienti per il testing dei loro codici, consentendo loro di raccogliere credenziali e altre informazioni sensibili da numerosi repository di codici.
- **Microsoft Exchange Server** (Gennaio 2021): Una serie di vulnerabilità zero-day nelle versioni locali di Microsoft Exchange Server ha permesso a un gruppo di hacker sponsorizzato dallo stato cinese di compromettere migliaia di server Exchange in tutto il mondo. Gli attaccanti hanno sfruttato queste vulnerabilità per rubare dati e installare malware.
- **SITA** (Marzo 2021): SITA, una società di servizi IT per il settore dell'aviazione, è stata vittima di un attacco supply chain che ha coinvolto numerosi partner e fornitori del settore aeronautico. L'attacco ha colpito diverse compagnie aeree, compromettendo dati e informazioni sensibili dei passeggeri.
- **Pulse Secure** (Maggio 2022): Un attacco ransomware ha colpito i dispositivi VPN della società Pulse Secure, sfruttando una vulnerabilità nota come CVE-2021-22893. Gli aggressori hanno sfruttato questa falla per accedere ai sistemi delle organizzazioni che utilizzavano i dispositivi VPN di Pulse Secure, compromettendo la sicurezza dei dati aziendali.
- **Microsoft Office 365** (Luglio 2022): Un gruppo di hacker ha sfruttato una vulnerabilità zero-day nel sistema di

autenticazione di Microsoft Office 365 per compromettere gli account di diversi utenti. L'attacco ha colpito sia utenti individuali che aziende, causando la perdita di dati sensibili e la diffusione di messaggi di phishing.

- **Toyota** (Marzo 2022): un ransomware colpisce il settore del manufacturing, vittima del cyber attacco un importante fornitore, la Kojima Industries, che ha rischiato di infettare direttamente i sistemi IT e OT della casa produttrice di automobili, insieme a tutte le altre aziende collaboratrici.
- **Tenda** (Ottobre 2022): Tenda, un produttore di dispositivi di rete, è stato vittima di un attacco supply chain che ha riguardato il firmware dei suoi router. Gli aggressori hanno introdotto una backdoor nei dispositivi, consentendo loro di accedere ai dati di navigazione degli utenti e di compromettere la sicurezza delle reti.
- **3CXDesktopApp**: nel 2023, un attacco informatico alla catena di fornitura ha messo nel mirino il software 3CX e i suoi clienti. L'applicazione 3CXDesktopApp, utilizzata per videochiamate e conferenze vocali, è stata infettata da un trojan, creando così le premesse per attacchi multi-fase ai danni degli utenti dell'app compromessa. Questo episodio è stato segnalato dall'agenzia per la sicurezza delle infrastrutture e cybersecurity (CISA) il 30 marzo 2023.

Questi attacchi alla supply chain sono solo alcuni esempi delle minacce sempre più sofisticate che le organizzazioni devono affrontare nella cyber sicurezza. La lezione da trarre da questi incidenti è l'importanza di adottare una strategia di sicurezza olistica e costantemente aggiornata per proteggere i sistemi e i dati aziendali da queste minacce sempre in evoluzione.

## Conclusioni

Le supply chain attack rappresentano una delle principali minacce per la sicurezza informatica delle organizzazioni. Gli esperti di cyber sicurezza e cyber crime devono essere consapevoli di questa minaccia invisibile e adottare misure preventive e di risposta adeguate. La costante vigilanza e il monitoraggio dei fornitori, insieme a una solida strategia di sicurezza informatica, sono fondamentali per proteggere le aziende da queste sofisticate minacce.

A cura della Redazione

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/articoli/supply-chain-attack-minaccia-invisibile-alla-sicurezza-informatica/>