proofpoint.

Attacchi alla supply chain

In breve

DESCRIZIONE

Gli attacchi alla supply chain rientrano in due categorie principali: frodi via email e software di terze parti. In questi attacchi, i criminali informatici compromettono gli account email dei fornitori o dei fornitori di servizi al fine di attaccare i loro clienti e partner. La violazione iniziale del fornitore spesso avviene tramite un attacco di phishing o di un malware. Una volta entrato nel sistema del fornitore, il criminale informatico può falsificare gli account email per lanciare un attacco di phishing, una frode delle fatture o altri tipi di attacco contro i clienti. Dopo essere riuscito a violare i sistemi dei clienti, il criminale informatico può sottrarre dati riservati, installare ransomware o utilizzare l'accesso per lanciare un'ulteriore serie di attacchi di phishing o di frodi via email.

STRUMENTI UTILIZZATI

Gli attacchi contro la supply chain utilizzano tipicamente attacchi di phishing per rubare le credenziali d'accesso (takeover degli account), malware (Stuxnet, NotPetya, Sunburst, Kwampirs) e minacce fraudolente come la violazione dell'email aziendale (BEC, Business Email Compromise).

TIPI

- **Violazione dell'email aziendale (BEC o frode via email).** Il criminale informatico si finge una persona di cui il destinatario si fida, tipicamente un partner commerciale, fornitore o rivenditore. Al destinatario viene richiesto di effettuare un bonifico bancario, di pagare una fattura falsa o alterata, di dirottare i pagamenti degli stipendi o di modificare le coordinate bancarie per i pagamenti futuri. In alcune campagne di frodi via email, il criminale informatico può compromettere l'account email reale del fornitore per violare la sua identità e persino sfruttare le conversazioni email esistenti.
- **Attacchi software alla supply chain.** Il criminale informatico ottiene l'accesso ai sistemi di un fornitore di servizi gestiti o di software e infetta le nuove build che vengono poi distribuite a clienti e partner. Tali attacchi sono più rari rispetto a quelli sopra elencati, ma possono colpire più vittime tramite un'unica violazione.

FATTORI DI RISCHIO

- Coinvolgimento di fornitori di servizi professionali o di consulenza
- Utilizzo di una soluzione di cybersecurity inadeguata
- Autorizzazione all'accesso a dipendenti negligenti o che non hanno ricevuto un'adeguata formazione di sensibilizzazione alla sicurezza
- Complessità della supply chain: le aziende si affidano sempre più a diversi servizi SaaS e piattaforme cloud

Gli attacchi alla supply chain sui media

Nel 2013, Target ha pagato 18,5 milioni di dollari a seguito di una violazione di dati che ha interessato 41 milioni di clienti

In seguito al furto di credenziali di accesso di un account di uno dei fornitori di Target, i criminali informatici hanno violato i sistemi del colosso della grande distribuzione e rubato le informazioni finanziarie sensibili di oltre 41 milioni di clienti.

Gli hacker attaccano la supply chain dei vaccini contro il COVID-19

Un attacco di phishing ha colpito i dirigenti di 44 aziende in diversi continenti nel tentativo di compromettere la supply chain globale dei vaccini contro il COVID-19.

Associazione no profit per l'edilizia popolare subisce una perdita di 1,2 milioni di dollari a causa di una truffa BEC

I criminali informatici hanno contraffatto il dominio di un fornitore per rubare quasi 1 milione di sterline da una cooperativa per l'edilizia popolare vicino a Londra.

Anatomia di un attacco alla supply chain

1. **Infiltrazione**

   I criminali informatici utilizzano diversi metodi per la violazione iniziale:

- Attacchi di forza bruta per mezzo di strumenti automatici per testare coppie di nome utente e password fino a trovare una corrispondenza

- Impersonificazione di un contatto fidato per inviare un'email di phishing o fraudolenta o link/allegati che contengono malware come keylogger o stealer

- Presa di controllo dell'account di un fornitore di fiducia

2. **Ricognizione**

- Una volta entrati in possesso di credenziali di accesso valide, i criminali informatici possono iniziare a sfruttare la rete e a danneggiare la reputazione del fornitore. Possono monitorare le comunicazioni tra il fornitore e i suoi clienti, alla ricerca di possibili vittime.

3. **Attacco**

- Terminata la fase di ricognizione, i criminali informatici possono utilizzare i sistemi compromessi del fornitore per violare le credenziali d'accesso, inviare fatture fraudolente o malware ai clienti.

Osservazioni della ricerca

Nel febbraio 2021, Proofpoint ha analizzato per una settimana i dati di 3.000 aziende di vari settori verticali negli Stati Uniti, nel Regno Unito e in Australia. In questo periodo, la maggior parte di queste aziende ha subito attacchi alla supply chain.

98% ha ricevuto una minaccia da un fornitore la cui identità era stata violata o il cui account era stato compromesso.

Il numero di attacchi è stato equamente distribuito tra tutti i paesi e i settori del campione preso in esame.

Quasi tre quarti di queste minacce implicavano un attacco di phishing o il furto d'identità.

Oltre il 30% delle email inviate dai domini dei fornitori conteneva malware.

IL "CRIMINE INFORMATICO COME SERVIZIO" HA FAVORITO GLI ATTACCHI ALLA SUPPLY CHAIN

Il dark web è un noto mercato per i kit di exploit e malware personalizzato utilizzati per vendere servizi come il noleggio di botnet e il ransomware. Come la maggior parte dei fornitori SaaS, i criminali informatici forniscono strumenti e piattaforme a coloro che effettuano attacchi alla supply chain, attacchi ransomware e altri crimini informatici. I criminali informatici che non dispongono di competenze tecniche avanzate possono ora perpetrare questo tipo di attacchi con facilità.

Come proteggere la tua azienda

Per contrastare le frodi e gli attacchi software alla supply chain di seguito alcuni controlli di sicurezza da implementare.

Frodi della supply chain

Per contrastare le frodi delle fatture dei fornitori, le aziende devono adottare un approccio completo a più livelli, dal momento che i criminali informatici spesso sfruttano congiuntamente più tecniche, spacciandosi per il fornitore e utilizzandone account compromessi.

Per contrastare le frodi delle fatture dei fornitori, le aziende devono adottare un approccio completo a più livelli, dal momento che i criminali informatici spesso sfruttano congiuntamente più tecniche, spacciandosi per il fornitore e utilizzandone account compromessi.

Gli attacchi di violazione dell'email aziendale (BEC, Business Email Compromise) spesso iniziano con un'email inviata da un criminale informatico che si spaccia per una persona di fiducia o che ne usurpa l'identità dopo aver compromesso il suo account. Dal momento che gli attacchi BEC non hanno un payload dannoso, sono difficili da rilevare da parte dei gateway di vecchia generazione che si basano unicamente sulla reputazione e sull'analisi del malware in un ambiente sandbox.

Di seguito come neutralizzare gli attacchi alla supply chain più comuni e costosi.

Visibilità sul rischio di frode via email da parte dei tuoi fornitori
Per comprendere meglio, comunicare e mitigare i rischi, poniti le seguenti domande:

- A quali rischi di attacchi BEC siamo esposti?
- Quali sono gli utenti più vulnerabili?
- Quali fornitori mettono in pericolo le nostre attività?
- Quali azioni dobbiamo intraprendere per mitigare i rischi?

Devi identificare gli utenti più colpiti dalle minacce fraudolente e quelli che hanno più probabilità di lasciarsi trarre in inganno.

Grazie a una visibilità granulare sui dettagli delle minacce BEC e all'identificazione di temi comuni sfruttati in tali attacchi, come le frodi nella fatturazione dei fornitori e il dirottamento degli stipendi, puoi comprendere e comunicare meglio i rischi legati agli attacchi BEC.

Rilevamento e blocco delle minacce fraudolente prima che si infiltrino nel tuo ambiente
Per bloccare le frodi dei fornitori che utilizzano l'email devi identificare tutte le tattiche correlate, tra cui lo spoofing del nome visualizzato, i domini fotocopia e le frodi sofisticate contro i fornitori. A tal fine, è necessaria una soluzione di sicurezza che analizzi in maniera dinamica i messaggi per identificare le numerose tattiche associate alle frodi delle fatture dei fornitori come:

- Dirottamento degli indirizzi di risposta
- Utilizzo di indirizzi IP dannosi
- Utilizzo di domini di fornitori la cui identità è stata usurpata
- Parole o espressioni comuni utilizzate nelle frodi dei fornitori

(La maggior parte delle soluzioni di protezione dell'email si basa esclusivamente su regole statiche o su dati contestuali limitati che richiedono un'ottimizzazione manuale).

Rafforzamento della resistenza degli utenti agli attacchi BEC
Gli attacchi BEC prendono di mira gli utenti e li inducono a perpetrare attività dannose. Poiché questi attacchi fraudolenti sfruttano il social engineering e il furto d'identità, i tuoi utenti sono spesso la tua ultima linea di difesa. Questo è il motivo per cui per ridurre i rischi di attacchi BEC sono necessarie sia la tecnologia che la formazione.

Insegna ai tuoi utenti a identificare e segnalare le email fraudolente sospette. Disporranno così delle conoscenze e delle competenze necessarie per proteggere la tua azienda da queste minacce innescate dall'uomo.

La visualizzazione di avvisi per le email sospette permette di valutare il rischio posto da ogni email. Per esempio, se i tuoi utenti vengono avvisati quando un messaggio viene inviato da un mittente esterno o da un dominio di recente registrazione saranno in grado di prendere decisioni più informate in caso di email sospette.

Protezione del tuo marchio contro gli attacchi di frode via email
Se da un lato sei preoccupato per i rischi posti dai tuoi fornitori, dall'altro i tuoi stessi clienti potrebbero nutrire preoccupazioni simili nei tuoi confronti.

I criminali informatici possono utilizzare il nome e il marchio della tua azienda per ingannare i tuoi clienti e partner commerciali. Anche se non si traduce necessariamente in perdite finanziarie dirette per la tua azienda, lo spoofing del marchio può danneggiare la sua reputazione, intaccare la fiducia della clientela e, in ultima analisi, avere conseguenze negative per la tua azienda.

Per prevenire l'invio di email fraudolente direttamente dal tuo account o da una terza parte designata, utilizza l'autenticazione delle email DMARC.

Attacchi software alla supply chain

Oltre ai più comuni attacchi alla supply chain presi in esame in precedenza, l'uso diffuso di software di terze parti o gestiti rappresenta un ulteriore tipo di rischio per la supply chain.

Se un fornitore compromesso offre software o servizi cloud, i criminali informatici possono alterare il codice sorgente e inserire malware nel processo di creazione e aggiornamento. I programmi o i servizi infettati dal payload dannoso incluso dal criminale informatico vengono poi distribuiti a clienti e partner.

Gli utenti non hanno sempre la possibilità di verificare i programmi delle terze parti che utilizzano, perciò devono confidare nell'affidabilità dei controlli di sicurezza implementati dai loro fornitori di software e rivenditori. La distribuzione di un software compromesso a un'azienda può esporla a un'ampia gamma di attacchi, dal furto di dati all'infezione da ransomware.

Questo tipo di attacco è particolarmente difficile da prevenire. Le vulnerabilità software senza patch sono uno dei vettori più comuni di attacco informatico. Per questo motivo, l'aggiornamento del software alla versione più recente è quindi la migliore difesa, ma costituisce ora anche un vettore d'attacco.

Per saperne di più

Considerato il numero di attacchi alla supply chain che conquistano i titoli dei giornali, è chiaro che i servizi di terze parti, i fornitori e i collaboratori rappresentano un serio rischio per il livello di sicurezza delle aziende. Una soluzione di sicurezza incentrata sulle persone in grado di rilevare nuovi strumenti di attacco, obiettivi e tattiche può contribuire a ridurre questo rischio.

Per saperne di più su come contrastare efficacemente gli attacchi alla supply chain, visita il sito **www.proofpoint.com/it**.