# Proteggere il settore della distribuzione dagli attacchi e-mail

Barracuda®
Your journey, secured.

# Aperto per i clienti, chiuso per i criminali

Il settore della distribuzione è sotto attacco. Gli attacchi informatici sono la nuova minaccia che va ad aggiungersi al taccheggio, alle frodi con carta di credito e ai furti da parte di dipendenti. Il vettore più comune per propagare questi attacchi è probabilmente costituito dalle e-mail e il settore della distribuzione è un bersaglio.

Quando si sente parlare di criminalità informatica legata alle e-mail, si pensa in primo luogo a messaggi spam pieni di errori, inviati da principi stranieri che offrono milioni. Per quanto queste e-mail possano essere oggetto di battute spiritose, funzionano ancora oggi. Ogni anno, sono migliaia le vittime. Nel 2018, calcolando soltanto i malcapitati negli Stati Uniti, queste frodi hanno fruttato 700.000 dollari. E questa antesignana forma di criminalità informatica legata alla posta elettronica ha dato origine a un'intera generazione di pericolosi discendenti.



Barracuda.

Si prevede che, entro il 2023, l'incidenza del Business Email Compromise (BEC), in cui i malintenzionati impersonificano un dipendente di un'azienda per tentare di trarre in inganno altri dipendenti e indurli a condividere informazioni o ad approvare transazioni finanziarie, andrà raddoppiando ogni anno, arrivando a sottrarre all'economia 5 miliardi di dollari. Barracuda riconosce i 13 tipi di minacce e-mail, classificate in diverse categorie:

**Spam:** volumi elevati di messaggi indesiderati, in genere inviati in massa. Influisce sulla produttività delle aziende intasando le caselle di posta in arrivo e sommandosi ai carichi dei server di posta: circa la metà del traffico globale di e-mail è costituito da spam.

**Malware:** progettato per causare danni, interrompere le attività, esfiltrare dati o accedere in altro modo a un sistema remoto. La distribuzione di malware avviene solitamente tramite allegati e-mail o URL che indirizzano a contenuti dannosi.

**Esfiltrazione di dati:** si verifica quando utenti non autorizzati copiano o recuperano dati da un sistema. I costi per rimediare ai danni e alla perdita di credibilità, oltre alle sanzioni normative, possono essere ingenti.

**Phishing:** e-mail aventi lo scopo di raggirare gli utenti finali, inducendoli a credere che il messaggio provenga da una fonte affidabile e a rispondere comunicando credenziali, trasferendo denaro o agendo secondo altre modalità pericolose.

**Impersonificazione del dominio:** si tratta di un tentativo, di solito associato al phishing, di convincere il destinatario che l'e-mail provenga da una persona, marchio o URL affidabile, al fine di svolgere attività illecite. I malintenzionati possono utilizzare un marchio attendibile per indurre il personale a fornire dati sensibili o credenziali per accedere ai sistemi dell'organizzazione.

Spams

Esfiltrazione di dati

Impersonificazione del dominio

Malwares

Phishing



Barracuda.

# Il settore della distribuzione è nel mirino

Le organizzazioni di vendita al dettaglio costituiscono un bersaglio di alto profilo. Si tratta di attività per loro stessa natura aperte al pubblico, in cui le interazioni sono la norma. Un servizio rapido ed efficiente è considerato un elemento distintivo. Durante la pandemia di COVID-19 abbiamo inoltre assistito alla crescita dell'e-commerce, che è passato dal 14% delle vendite al dettaglio globali nel 2019 al 17% nel 2020. I rivenditori hanno incrementato la loro presenza online e si è ampliata anche la superficie di attacco. Il problema diventa quindi come mantenere al sicuro l'attività senza influire negativamente sul servizio.

Sebbene tutte le organizzazioni siano destinatarie di attacchi e ricevano in media 14 e-mail dannose per dipendente all'anno, nel settore retail i dipendenti ne ricevono ben 49. Questo fa della distribuzione il principale bersaglio di attacchi e-mail.

Le organizzazioni di vendita al dettaglio sono realtà molto diversificate e variano da negozi singoli a catene regionali, fino a grandi aziende nazionali o multinazionali. Sono tuttavia accomunate da diversi fattori, che le rendono un bersaglio allettante. Essere consapevoli dei rischi è importante per attenuarli. Fra questi figurano:

**Incremento dell'e-commerce:** l'e-commerce era già in espansione, ma durante la pandemia ha visto crescere esponenzialmente la sua popolarità. Il volume di e-mail è aumentato, tanto per effetto di ordini e richieste dei clienti quanto per le comunicazioni interne e con i fornitori, ponendo sotto stress sia i sistemi che i dipendenti.

**Varie sedi:** molte aziende del settore hanno più sedi, fra cui negozi, magazzini, contact center e uffici. Un attacco e-mail andato a segno in una qualsiasi delle sedi può fornire ai criminali l'accesso all'intera rete.

**Dati di valore:** mentre alcuni attacchi sono semplicemente atti malevoli, la maggior parte di quelli inviati via e-mail ha lo scopo di trarre profitti materiali o finanziari. Le aziende del settore retail detengono grandi quantità di dati di valore, fra cui le informazioni di identificazione personale di clienti, dipendenti e fornitori, oltre a informazioni su conti e pagamenti.

**Necessità di formazione per gli utenti:** gli utenti costituiscono la prima, e probabilmente anche la migliore, linea di difesa nei confronti della compromissione. Fornendo loro la formazione necessaria a riconoscere e segnalare le minacce e-mail è possibile migliorare la sicurezza.

**Diversi fornitori:** in questo settore di attività si intrattengono rapporti con fornitori e partner, creando complesse reti di approvvigionamento. È essenziale garantire che le parti coinvolte mantengano anche una buona pulizia dell'e-mail. Una delle più vaste compromissioni di un'azienda del settore retail mai avvenute è stata la violazione dei dati a carico di Target, messa a segno tramite un fornitore di sistemi di climatizzazione e riscaldamento con sede negli Stati Uniti  caduto vittima di un attacco di phishing che ha avuto origine da un'e-mail.

È importante tenere presente che gli attacchi e-mail non sono fini a sé stessi. Un attacco spam generico può essere finalizzato a indurre gli utenti a fare clic su un link che scarica malware, che a sua volta scatena un attacco ransomware nella rete. Un'e-mail di phishing può essere un tentativo di ottenere credenziali di accesso dagli utenti. Una volta entrati nel sistema, i criminali possono esfiltrare dati, rubando file e carpendo informazioni o proprietà intellettuali. Una buona sicurezza dell'e-mail può essere paragonata a chiudere le porte e le finestre di un edificio: non è la sola cosa da fare, ma se non la si fa, tutti gli altri passaggi risulteranno più difficili e meno efficaci.

# Una buona sicurezza dell'e-mail è un ottimo punto di partenza

La crescita dell'e-commerce è stata una manna per le organizzazioni di vendita al dettaglio, ma ha cambiato il loro modo di interagire con il mondo. La difesa delle comunicazioni e-mail, essenziale per salvaguardare l'intera rete, deve tenersi al passo con il numero crescente di attacchi. Fortunatamente si possono applicare più livelli di sicurezza alla posta elettronica.

Gli attacchi e-mail si sono evoluti nel corso degli anni e le difese tradizionali non bastano. La protezione del gateway è sempre necessaria per le organizzazioni, che devono però difendersi anche ad altri livelli:

1. **Livello del gateway**
2. **Livello della casella di posta in arrivo**
3. **Livello umano**




Barracuda.

## 1. Livello del gateway

I gateway e-mail sono il punto di partenza per la sicurezza della posta elettronica. Bloccano la maggior parte dei messaggi dannosi, inclusi quelli di spam, gli attacchi di phishing su larga scala, il malware, i virus e gli attacchi zero-day. Le organizzazioni che li utilizzano correttamente potenziano l'efficacia dei livelli successivi.

## 2. Livello della casella di posta in arrivo

La protezione sul piano del gateway non è sufficiente. Il successivo requisito è la difesa a livello della casella di posta in arrivo basata su API, utile per identificare le e-mail dannose che superano la barriera del gateway, utilizzando informazioni sulle comunicazioni interne e cronologiche per segnalare i messaggi potenzialmente dannosi.

## 3. Livello umano

Gli attacchi sono in costante evoluzione e diventano sempre più sofisticati. Abbiamo assistito al passaggio dallo spam generico allo spear phishing (che è più mirato), fino ad arrivare a impersonificazioni e furti di account estremamente sofisticati che, in alcuni casi, sono riusciti addirittura a convincere le persone di stare seguendo le disposizioni del CEO. La formazione per gli utenti, fra i quali possono rientrare studenti, genitori, docenti e personale, apporta un livello di sicurezza essenziale e insegna loro a riconoscere e segnalare i contenuti dannosi.

# Conclusione

Seguendo le best practice di sicurezza per l'email si possono ridurre sostanzialmente i rischi, ma deve sempre esistere un piano di backup (inteso sia in modo figurato che letterale) in caso di possibili infiltrazioni. La difesa strutturata su più livelli riduce i rischi e contiene i danni al minimo.

Sebbene i rischi siano reali, per quanto riguarda la difesa dell'e-mail le notizie sono confortanti. Se gli attacchi aumentano per numero e sofisticatezza, migliorano anche gli strumenti a disposizione per difendersi. Da ogni attacco sono state ricavate informazioni utili che hanno portato allo sviluppo di algoritmi sempre più sofisticati e strumenti di formazione migliori. È possibile tenere aperti i negozi mantenendo al sicuro la posta elettronica. Saremmo lieti di approfondire l'argomento con voi.

# Informazioni su Barracuda

Barracuda si adopera per rendere il mondo più sicuro. Crediamo che tutte le aziende meritino l'accesso a soluzioni di sicurezza di livello enterprise cloud-first, che siano semplici da acquistare, implementare e utilizzare. Proteggiamo l'e-mail, le reti, i dati e le applicazioni con soluzioni innovative espandibili e adattabili lungo il percorso dei clienti. Oltre 200.000 organizzazioni di tutto il mondo si affidano a Barracuda per essere protette in modi per cui non sanno nemmeno di essere a rischio, per potersi concentrare sulla propria attività e salire di livello. Per ulteriori informazioni visitate il sito barracuda.com.

Barracuda®
Your journey, secured.

Contattateci liberamente per sottoporci domande sulla protezione della vostra organizzazione dalle minacce e-mail.