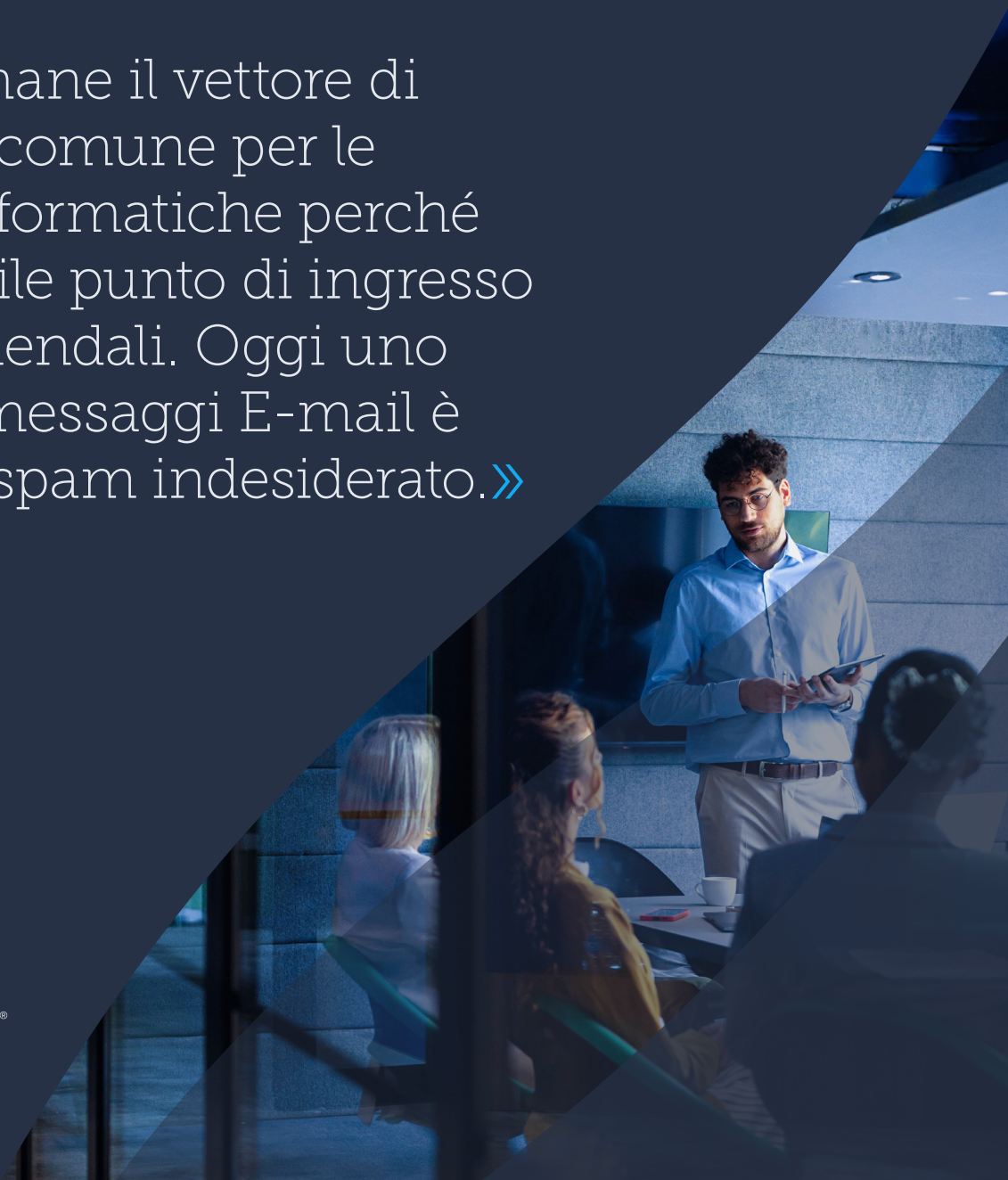
RAPPORTO SULLE MINACCE E-MAIL DEL 2025

Risultati chiave sull'evoluzione delle minacce basate sulla posta elettronica

L'E-mail rimane il vettore di attacco più comune per le minacce informatiche perché offre un facile punto di ingresso nelle reti aziendali. Oggi uno su quattro messaggi E-mail è dannoso o spam indesiderato.»



Barracuda

Sommario

Risultati principali

1 E-mail su 4 è dannoso o spam indesiderata.

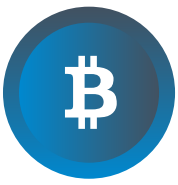
L'**83%** dei documenti dannosi di Microsoft 365 contiene codici QR che portano a siti web di phishing.

Il 20% delle aziende subisce almeno un incidente di furto di account (ATO) ogni mese.

Quasi la metà di tutte le aziende non ha configurato una policy dMARC, esponendole al rischio di spoofing, attacchi di phishing e compromissione di posta elettronica aziendale.

Quasi **un quarto** di tutti gli allegati HTML sono dannosi.

Più di **tre quarti** delle aziende non prevengono attivamente le e-mail di spoofing.



Le truffe di tipo "sextortion" basate su Bitcoin, una tendenza emergente, rappresentano **Il 12%** degli allegati PDF dannosi.

L'evoluzione e l'impatto delle minacce basate su e-mail

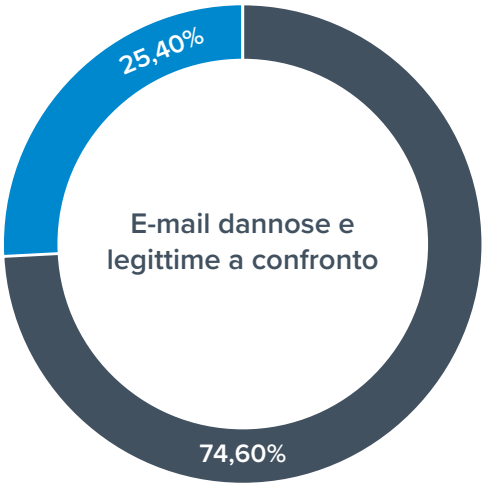
Il panorama delle minacce e-mail è in continua evoluzione, poiché i criminali informatici sviluppano tattiche più sofisticate per sfruttare individui e organizzazioni. L'E-mail rimane il vettore di attacco più comune per le minacce informatiche perché fornisce un facile punto di accesso alle reti aziendali. **Un messaggio E-mail su quattro oggi è dannoso o spam.** Gli attori delle minacce utilizzano una combinazione di social engineering, automazione e malware avanzato per aggirare le difese di sicurezza e indurre i destinatari ad agire, ad esempio facendo clic su un link dannoso, aprendo un allegato infetto o trasferendo fondi su conti fraudolenti.

Metodologia

Questo rapporto contiene una ricerca proprietaria di Barracuda raccolta nel febbraio 2025. Durante quel periodo di tempo, sono stati analizzati quasi 670 milioni di E-mail dannose, spam o indesiderate. Il rapporto presenta i risultati chiave sui dati relativi a quella minaccia.

L'impatto degli attacchi basati su e-mail può essere grave, spaziando da perdite finanziarie e violazioni dei dati a sanzioni normative e danni alla reputazione. Un attacco riuscito può interrompere le operazioni aziendali, esporre informazioni sensibili su clienti e dipendenti e portare a conseguenze finanziarie e legali a lungo termine.

Poiché gli attaccanti perfezionano costantemente le loro tattiche per eludere le misure di sicurezza tradizionali, le organizzazioni devono mitigare i rischi adottando un approccio multilivello alla sicurezza e-mail, sfruttando il rilevamento delle minacce basato sull'IA, il monitoraggio in tempo reale e la formazione sulla consapevolezza dell'utente.



Impatto sulle piccole e medie imprese

Le piccole imprese sono particolarmente vulnerabili alle minacce e-mail, a causa delle risorse limitate per la sicurezza informatica, dei team IT ridotti e delle infrastrutture di sicurezza meno sviluppate. Spesso devono fare affidamento su soluzioni di sicurezza email di base che potrebbero non essere in grado di gestire attacchi sofisticati, come il Business Email Compromise (BEC), il phishing e il ransomware. Un attacco riuscito può avere conseguenze devastanti, portando a perdite finanziarie, danni alla reputazione e persino alla chiusura dell'attività. Con i requisiti normativi che diventano più severi, anche una piccola violazione dei dati potrebbe comportare multe e conseguenze legali.

Ecco uno sguardo ad alcuni degli attacchi più comuni rilevati dai sistemi Barracuda che verranno trattati in questo rapporto.

24%

Le e-mail di massa possono ingombrare le caselle di posta, rendendo più difficile per gli utenti identificare i messaggi importanti e potenzialmente causando la trascuratezza delle e-mail critiche.

21%

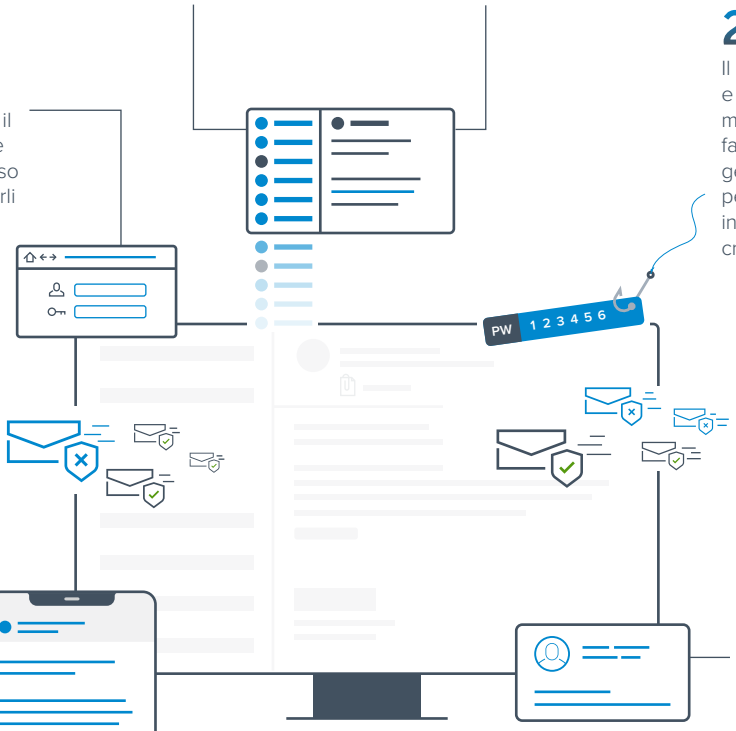
Spam può sovraccaricare i sistemi di posta elettronica, portando a una diminuzione della produttività e a un aumento dei costi operativi per le aziende.

2%

Spoofing e attacchi di furto d'identità coinvolgono attaccanti che falsificano l'indirizzo E-mail o il dominio del mittente per apparire come una fonte attendibile, spesso per ingannare i destinatari e indurli a divulgare informazioni sensibili.

23%

Il **Phishing** è un attacco su larga scala e indiscriminato che prende di mira molti destinatari contemporaneamente, facendo affidamento su esche generiche. Gli attacchi sono progettati per indurre i destinatari a rivelare informazioni sensibili, come le credenziali di accesso.



7%

La **posta non autenticata** si riferisce alle e-mail che mancano di una verifica adeguata tramite protocolli di autenticazione come SPF, DKIM o DMARC. Queste e-mail possono essere più suscettibili allo spoofing, al phishing e ad altre attività fraudolente.

0.02%

Dirottamento delle conversazioni comporta che gli attaccanti si infiltrino nei thread di posta elettronica compromettendo gli account email e inserendosi nelle comunicazioni in corso.

0.2%

Email di estorsione minacciano i destinatari con conseguenze negative, come la divulgazione di informazioni sensibili o il lancio di attacchi informatici, a meno che non venga pagato un riscatto.

0.25%

Spear phishing è un attacco altamente mirato, personalizzato per individui o organizzazioni specifiche, che utilizza il social engineering, il furto d'identità e contenuti personalizzati per aumentare la credibilità e aggirare le difese di Sicurezza tradizionali.

0.5%

Gli allegati dannosi contengono codice malevolo che può installare ransomware, spyware e altri tipi di malware, portando a violazioni dei dati o compromissioni del sistema.

0.03%

La Business Email Compromise (BEC) comporta il furto d'identità di persone fidate, come dirigenti o partner commerciali, per ingannare i dipendenti a trasferire fondi o divulgare informazioni sensibili.

22%

La **Category** include la posta bloccata e messa in quarantena, come i messaggi con destinatari non validi o quelli contrassegnati a causa di politiche personalizzate.

Allegati dannosi utilizzati per distribuire malware e sfruttare le vulnerabilità

Gli allegati E-mail sono spesso utilizzati per distribuire malware, avviare campagne di phishing e sfruttare le vulnerabilità. I dati mettono in evidenza la diffusione di allegati dannosi tra diversi tipi di file.

I file HTML vengono utilizzati come armi più spesso

Nonostante un volume totale relativamente basso, **gli allegati HTML si distinguono come i file più utilizzati per attacchi, costituendo più di tre quarti dei file dannosi rilevati. Con il 23% contrassegnato come dannoso**, sono uno dei tipi di file più rischiosi. Gli attaccanti utilizzano spesso file HTML per il phishing, incorporando script dannosi che reindirizzano gli utenti a pagine di accesso false progettate per rubare credenziali. I team di sicurezza devono implementare politiche rigorose sugli allegati HTML, come la scansione degli script incorporati e il blocco definitivo dei file sospetti.

I documenti di Microsoft 365 hanno un tasso di rischio relativamente basso, ma rimangono una minaccia

I documenti di Microsoft 365 sono comunemente utilizzati sia nelle comunicazioni aziendali legittime che negli attacchi informatici. Con un tasso di attacchi dannosi relativamente basso (0,17%), gli attaccanti continuano a sfruttare i documenti di Microsoft 365 per distribuire malware, spesso utilizzando macro o link incorporati.

I PDF hanno meno probabilità di essere dannosi

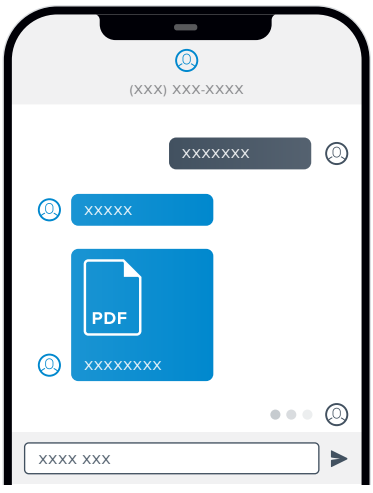
I PDF sono di gran lunga il tipo di file più frequentemente condiviso negli allegati e-mail. Hanno un basso livello di rischio, con solo lo 0,13% dei PDF che risultano dannosi.

Tuttavia, i PDF stanno iniziando a essere utilizzati più frequentemente nelle campagne di phishing, spesso contenenti script incorporati o link ingannevoli per indirizzare i destinatari a siti di raccolta di credenziali.

Le truffe di sextortion con Bitcoin, una tendenza emergente, rappresentano il 12% degli allegati PDF dannosi. In questi attacchi, i criminali informatici inviano e-mail contenenti PDF che affermano di avere informazioni compromettenti sulla vittima, spesso sostenendo di avere filmati della webcam hackerati o cronologia di navigazione rubata. I PDF includono messaggi minacciosi che richiedono pagamenti in Bitcoin per evitare la diffusione di queste presunte prove. Queste truffe si basano sulla paura e sull'urgenza per spingere le vittime a pagare, anche quando non c'è stato alcun vero compromesso.

12%

gli allegati PDF dannosi vengono utilizzati nel sextortion



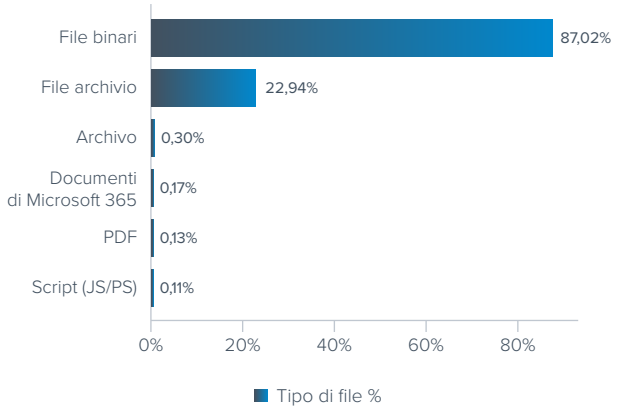
I file binari rappresentano un rischio estremo

Un allarmante 87% dei file binari rilevati erano dannosi. Ciò evidenzia la necessità di politiche rigorose contro l'invio di file eseguibili tramite e-mail. Poiché gli eseguibili possono installare direttamente malware, i team di sicurezza dovrebbero considerare il blocco dei file binari (a meno che non siano assolutamente necessari) e assicurarsi che tutti i download vengano scansionati prima dell'esecuzione.

I file di archiviazione e gli script hanno bassi tassi di rilevamento ma presentano comunque dei rischi

I file di archivio, come ZIP e RAR, hanno un tasso di malware relativamente basso dello 0,3%. Tuttavia, gli attaccanti li utilizzano per raggruppare malware ed eludere il rilevamento. Allo stesso modo, gli script (inclusi JavaScript e PowerShell) sono rari e solo lo 0,11% è stato segnalato come dannoso. Ma questo non elimina il rischio poiché gli script possono eseguire payload pericolosi, specialmente quando sono incorporati in altri tipi di file.

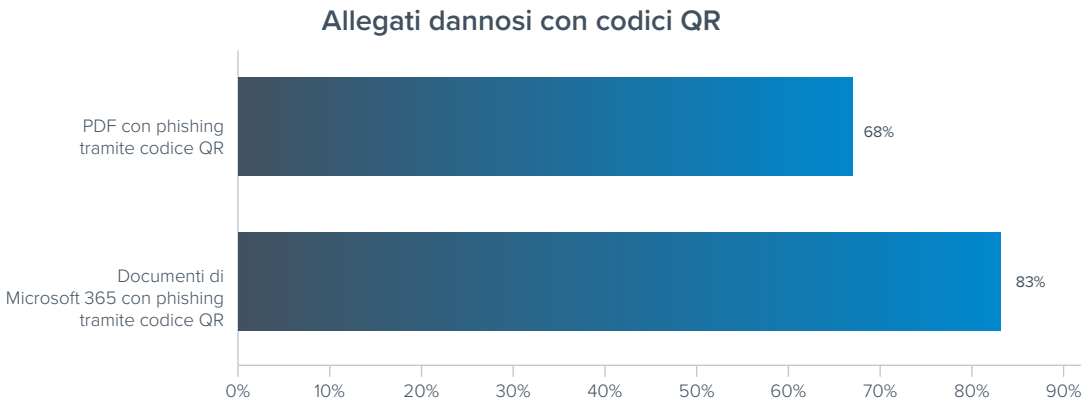
Percentuali dei diversi tipi di allegati dannosi



Codici QR negli allegati

I criminali informatici stanno sempre più spesso incorporando codici QR dannosi negli allegati e-mail per ingannare gli utenti e aggirare la sicurezza tradizionale.

I codici QR dannosi sono incorporati nei formati di file comunemente utilizzati. **Il 68% dei PDF dannosi e l'83% dei documenti Microsoft 365 dannosi contengono codici QR** che conducono a siti web di phishing o altri siti dannosi. Questi tipi di file sono ampiamente fidati negli ambienti aziendali, rendendoli efficaci negli attacchi di social engineering. Una volta scansionato il codice QR, le vittime vengono reindirizzate a pagine di phishing che imitano i portali di accesso di Microsoft 365, dove gli attaccanti rubano le credenziali per compromettere gli account aziendali. Questa tendenza crescente evidenzia la necessità di misure di sicurezza avanzate in grado di analizzare i codici QR negli allegati.



Gli attaccanti favoriscono sempre più l'uso dei codici QR per diversi motivi:

Evasione dei filtri di sicurezza tradizionali

I tradizionali sistemi di sicurezza e-mail si concentrano spesso sul rilevamento di URL e allegati dannosi. I codici QR, essendo immagini, possono eludere questi filtri, rendendo più facile per gli attaccanti consegnare i loro payload inosservati.

Fiducia e coinvolgimento degli utenti

I codici QR sono diventati comuni nella vita quotidiana, utilizzati per tutto, dalla visualizzazione del menu di un ristorante all'effettuazione di un pagamento senza contatto. Questa familiarità può indurre gli utenti a scansionare i codici senza sospetti, aumentando la probabilità di attacchi riusciti.

Targeting dei dispositivi mobili

La scansione dei codici QR di solito coinvolge dispositivi mobili, che potrebbero non disporre dei robusti controlli di sicurezza presenti sui computer desktop aziendali. Questo cambiamento consente agli attaccanti di portare l'attacco al di fuori del firewall della vostra azienda.

Identificare i codici QR dannosi negli allegati e-mail è una sfida perché il contenuto codificato rimane invisibile fino alla scansione, impedendo agli utenti di valutarne la legittimità in anticipo. Molti scanner di sicurezza danno priorità alle minacce basate su testo, spesso trascurando i codici QR incorporati nelle immagini e nei PDF.

I link dannosi costituiscono una minaccia persistente e diffusa

I link dannosi rimangono uno degli strumenti più comuni ed efficaci per i criminali informatici. Con dati che dimostrano che **1 link su 100** è dannoso, le organizzazioni devono affrontare una minaccia persistente e diffusa. Questi link sono incorporati nelle e-mail di phishing, negli attacchi di impersonificazione e nelle campagne di malware. Alcuni potrebbero aggirare i filtri di sicurezza tradizionali apparendo legittimi a prima vista.

Dove conducono i link dannosi e il loro impatto

Pagine di phishing e acquisizione di credenzialig

Gli attaccanti creano pagine di accesso false che imitano servizi legittimi, come Microsoft 365. Quando le vittime inseriscono le proprie credenziali, le informazioni vengono inviate direttamente agli attaccanti. Una volta compromessi, questi account vengono utilizzati per ulteriori attacchi, tra cui il phishing interno e il Business Email Compromise (BEC).

Download di malware e ransomware

I link dannosi conducono a siti web che ospitano download infetti da malware, spesso camuffati da fatture, aggiornamenti software o avvisi di sicurezza.

Portali di pagamento falsi e fraud

I criminali informatici si spacciano per dirigenti aziendali o fornitori, inviando fatture con collegamenti a siti di pagamento fraudolenti progettati per rubare dati sensibili o avviare transazioni non autorizzate.

Dato che l'1% di tutti i link è dannoso, le aziende devono presumere che i dipendenti si imbatteranno inevitabilmente in URL dannosi. Combinando misure di sicurezza proattive con l'educazione degli utenti, le organizzazioni possono ridurre significativamente i rischi posti da queste minacce ingannevoli.

Il furto di account consente il furto di dati e il phishing laterale

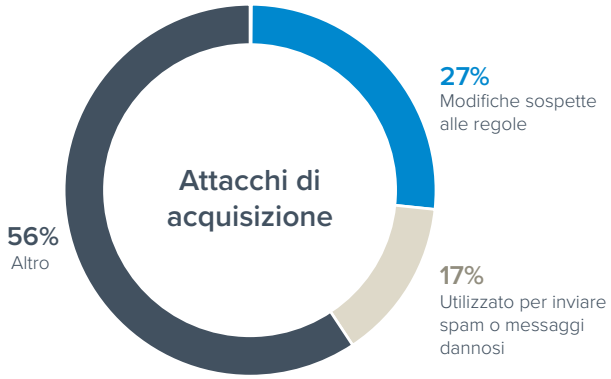
Il Furto di account (ATO) è una minaccia informatica comune, con il 20% delle aziende che subiscono almeno un incidente ATO al mese. Gli attaccanti tipicamente ottengono l'accesso tramite phishing, credential stuffing o sfruttando password deboli o riutilizzate. Una volta all'interno di un account, possono rubare dati sensibili, muoversi lateralmente all'interno dell'organizzazione e inviare e-mail di phishing che sembrano provenire da una fonte affidabile.

20%

delle aziende subiscono almeno un incidente di furto di account al mese

I segni più comuni dell'ATO includono accessi sospetti da località o dispositivi sconosciuti, regole di inoltro email non autorizzate, richieste improvvise di reimpostazione della password e un aumento delle e-mail di phishing in uscita da account compromessi.

Gli attacchi ATO creano rischi di Sicurezza a lungo termine, consentendo agli attaccanti di condurre attività di ricognizione e diffondere ulteriori attacchi. **Il 27% degli incidenti ATO ha coinvolto modifiche sospette delle regole**, come l'impostazione dell'inoltro di E-mail a un indirizzo esterno o l'eliminazione automatica degli avvisi di sicurezza in arrivo. Queste tattiche aiutano gli attaccanti a mantenere la persistenza e a evitare il rilevamento. Inoltre, **il 17% degli account compromessi è stato utilizzato per inviare spam o messaggi dannosi**, spesso portando a ulteriori attacchi di phishing, distribuzione di malware o truffe BEC.



Per mitigare i rischi associati all'ATO, le PMI dovrebbero dare priorità all'autenticazione a più fattori (MfA), al Training per la sensibilizzazione sulla sicurezza e al monitoraggio automatico delle attività sospette sugli account.

Proteggere le aziende dallo spoofing delle e-mail

Domain-based Message Authentication, Reporting and Conformance (dMARC), un protocollo di autenticazione delle E-mail, protegge i domini di posta elettronica dall'uso non autorizzato, inclusi attacchi di spoofing e di furto d'identità. Sfruttando il Sender Policy Framework (SPF) e DomainKeys Identified Mail (DKIM), dMARC garantisce che solo i mittenti autorizzati possano inviare E-mail dal tuo dominio.

Quando configurato in modo efficace, DMARC fornisce alle organizzazioni:

- Protezione contro lo spoofing di dominio per salvaguardare la loro reputazione
- Approfondimenti di reporting attuabili per monitorare l'autenticazione delle e-mail e l'uso non autorizzato del loro dominio
- Migliorata la recapitabilità delle E-mail costruendo fiducia con i fornitori di servizi di posta elettronica

Tuttavia, quasi la metà dei domini non ha una politica DMARC configurata e solo il 23% ha l'applicazione DMARC impostata.

Il fatto che **il 77% delle aziende** (il 47% senza registrazione e il 30% con una politica di "solo monitoraggio") **non stia prevenendo attivamente le email contraffatte** rappresenta una significativa lacuna di sicurezza. Senza un'applicazione rigorosa, gli attaccanti possono impersonare aziende legittime con Business Email Compromise (BEC), attacchi di phishing e altre minacce. Questa mancanza di protezione non solo mette a rischio l'organizzazione, ma danneggia anche la reputazione del marchio quando clienti o Partners ricevono email fraudolente che sembrano provenire da un dominio affidabile.

Per le aziende, la mancata applicazione dell'applicazione DMARC comporta:

- Aumento del rischio di attacchi di furto d'identità che portano a perdite finanziarie e di dati
- Tassi di fraud via E-mail più elevati, poiché i criminali informatici sfruttano domini non protetti
- Riduzione della recapitabilità delle E-mail, poiché i provider di posta elettronica preferiscono sempre più i domini autenticati

Perché le organizzazioni dovrebbero adottare l'applicazione del DMARC

Per proteggersi completamente dallo spoofing del dominio, le aziende dovrebbero passare gradualmente da una politica dMARC impostata su «p=none», che è la modalità di solo monitoraggio, a una politica impostata su «p=reject», che rifiuterà completamente le e-mail non autenticate. Questo assicura che le e-mail non autorizzate vengano bloccate, riducendo il rischio di phishing e migliorando la fiducia nelle comunicazioni e-mail aziendali. Le organizzazioni dovrebbero inoltre esaminare regolarmente i report dMARC per ottenere informazioni sulle attività di E-mail non autorizzate e perfezionare le proprie politiche di conseguenza.

DMARC è un controllo di Sicurezza fondamentale ma sottoutilizzato che aiuta le organizzazioni a difendersi dal phishing e dalle frodi via E-mail. Con quasi la metà delle aziende prive di protezione dMARC e solo l'11% che applica le politiche dMARC, gli attaccanti continuano a sfruttare l'E-mail come vettore di attacco principale. Le aziende devono dare priorità all'applicazione del dMARC per rafforzare la loro postura di sicurezza e-mail e proteggere il loro marchio, i dipendenti e i clienti dalle minacce e-mail.

Best practice per proteggersi dagli attacchi basati su e-mail

Mentre i criminali informatici continuano ad adattare le loro tattiche, i professionisti IT e della Sicurezza devono rimanere concentrati sull'evoluzione degli attacchi email.

Ecco cinque pratiche migliori di sicurezza informatica che tutte le organizzazioni dovrebbero implementare per ridurre il rischio e aumentare la resilienza informatica.

1. **Implementa una sicurezza e-mail multilivello.** La maggior parte delle organizzazioni oggi dispone di robusti filtri antispam e antimalware, ma non sempre sono configurati correttamente per bloccare efficacemente i messaggi dannosi. I team IT devono eseguire regolarmente un controllo dello stato delle impostazioni del gateway di posta elettronica per garantire prestazioni ottimali.

   Con l'evolversi delle minacce, dovrebbe evolversi anche la protezione della Sua organizzazione. I truffatori stanno adattando le loro tattiche per aggirare i gateway e i filtri antispam, quindi è fondamentale disporre di una soluzione che rilevi e protegga dagli attacchi di phishing. Integra i suoi gateway con una tecnologia di sicurezza e-mail cloud basata sull'IA che non si affida esclusivamente alla ricerca di link o allegati dannosi.

2. **Protegga l'accesso degli utenti.** La protezione degli accessi e degli account degli utenti dovrebbe essere parte integrante della strategia di sicurezza informatica della sua organizzazione. Inizi a utilizzare l'autenticazione a più fattori (MfA), che fornisce un ulteriore livello di sicurezza oltre a nome utente e password. Oggi, le organizzazioni dovrebbero prendere in considerazione una strategia Zero Trust più avanzata, per verificare continuamente e consentire solo agli utenti giusti di accedere alle risorse giuste. L'implementazione della tecnologia Zero Trust Access protegge l'accesso e riduce l'esposizione agli attacchi laterali.

3. **Automatizza l'Incident Response.** Una soluzione automatizzata per l'Incident Response La aiuterà a eliminare rapidamente qualsiasi minaccia trovata nelle caselle di posta degli utenti, rendendo la correzione più efficiente per tutti i messaggi E-mail in futuro.

4. **Migliorare la consapevolezza della sicurezza informatica.** Educare gli utenti sulle ultime Minacce e-mail rendendole parte del Training per la sensibilizzazione sulla sicurezza. Assicurarsi che i dipendenti possano riconoscere questi attacchi, comprenderne la natura fraudolenta e sapere come segnalarli. Utilizzare la Simulazione del phishing per E-mail e Casella vocale per addestrare gli utenti a identificare gli attacchi informatici, testare l'efficacia della formazione e valutare gli utenti più vulnerabili agli attacchi.

5. **Proteggi ed esegui il backup di tutti i dati.** Per evitare la perdita di dati a seguito di un attacco basato su e-mail, come il ransomware, i tuoi dati devono essere adeguatamente protetti, isolati e sottoposti a backup. È inoltre necessario assicurarsi che la soluzione di backup consenta di ripristinare i dati in un lasso di tempo ragionevole. Assicurati di eseguire esercitazioni e di testare regolarmente i tuoi backup per assicurarti di essere completamente preparato.

Informazioni su Barracuda

Barracuda è un'azienda leader nel settore della sicurezza informatica, in grado di fornire una protezione completa contro le minacce complesse. La nostra piattaforma protegge e-mail, dati, applicazioni e reti con soluzioni innovative e un servizio XDR gestito, per rafforzare la resilienza informatica. Centinaia di migliaia di professionisti IT e fornitori di servizi gestiti in tutto il mondo si affidano a noi per avere protezione e supporto con soluzioni facili da acquistare, implementare e utilizzare. Per ulteriori informazioni, visitare il sito barracuda.com.

Barracuda