Isolamento dei link e-mail

Isolare i link delle e-mail per ridurre la superficie d'attacco e semplificare le operazioni

Ridurre i rischi di phishing applicando tecniche di isolamento e controllo dei browser

La sfida: sofisticate tecniche di phishing multicanale

Il phishing multicanale viene attuato con l'impiego di e-mail e siti web configurati in modo da aggirare le regole di filtering. Tra le tipologie più comuni di questo tipo di truffa troviamo:

- **Phishing differito**: un link inizialmente innocuo all'interno di un'e-mail viene "letalizzato" dopo la consegna associandolo a una destinazione dannosa.
- **Phishing di servizi cloud:** collegamenti HTTPS pericolosi che assomigliano ai servizi cloud più diffusi (ad es., Google Drive, Box)

Per fermare questi tipi di minacce, un sistema di protezione delle e-mail moderno deve poter essere in grado di applicare a tutti i link la filosofia di controllo Zero Trust: "fidarsi mai, verificare sempre".

La soluzione: l'isolamento dei link e-mail

L'integrazione delle capacità di isolamento in remoto dei browser (Remote Browser Isolation, RBI) con la Cloud Email Security (CES) consente di incrementare notevolmente la protezione contro il phishing. I clienti di Cloudflare Area 1 possono attivare Cloudflare Browser Isolation per neutralizzare queste minacce multicanale.

Gli amministratori hanno la possibilità di controllare le interazioni degli utenti sulle pagine web isolate (ad esempio limitando gli input della tastiera e i caricamenti di file) per prevenire conseguenze spiacevoli come la raccolta fraudolenta di credenziali o il furto di dati riservati.

Inoltre, l'apertura dei link in un browser isolato neutralizza il malware caricandone il codice sul cloud, lontano dai dispositivi in locale.

Cosa dicono gli analisti:

"Gli URL basati su e-mail con risoluzione esterna sono utilizzati di frequente per il phishing dei dipendenti. Il loro isolamento è in grado di ridurre con successo gli attacchi di phishing."

"La maggior parte degli attacchi viene condotta sfruttando l'Internet pubblico, sia tramite la navigazione sul web che con collegamenti inviati via e-mail che inducono con l'inganno i destinatari a visitare siti dannosi. La semplice rimozione (o, ancora più efficace, l'isolamento) del browser dal desktop dell'utente finale migliora considerevolmente lo stato di sicurezza di un'azienda, tutelandola anche da attacchi di tipo ransomware."

"Il consiglio è valutare e implementare a titolo sperimentale una soluzione per l'isolamento dei browser per specifici utenti ad alto rischio (come il team Finanza) o determinati casi d'uso (come il rendering degli URL basati su e-mail), specialmente se la propria azienda è avversa al rischio." [1]

Gartner

Leggi di più

I vantaggi per l'azienda derivanti dall'integrazione di CES e RBI

Potenziamento della protezione dal phishing

L'isolamento delle e-mail non solo è in grado di impedire al codice dannoso di un link di phishing di andare in esecuzione localmente, ma applica anche controlli di protezione dei dati per evitare che informazioni sensibili possano cadere in mani sbagliate.

Migliore produttività dei team IT e di sicurezza informatica

Bastano pochi clic per attivare l'isolamento delle e-mail per qualunque sito web.

I team IT e della sicurezza informatica sono sollevati dall'incombenza di configurare politiche di filtering che rischiano di bloccare eccessivamente (limitando la produttività dell'utente) o non a sufficienza (lasciando campo libero alle minacce).

Caso d'uso esemplificativo: fermare il phishing differito

Il problema: il phishing differito sfugge al rilevamento

Con le giuste tattiche e motivazioni, le campagne di phishing differito sono in grado di aggirare le protezioni tradizionali.

Avviamento della campagna: gli aggressori cominciano inviando un'e-mail all'apparenza autentica da un dominio appena creato, utilizzando i protocolli di autenticazione e-mail corretti (SPF, DKIM, DMAR) e una pagina web innocua.

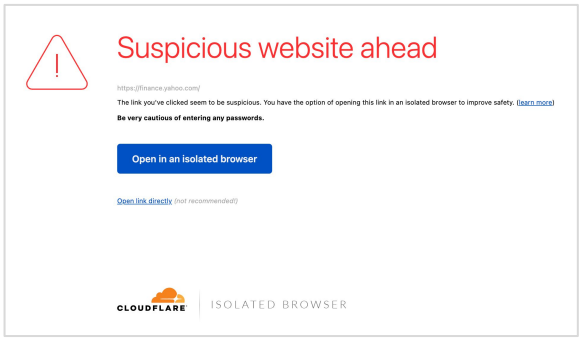
Consegna alle caselle di posta: queste e-mail possono sfuggire ai rilevamenti dei gateway di sicurezza, dei filtri basati su autenticazione o di altri servizi che sfruttano segnali reputazionali e altre tecniche deterministiche.

Trasformazione in link dannoso: una volta che l'e-mail è stata consegnata, l'autore dell'attacco può "girare" il link verso una destinazione dannosa modificando la pagina web da lui controllata. Uno degli esempi più classici è l'indirizzamento a una pagina di login falsa utilizzata per la raccolta fraudolenta delle credenziali.

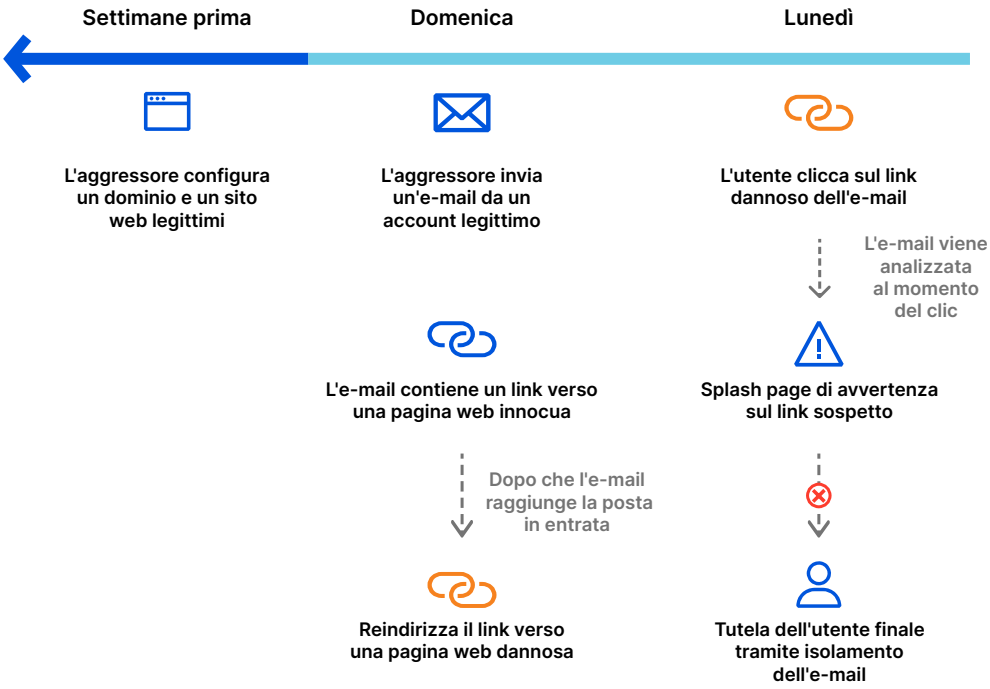
Soluzione: isolare i link sospetti dopo la consegna

L'isolamento dei link inviati tramite e-mail offre un livello di protezione post-consegna indispensabile. Cloudflare analizza tutti i link contenuti in una e-mail e cliccati da un utente. Se il link viene ritenuto rischioso o sospetto, Cloudflare mostra una splash page di avvertimento *(vedere sotto)*, e se l'utente decide comunque di procedere, provvede a isolare la pagina web.

Gli amministratori prevengono l'esecuzione di codice dannoso sui dispositivi locali e possono applicare controlli per la protezione dei dati, come ad esempio limitare il caricamento e lo scaricamento di file, inibire gli input provenienti dalla tastiera dell'utente, o aprire la pagina in modalità di sola lettura.



Sequenza temporale di una campagna di phishing differito



Cloudflare analizza ciascun link al momento del clic

Link sicuro: gli utenti sono reindirizzati verso il sito in modo trasparente.

Link dannoso: agli utenti viene inibita la navigazione.

Link sospetto: agli utenti viene sconsigliata la navigazione sul sito e viene loro mostrata una pagina di avvertenza con il consiglio di visualizzare il link in un browser isolato.

Integrare la CES con Cloudflare Zero Trust

Sicurezza moderna con Zero Trust

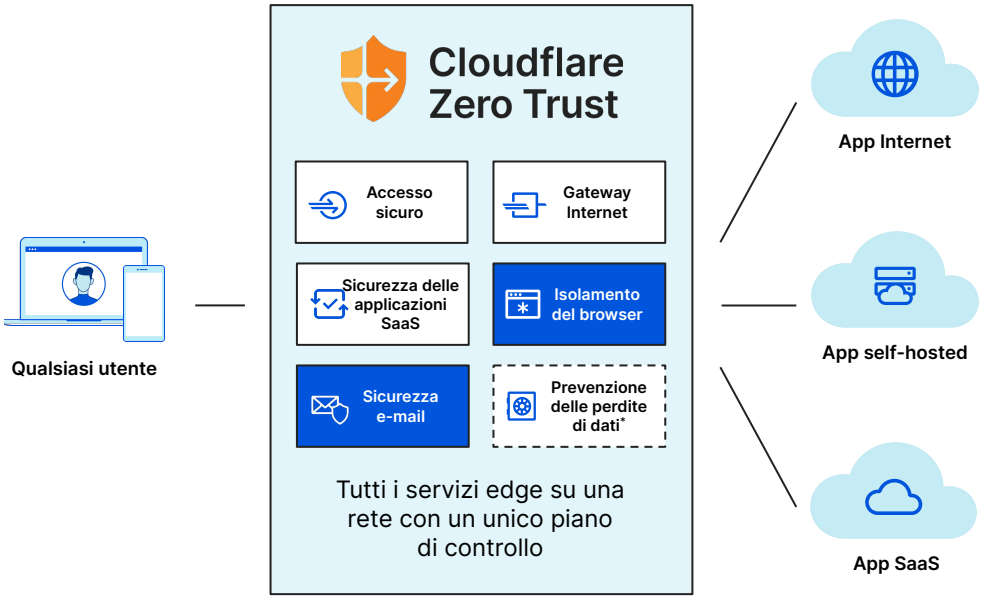
Cloudflare Zero Trust aumenta la visibilità, elimina la complessità e riduce i rischi quando gli utenti, sia in sede che in remoto, si collegano alle applicazioni aziendali e all'Internet pubblico.

Il 1° aprile 2022 Cloudflare ha concluso l'acquisizione di Area 1 Security, con l'obiettivo di potenziare gli strumenti con cui la nostra piattaforma Zero Trust difenderà gli utenti da attacchi di phishing negli ambienti di rete, sul web e nella posta elettronica. Leggi qui per saperne di più.

Sicurezza delle e-mail: potenziamento del modello Zero Trust

La soluzione Cloudflare Area 1 per la sicurezza della posta elettronica migliora il modello Zero Trust eliminando la fiducia implicita dalle e-mail, con l'obiettivo di bloccare preventivamente gli attacchi di phishing e BEC (Business Email Compromise).

Non bisogna mai fidarsi di nessun mittente, nemmeno di quelli interni. Bisogna invece assicurarsi che tutto il traffico degli utenti, e-mail comprese, sia verificato, filtrato, ispezionato e infine isolato dalle minacce provenienti da Internet. La sicurezza della posta elettronica sarà integrata nei nostri servizi Zero Trust e combinata con RBI, CASB e altro ancora.



La **sostituzione delle VPN** semplifica e protegge la connessione di qualsiasi utente a qualsiasi risorsa

Protezione Internet
mantieni i dati sicuri dalle minacce su qualsiasi porta e protocollo

Sicurezza SaaS semplificata
visibilità e controllo delle applicazioni, compresa la posta elettronica

Modernizzazione della sicurezza
maggiore produttività, operazioni semplificate, superficie d'attacco ridotta

*Unisciti alla nostra lista d'attesa per DLP

Cloud Email Security (CES)

- Riduzione del 90% dei tempi di risposta agli eventi di phishing.
- Identificazione precoce dell'infrastruttura dell'aggressore e dei meccanismi di consegna per fermare il phishing nelle prime fasi del ciclo di attacco.
- Rimozione della fiducia implicita dalle e-mail tramite l'analisi dei contenuti, del contesto e delle mappe di comunicazione.
- Eccellente integrazione con Microsoft, Google e altri ambienti per potenziare ulteriormente il livello di sicurezza incorporato.

Remote Browser Isolation (RBI)

- Rischio ridotto di compromissione delle credenziali, dato che i siti rischiosi vengono aperti in modalità di sola lettura e le interazioni dell'utente sono controllate (ad es., input dalla tastiera, copia e incolla, upload/download).
- Esecuzione del codice del browser sulla rete di Cloudflare e isolamento dal codice dannoso dei dispositivi in locale.
- Esperienza dell'utente finale impeccabile e veloce. Invece del solito pixel streaming, disegniamo una replica esatta della pagina da un browser in remoto, ad appena <50 ms dal 95% degli utenti di Internet in tutto il mondo.

Richiedi una valutazione del rischio di phishing oggi stesso **Contattaci**

+44 20 3514 6970 | enterprise@cloudflare.com | www.cloudflare.com/it-it/

REV: PMM-2022JUN

[1] *Gartner Hype Cycle for Network Security, 2021* | GARTNER e HYPE CYCLE sono marchi commerciali registrati e marchi di servizio di Gartner, Inc, e/o delle sue controllate negli Stati Uniti e a livello internazionale, e vengono utilizzati qui previa autorizzazione. Tutti i diritti sono riservati.