Proofpoint Threat Response Auto-Pull

Quarantena automatica delle email dannose dopo la loro consegna

VANTAGGI PRINCIPALI

- Quarantena automatica delle email dannose che aggirano le difese perimetrali
- Riduzione esponenziale del tempo che i team di sicurezza e di messaggistica dedicano all'orchestrazione della sicurezza dell'email e alla risposta agli incidenti
- Classificazione delle minacce con il sistema di intelligence sulle minacce di Proofpoint
- Monitoraggio automatico della casella di posta degli abusi per le minacce
- Quarantena dei messaggi inoltrati a singoli o liste di distribuzione
- Monitoraggio delle campagne di phishing segnalate parzialmente ed eliminazione del tempo dedicato ai messaggi segnalati in modo errato

Proofpoint Threat Response Auto-Pull (TRAP) permette agli amministratori del sistema email e della sicurezza di ottimizzare il processo di risposta agli incidenti. Quando viene rilevata un'email pericolosa, TRAP analizza le email e rimuove automaticamente i messaggi dannosi. Inoltre, mette in quarantena le email indesiderate che hanno raggiunto le caselle di posta in arrivo degli utenti. TRAP è una soluzione potente che permette di ridurre in modo esponenziale il tempo che i team dedicati all'email e alla sicurezza dedicano a ripulire l'email dai messaggi dannosi e indesiderati.

Oltre il 90% delle violazioni dei dati inizia con la ricezione di un'email, il principale vettore d'attacco. Con la costante evoluzione delle minacce propagate via email, le aziende sono esposte a un numero sempre maggiore di messaggi dannosi. Le email dannose possono contenere link di phishing il cui carico dannoso può attivarsi dopo la consegna o utilizzare delle tecniche di elusione che producono falsi negativi e ne determinano la consegna agli utenti. I team dedicati alla sicurezza dell'email hanno spesso il compito di analizzare ed eliminare i messaggi dannosi per ridurre l'esposizione alle minacce e limitare i danni potenziali. Mettere in quarantena un singolo messaggio non è un compito molto laborioso e può richiedere solo 10-15 minuti, ma quando si tratta di decine di messaggi l'attività può diventare noiosa, con ritardi che si accumulano rapidamente.

Condivisione di threat intelligence su più vettori grazie al grafico delle minacce Nexus di Proofpoint

Il grafico delle minacce Nexus di Proofpoint aggrega e confronta i dati delle minacce a livello di email, cloud, rete e social media. Assicura protezione e risposta in tempo reale contro le minacce per tutti i tuoi prodotti Proofpoint. Poiché è integrato nella piattaforma Proofpoint, non è richiesta l'installazione, distribuzione o gestione di alcunché. Entrando a far parte di questa rete e rimanendo un passo avanti rispetto alle minacce in costante evoluzione, godrai dei seguenti vantaggi:

- Threat intelligence in tempo reale proveniente da oltre 115.000 clienti
- Visibilità su più vettori, inclusi email, cloud, rete e social media
- Tracciamento di oltre 100 criminali informatici per comprenderne le motivazioni e le tattiche utilizzate per una maggiore protezione

TRAP sfrutta il grafico delle minacce Nexus per correlare i destinatari con le identità degli utenti, identificando le campagne associate e analizzando gli indirizzi IP e i domini dell'attacco. Quindi, intraprende azioni automatizzate basate su utenti mirati che appartengono a specifici dipartimenti o gruppi con permessi speciali.

Inoltre, se rileviamo un'email che contiene link o allegati dannosi o indirizzi IP sospetti nel sito di un cliente, condivideremo queste informazioni con i nostri clienti in modo che possano proteggersi prima della consegna di un'email. Infine, cancelliamo e mettiamo in quarantena tutti i messaggi che sono stati consegnati alle caselle email degli utenti.

Identificazione e riduzione dei rischi di phishing con CLEAR

Un dipendente informato può rappresentare la tua ultima linea di difesa contro un attacco informatico. Con Closed-Loop Email Analysis and Response (CLEAR), il processo di segnalazione, analisi e neutralizzazione delle email potenzialmente dannose si riduce da giorni a minuti. Alimentato dal sistema di informazioni sulle minacce di Proofpoint, CLEAR blocca gli attacchi attivi con un solo clic. Il tuo team di sicurezza può risparmiare così tempo ed energia mettendo automaticamente in quarantena i messaggi dannosi.

CLEAR è una soluzione completa che combina le funzionalità di PhishAlarm, il tasto di segnalazione delle email, PhishAlarm Analyzer, la soluzione di categorizzazione e assegnazione delle priorità basata sul sistema di informazioni sulle minacce di Proofpoint, e TRAP, che arricchisce i messaggi e automatizza la messa in quarantena dei messaggi dannosi.

I messaggi segnalati vengono inviati a una casella email di segnalazione degli abusi per essere analizzati da CLEAR e vengono monitorati ed elaborati allo stesso modo da TRAP. Vengono poi analizzati utilizzando il sistema di informazioni sulle minacce di Proofpoint e altre fonti di terze parti per stabilire se uno qualsiasi dei contenuti include dei marcatori dannosi. I messaggi vengono automaticamente rimossi dalla casella di posta in arrivo del destinatario.

Gestione delle email al di fuori dei canali abituali

TRAP supporta anche i file CSV e Proofpoint SmartSearch. Puoi caricare i risultati SmartSearch o i file CSV oppure inserire manualmente gli incidenti con le informazioni fondamentali per avviare un'azione di quarantena per una singola email o migliaia di messaggi. In pochi istanti le email che violano le policy o che rappresentano una minaccia per la sicurezza possono essere rimosse dalle caselle email. Una lista di attività indica chi ha letto le email, così come il successo o il fallimento del tentativo di richiamo del messaggio.

Quarantena automatica dei messaggi inoltrati

Le email dannose e indesiderate possono essere inoltrate ad altre persone, dipartimenti o liste di distribuzione. Molti amministratori hanno difficoltà a eliminare questi messaggi dopo la consegna. TRAP risolve il problema grazie a una logica di business integrata e a un sistema di intelligence che rileva quando i messaggi vengono inoltrati o inviati alle liste di distribuzione, e poi rintraccia automaticamente i destinatari per ritrovare e cancellare questi messaggi. In questo modo, risparmi tempo prezioso ed eviti ogni frustrazione.

Processo di ordinamento migliorato

TRAP fornisce agli analisti dei centri SOC un processo di ordinamento migliorato delle email contenenti URL. Gli URL possono essere analizzati in modo sicuro sfruttando la tecnologia Proofpoint Browser Isolation. Questo permette agli analisti di valutare i contenuti dell'URL, prevenendo al contempo i rischi per l'azienda.

APPROFONDISCI

Per maggiori informazioni visita **proofpoint.com/it**.