proofpoint.

SCHEDA TECNICA

Proofpoint Account Takeover

Rileva, analizza e neutralizza i takeover degli account in più fasi

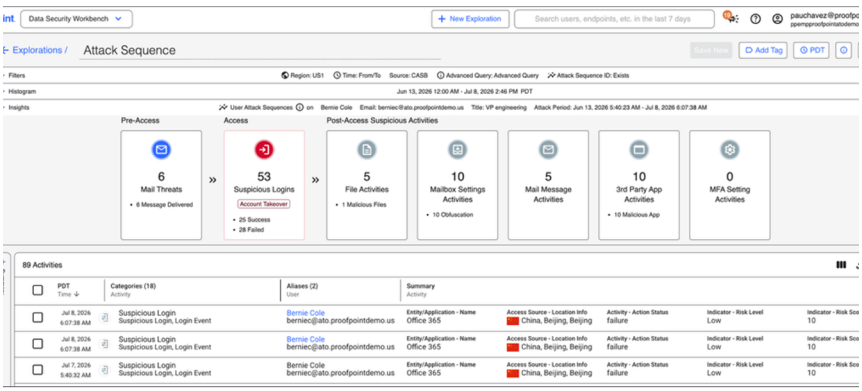
Vantaggi principali

- **Rilevamento delle violazioni dell'account in più fasi con una precisione elevata**
- **Accelerazione delle indagini grazie a una visibilità unificata sull'intero ciclo di vita degli attacchi**
- **Riduzione del tempo di permanenza dei criminali informatici grazie alla risposta e alla correzione automatizzate**
- **Prevenzione di frodi, perdita di dati e interruzioni delle attività derivanti da account compromessi**
- **Rafforzamento della difesa in profondità con Proofpoint Collaboration Security Prime**

Proofpoint Account Takeover Protection aiuta le aziende a rilevare, analizzare e contenere gli account utente compromessi lungo l'intero ciclo di vita dei takeover degli account (ATO), dagli indicatori pre-accesso e di violazione riuscita alle attività dei criminali informatici dopo l'accesso.

Ottimizzato e dalla threat intelligence di Proofpoint Nexus® AI, Proofpoint Account Takeover Protection offre un rilevamento estremamente affidabile delle violazioni dell'account confermate, fornendo al contempo una visibilità completa sul comportamento dei criminali informatici. I team della sicurezza possono comprendere rapidamente la portata di un incidente, accelerare le indagini e contenere le minacce prima che si trasformino in violazioni dell'email aziendale (BEC, Business Email Compromise), furto di dati, spostamenti laterali o altri attacchi con un impatto sulle attività.

Nell'ambito di Proofpoint Collaboration Security Prime, Proofpoint Account Takeover Protection si integra con Threat Protection Workbench e con la Threat Interaction Map per estendere le indagini oltre il singolo account compromesso. Correlando le violazioni dell'identità con le minacce via email, le interazioni con gli utenti e le attività dei criminali informatici, aiuta i team della sicurezza a comprendere meglio la campagna d'attacco. Ciò consente di accelerare le indagini, informare meglio le decisioni di risposta e rafforzare l'applicazione di misure correttive.



1. Figura 1. Ottieni una visibilità completa sull'intero ciclo di vita degli attacchi ATO, dalle attività di pre-accesso alle attività post-accesso.

Rilevamento estremamente affidabile degli attacchi ATO

Ottimizzato da Proofpoint Nexus® AI, Proofpoint Account Takeover Protection offre un rilevamento estremamente affidabile delle violazioni degli account confermate relative a Microsoft 365, Google Workspace e Okta.

Analizzando continuamente le attività degli utenti durante l'intero ciclo di vita del takeover degli account (dagli indicatori pre-accesso al comportamento dei criminali informatici post-accesso), Proofpoint Account Takeover Protection identifica le violazioni confermate con un'elevata affidabilità e assegna le priorità ai rilevamenti in base alla gravità del rischio (critico, elevato o moderato). Ogni rilevamento include gli indicatori comportamentali e le prove che hanno contribuito all'identificazione, aiutando così gli analisti a comprendere rapidamente perché un account è stato identificato come compromesso, assegnare le priorità alle azioni di risposta e intervenire con sicurezza.

Visibilità completa sull'attacco

Una volta confermata la violazione dell'account, Proofpoint Account Takeover Protection offre visibilità completa sulla sequenza dell'attacco, consentendo ai team della sicurezza di comprendere come si è svolto l'attacco e cosa ha fatto il criminale informatico dopo aver ottenuto l'accesso.

Analisi forensi complete rivelano le attività successive all'accesso, tra cui manipolazione delle caselle email, regole di posta in arrivo dannose, uso improprio di OAuth, modifiche dei privilegi, phishing interno, attività email sospette e tecniche di persistenza. Questo aiuta gli analisti a determinare rapidamente la portata, il livello di complessità e l'estensione dell'attacco. Ricostruendo la sequenza d'attacco e mettendo in evidenza gli utenti e le risorse interessati, Proofpoint Account Takeover Protection contribuisce ad accelerare le indagini, supporta decisioni di risposta più informate e migliora l'applicazione di misure correttive.

Risposta automatizzata alle minacce

Proofpoint Account Takeover Protection aiuta le aziende a contenere rapidamente le minacce attive grazie a azioni correttive automatizzate che interrompono l'accesso dei criminali informatici e accelerano il ripristino. Le azioni di risposta includono la modifica forzata della password, il ripristino delle password degli utenti, la revoca delle sessioni utente attive, la rimozione delle regole della casella email dannose, la revoca delle applicazioni OAuth di terze parti non autorizzate e altre misure correttive concepite per eliminare la persistenza dei criminali informatici e ripristinare l'integrità degli account.

Automatizzando le azioni di contenimento critiche, i team della sicurezza possono ridurre il tempo di permanenza dei criminali informatici, limitare gli spostamenti laterali, minimizzare le interruzioni delle attività e accelerare il ripristino dopo la violazione dell'account.

Difesa in profondità con Proofpoint Collaboration Security Prime

Nell'ambito di Proofpoint Collaboration Security Prime, Proofpoint Account Takeover Protection va oltre le violazioni dell'account per offrire una protezione coordinata lungo l'intero ciclo di vita degli attacchi umani. Mentre Proofpoint Account Takeover Protection rileva, analizza e contiene gli account compromessi, Proofpoint Prime rafforza la protezione bloccando le minacce prima che si verifichi la violazione, correlando gli attacchi sui canali di posta e collaborazione, migliorando il comportamento degli utenti attraverso una formazione adattiva e fornendo indagini e una risposta unificate tramite Threat Protection Workbench e la Threat Interaction Map.

Insieme, queste funzionalità supportano una strategia di difesa in profondità che aiuta le aziende a prevenire gli attacchi, mitigare le minacce attive, rafforzare la resilienza degli utenti e migliorare continuamente il loro livello di sicurezza grazie a una piattaforma integrata.

Per saperne di più, visita il sito **proofpoint.com/it**.

proofpoint.