Come Proofpoint blocca il takeover degli account cloud

Prevenire e bloccare il takeover degli account cloud con conseguenze potenzialmente devastanti.

Prodotti

- Proofpoint Cloud App Security Broker
- Proofpoint Zero Trust Network Access
- Proofpoint Browser Isolation
- Proofpoint Email Isolation
- Piattaforma Proofpoint Threat Protection
- Proofpoint Targeted Attack Protection

Vantaggi principali

- Prevenzione dei tentativi di takeover iniziale degli account bloccando gli attacchi di phishing volti a rubare le credenziali d'accesso o attivare il malware
- Rilevamento e blocco di tutti i tentativi di takeover degli account cloud
- Protezione delle tue risorse di valore dalle minacce
- Prevenzione dell'introduzione di minacce nel tuo ambiente a causa della negligenza dei dipendenti
- Raccolta di informazioni preziose per prepararti a contrastare potenziali minacce emergenti

I criminali informatici si stanno adattando alla migrazione delle aziende verso il cloud. A fronte della crescente adozione da parte delle aziende di servizi email in hosting e webmail, applicazioni di produttività cloud come Microsoft 365 e Google Workspace, e ambienti di sviluppo cloud come AWS e Azure, i criminali informatici hanno rapidamente capito che le credenziali di accesso agli account aziendali di base possono portare loro denaro e potere. Ora prendono di mira queste credenziali con un crescente numero di campagne di minacce. I loro sforzi senza sosta sono solo il primo passo della loro missione volta a eseguire bonifici bancari fraudolenti, campagne di spionaggio industriale, furti di dati personali e molto altro ancora.

Come parte di un attacco di takeover degli account cloud (una forma di furto d'identità), i criminali informatici iniziano violando le credenziali d'accesso per infiltrarsi nei sistemi degli utenti. Questi attacchi vengono spesso distribuiti tramite email che contengono malware o incitano gli utenti a rivelare le loro credenziali d'accesso. Una volta ottenuto il controllo di un account, i criminali informatici possono spacciarsi per persone legittime o fidate all'interno dell'azienda dell'utente. Gli infiltrati possono spostarsi lateralmente e causare danni considerevoli. Possono rubare o crittografare dati importanti. Possono anche caricare malware per utilizzare le funzionalità di sincronizzazione e condivisione tra i tuoi endpoint, Microsoft 365 e altri repository cloud. Da lì, possono diffondersi rapidamente nella tua azienda o scaricare file sensibili a fini di estorsione.

Con il crescente utilizzo di sistemi di single sign-on, è sufficiente una credenziale d'accesso compromessa per consentire a un criminale informatico di accedere a numerosi sistemi diversi in azienda.

Il ransomware è uno dei tipi più pericolosi e destabilizzanti di takeover degli account cloud. Questo tipo di attacco informatico causa il fallimento delle aziende, costringe gli ospedali a rifiutare i pazienti e può bloccare l'attività delle amministrazioni pubbliche. Solo l'anno scorso, gli Stati Uniti hanno subito più di 65.000 attacchi di ransomware. Secondo Unit 42, il team di threat intelligence di Palo Alto Networks, i tre quarti di questi attacchi sono stati distribuiti tramite email[1]. Si tratta di una grande preoccupazione per i CISO. Sono diventati addirittura una questione di sicurezza nazionale.

Soluzioni Proofpoint

I criminali informatici utilizzano diverse strategie e vettori di minacce per infiltrarsi nella tua rete. Spesso impiegano approcci ibridi per appropriarsi delle informazioni di cui hanno bisogno. Il loro arsenale può includere attacchi di forza bruta, campagne di social engineering e malware. Hai bisogno di difese complete a più livelli per proteggerti dai loro stratagemmi. Proofpoint offre numerosi prodotti e servizi che possono esserti d'aiuto.

Usate insieme, le soluzioni Proofpoint contribuiscono a proteggerti contro la minaccia del takeover degli account cloud tramite i seguenti metodi:

- Prevenzione del takeover iniziale degli account
- Rilevamento e blocco dei tentativi di takeover degli account cloud
- Protezione delle tue risorse di valore (persone e sistemi) dalle minacce esterne
- Prevenzione dell'introduzione di minacce nel tuo ambiente a causa della negligenza dei dipendenti
- Raccolta di informazioni preziose per prepararti a contrastare potenziali minacce emergenti

Prevenzione, rilevamento e blocco

La piattaforma Proofpoint Threat Protection è una soluzione integrata a più livelli che riduce il rischio di tentativi di takeover degli account cloud. Fornisce rilevamento delle minacce avanzato che impedisce agli utenti di ricevere malware, tentativi di phishing delle credenziali di accesso e altri tipi di attacchi distribuiti tramite email. Inoltre, orchestra la sicurezza per neutralizzare gli account compromessi, riducendo il tempo di risposta agli incidenti e il carico di lavoro del team IT. Gli utenti presi di mira e quelli che si lasciano ingannare dalle minacce di violazione delle credenziali d'accesso possono ricevere brevi sessioni tempestive di formazione e di sensibilizzazione alla sicurezza informatica. Attraverso banner HTML informativi e personalizzabili, la piattaforma può stimolare gli utenti a diffidare di messaggi potenzialmente pericolosi. Può autenticare i messaggi in entrata e in uscita tramite DMARC. Può anche identificare gli account dei fornitori compromessi. Questo approccio a più livelli è il motivo per cui oltre il 60% delle aziende Fortune 1000 si affida alle soluzioni di protezione contro le minacce di Proofpoint per ridurre i rischi legati al takeover degli account cloud.

1 Unit 42, Palo Alto Networks *(https://unit42.paloaltonetworks.com/ransomware-families/)*. "Ransomware Families: 2021 Data to Supplement the Unit 42 Ransomware Threat Report" (Famiglie di ransomware: dati 2021 a completamento del report sui ransomware di Unit 42), luglio 2021.

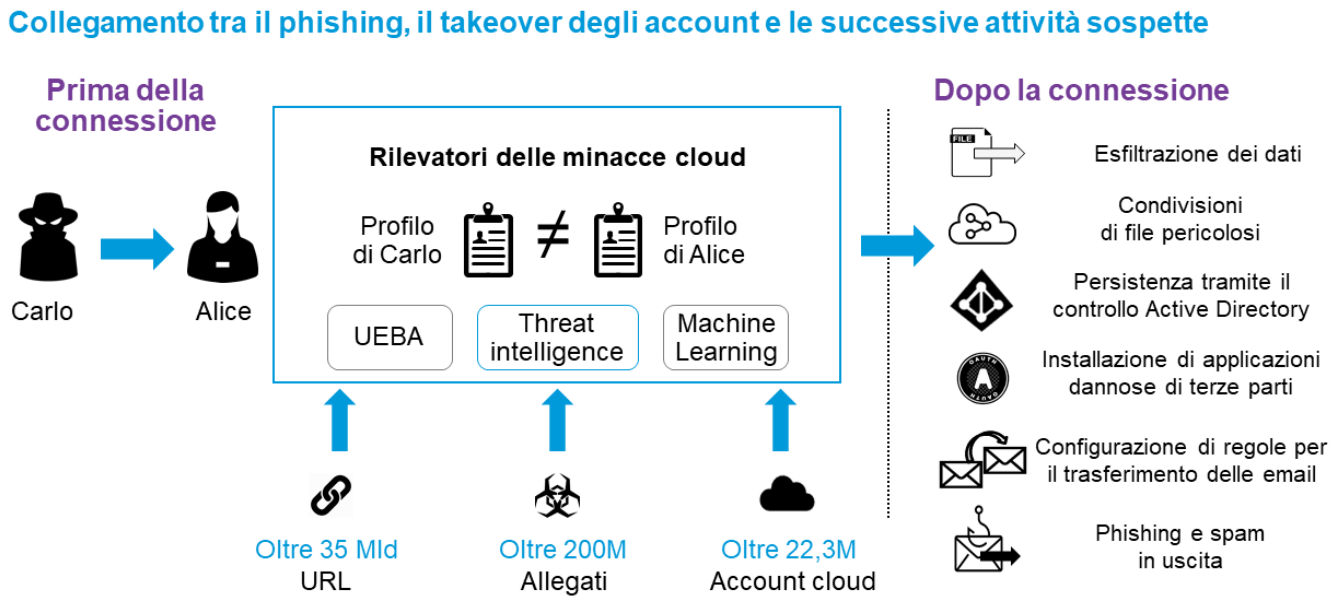

Figura 1. Rilevamento degli account compromessi con Proofpoint CASB

Proofpoint Cloud App Security Broker (CASB) è il caposaldo della nostra difesa contro il takeover degli account cloud. Grazie al suo approccio incentrato sulle persone, protegge i tuoi utenti dalle minacce nel cloud e tutela i tuoi dati sensibili. La sua difesa inizia con la visibilità e i controlli d'accesso. Senza questi elementi fondamentali, è impossibile proteggersi in modo efficace contro gli attacchi di takeover degli account cloud. Proofpoint CASB ti aiuta a implementare misure di sicurezza preventive come i controlli adattivi degli accessi, inclusa un'autenticazione rafforzata. Rileviamo tutti i tentativi di takeover e ti informiamo delle attività dei criminali informatici una volta che hanno ottenuto l'accesso a un account. Proofpoint CASB sospende gli account compromessi e neutralizza tutte le minacce post-takeover. Ciò significa che anche se un criminale informatico ottiene l'accesso a uno dei tuoi account, Proofpoint CASB può impedirgli di utilizzarlo per trasferire email o delegare, esfiltrare i dati o inviare email di phishing o di spam.

Alternativa Zero Trust alla VPN

La forza lavoro mobile e in telelavoro sono in aumento in tutto il mondo. Con la crescente migrazione delle applicazioni verso il cloud, il perimetro della rete sta scomparendo. Molte aziende iniziano solo ora ad affrontare le nuove sfide in tema di sicurezza che accompagnano questo nuovo paradigma. Di conseguenza, scoprono solo ora che i loro sistemi di sicurezza di vecchia generazione, che si basano su connettività e stack di sicurezza incentrati sui siti, non sono in grado di proteggerle.

Proofpoint Zero Trust Network Access (ZTNA) permette ai tuoi utenti di accedere in tutta sicurezza alle applicazioni ospitate nei data center e nel cloud. Questa alternativa, incentrata sulle persone, alla VPN microsegmenta le autorizzazioni, riducendo in modo considerevole la superficie d'attacco di una rete. Il suo perimetro software-defined fornisce un accesso alla rete Zero Trust.

Isolamento del browser e dell'email

I team IT e della sicurezza devono garantire un ambiente operativo sicuro ai loro utenti. Ma devono anche permettere loro di effettuare ricerche e collaborare in modo efficace con i membri del loro team. Non è un compito facile, poiché due dei principali vettori degli attacchi di takeover degli account cloud sono gli stessi strumenti utilizzati per le ricerche e la comunicazione, ovvero il web e l'email. Proofpoint offre due soluzioni che permettono ai tuoi team di combinare il meglio dei due mondi. Queste soluzioni forniscono esperienze di navigazione e comunicazione fluide, mentre proteggono gli utenti dalla violazione degli account cloud.

Proofpoint Browser Isolation ti protegge dalla violazione degli account cloud consentendo agli utenti di navigare sul web e impedendogli di fare clic inavvertitamente su link di phishing e scaricare file dannosi sui dispositivi della tua azienda.

Proofpoint Email Isolation estende le funzionalità di Proofpoint Targeted Attack Protection (TAP). Isola i clic sugli URL all'interno delle email aziendali in base al livello di rischio. Può inoltre mettere in evidenza gli utenti più attaccati e determinare gli URL più pericolosi che arrivano nelle caselle in entrata dei tuoi collaboratori.

Informazioni aggiornate

Una comprensione ampia e profonda del panorama delle minacce è essenziale per prepararti a contrastare le minacce future. Il grafico delle minacce Nexus di Proofpoint ti offre threat intelligence completa di cui hai bisogno per proteggerti contro le minacce informatiche attuali più temibili. Combina in tempo reale migliaia di miliardi di punti dati su molteplici vettori delle minacce in tutto il mondo, con l'intelligenza artificiale avanzata, il machine learning e un gruppo globale di esperti di sicurezza informatica.

PER SAPERNE DI PIÙ

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

INFORMAZIONI SU PROOFPOINT

Proofpoint è un'azienda leader nella cybersecurity e nella conformità, che protegge dai rischi il patrimonio più importante di un'azienda: le persone. Con una suite integrata di soluzioni basate su cloud, Proofpoint aiuta le aziende di tutto il mondo a bloccare le minacce mirate, a salvaguardare i propri dati e a proteggere gli utenti dagli attacchi IT. Aziende di ogni dimensione, tra cui più della metà delle Fortune 1000, si affidano alle soluzioni di sicurezza e di conformità incentrate sulle persone di Proofpoint per mitigare i rischi di sicurezza veicolati via email, cloud, social media e web. Per ulteriori informazioni: **www.proofpoint.com/it**.