Proofpoint TAP Account Takeover

Detecte e remedeie contas comprometidas em seus ambientes de e-mail e de nuvem

Principais vantagens

- Utilize inteligência sobre ameaças e análise comportamental para detectar contas de e-mail comprometidas
- Proteja-se contra desvio de autenticação por múltiplos fatores
- Acelere e unifique investigações de ameaças de e-mail em ataques de sequestro de contas e atividades de nuvem pós-comprometimento
- Remedeie contas, mudanças maliciosas em regras de caixa de entrada, manipulações de aplicativos de terceiros e vazamento de dados em ambientes de e-mail e de nuvem

O Proofpoint TAP Account Takeover estende o poder do Proofpoint Targeted Attack Protection (TAP) detectando contas comprometidas e protegendo os seus ambientes de e-mail e de nuvem. Ele defende contra phishing, ataques de força bruta, comprometimento de e-mail corporativo (BEC), malware, vazamento de dados e acesso persistente de atacantes.

O TAP Account Takeover utiliza inteligência artificial (IA), bem como inteligência sobre ameaças correlacionada e análise comportamental, para detectar atividades suspeitas em toda a cadeia de ataque a contas de e-mail. Ele permite que você veja quais tipos de ameaças visam contas. Se um atacante acessa uma conta, você pode tomar providências para protegê-la. Ele também remedeia automaticamente mudanças maliciosas em regras de caixa de entrada, aplicativos de terceiros sujeitos a abuso e compartilhamento excessivo de arquivos confidenciais. O TAP Account Takeover oferece a você um relatório detalhado de logins suspeitos, de sequestros de contas, de usuários afetados e das ações executadas para remediar as ameaças. Esses insights ajudam você a investigar rapidamente atividades maliciosas, responder a ameaças e limitar o risco.

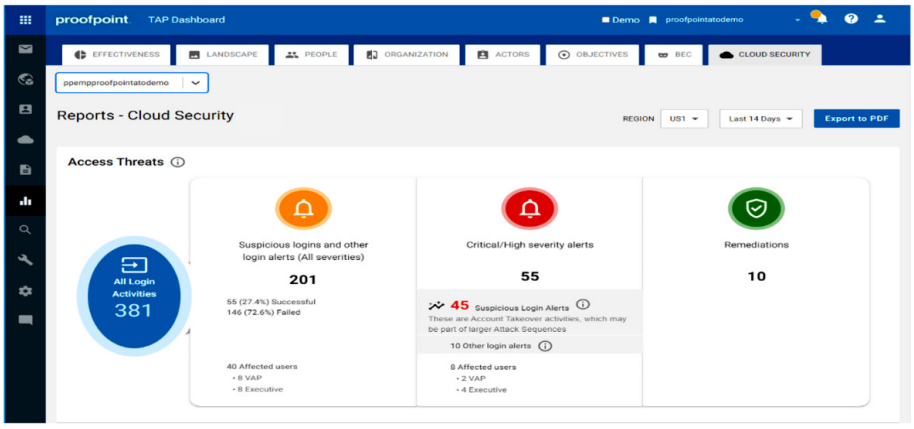

Figura 1. A Proofpoint monitora toda atividade de login. E o relatório Access Threats ajuda você a visualizar logins suspeitos e remediações automatizadas.

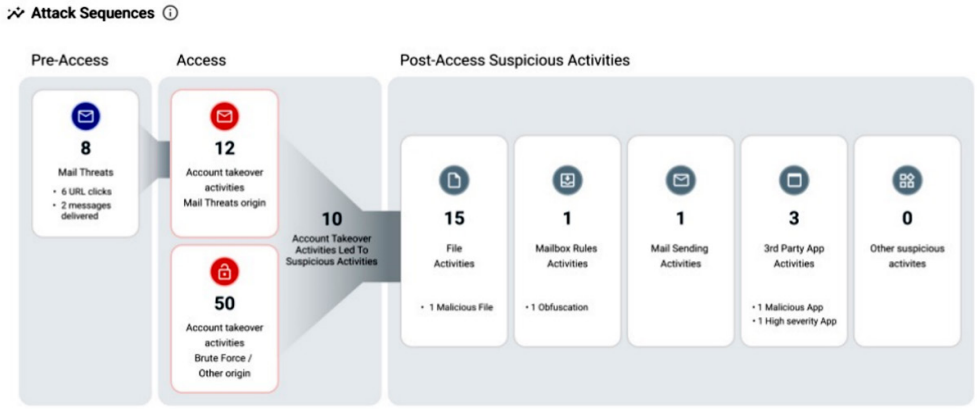

Figura 2. O relatório Attack Sequence mostra ameaças de acesso em toda a cadeia de ataque.

Visibilidade

O TAP Account Takeover revela contas comprometidas e atividades pós-acesso suspeitas nos seus ambientes de e-mail e de nuvem. Ele correlaciona inteligência sobre ameaças com inteligência artificial/autoaprendizagem e análise comportamental para detectar eventos maliciosos. Essa abordagem oferece a você total visibilidade. Você pode ver de quem são as contas comprometidas e como elas foram comprometidas. Isso também reduz alertas de falsos positivos. Dessa forma, você pode ter mais confiança nos vereditos de sequestro de contas.

O TAP Account Takeover emite alertas automatizados no dashboard do TAP quando uma conta é comprometida. Uma cronologia da sequência de ataque mostra uma visão geral do risco de sequestro de conta. Ele também mostra as contas afetadas e atividades maliciosas, tanto antes quanto depois do acesso. Ele pode dizer como os atacantes acessaram a conta e o que eles fizeram após entrar na conta. Ele pode informar sobre suas atividades em arquivos, por exemplo. Ele também pode identificar regras de caixa de entrada alteradas que ajudem a ocultar sua presença no seu sistema, suas atividades de envio de e-mail e quando manipulam aplicativos de terceiros.

Acelere as investigações

Com o TAP Account Takeover, os seus analistas de segurança podem compreender rapidamente o que aconteceu e como limitar o risco. Informações sobre sequestro de contas são integradas com o processo e o sistema de investigação do TAP. Você obtém a mesma inteligência sobre ameaças e os mesmos insights centrados em pessoas, correlacionados e fornecidos no dashboard do TAP. Uma visão cronológica de atividades oferece insights sobre contas que foram sequestradas. Todos os dados são clicáveis. Isso permite aos analistas detalhar e investigar cada incidente após o comprometimento da conta. Você pode ver se o usuário é uma pessoa muito atacada (Very Attacked Person™ ou VAP). Você também pode ver como a conta foi comprometida, bem como a localização do atacante. E pode saber se outros usuários foram atingidos por ameaças semelhantes.

Resposta automatizada

O TAP Account Takeover detecta e remedeia automaticamente alterações feitas por atacantes em regras de caixa de entrada. Os atacantes frequentemente alteram essas regras para ocultar sua identidade antes de iniciarem um ataque de BEC. O TAP Account Takeover também detecta e revoga aplicativos de terceiros que sofreram abuso e que podem ajudar os atacantes a controlar uma conta sem serem detectados. Essas ações ajudam a reduzir o tempo de permanência dos atacantes na contas. Elas podem limitar os danos à sua organização e reduzir a carga de trabalho da sua equipe. Se uma investigação revelar outras atividades maliciosas, você pode executar ações para remediar as contas que foram sequestradas. Você pode limitar a perda de dados. E pode excluir arquivos maliciosos que os atacantes tenham inserido no seu ambiente.

SAIBA MAIS

Para obter mais informações, visite **proofpoint.com/br**.