Proofpoint Identity Protection

하이브리드 기업 전반에서 계정 탈취에 대한 심층 방어 접근 방식 채택

주요 이점

- 전체 공격 사슬(attack chain)에서 계정 탈취로부터 보호
- 조직의 ID 인프라에서 ID 취약성 검색, 우선순위 지정 및 자동 수정
- 위협 인텔리전스와 행동 분석을 적용하여 손상된 계정 탐지
- 공격자가 조직의 중요한 IT 자산에 도달하기 전에 공격자의 수평 이동 시도 차단
- 손상된 계정을 자동으로 격리하고, 악의적인 메일함 규칙 변경 및 타사 앱 조작을 되돌리고, 데이터 유출 차단

위협 행위자가 사용자의 계정 및 자격 증명을 손상한 후 해당 사용자의 디지털 ID를 제어하게 됩니다. 성공한 경우 훨씬 더 많은 사용자 계정을 익스플로잇하려고 시도합니다. 또한 권한을 높이고 클라우드 계정, 플랫폼, 응용 프로그램 및 네트워크 엔드포인트에서 측면으로 이동하려고 합니다. 그런 다음 피싱 및 랜섬웨어 공격을 시작하고, 민감한 데이터를 유출하고, 지속적으로 액세스할 수 있습니다. 하지만 Proofpoint Identity Protection을 사용하면 전체 공격 사슬(attack chain)을 포괄하는 견고한 심층 방어 접근 방식에 따라 계정 탈취로부터 보호할 수 있습니다.

계정 탈취 문제는 광범위한 관심사입니다. 연구에 따르면 위협 행위자는 2023년에 모든 조직의 98%를 목표로 삼았으며 그중 62%가 손상을 경험했다고 합니다. 또한 손상된 조직의 약 1/3이 다단계 인증(MFA) 솔루션을 도입했다고 합니다. 안타깝게도 MFA는 계정 탈취 방어를 위한 묘책이 아닙니다. 그동안 공격자는 ID에 집중하도록 전술 및 기술을 표준화했습니다. Verizon DBIR 보고서에 따르면 성공한 공격의 94%에서 Active Directory 및 권한 있는 ID를 사용하여 권한을 높임으로써 대상 조직을 심층적으로 분석할 수 있었다고 합니다.

또한 Proofpoint 연구에 따르면 기업 엔드포인트(클라이언트 및 서버) 6곳 중 1곳에서 ID 취약성을 포함하고 있다고 합니다. 이러한 취약성은 쉽게 악용될 수 있으며, 공격자는 관리자 권한을 얻기 위해 이 취약성을 목표로 삼습니다. 많은 취약성이 정상적인 비즈니스 및 IT 운영 절차에서 발생합니다. 예를 들어 브라우저, 클라이언트 측 유틸리티와 같은 사용자 앱에서 사용자 이름과 암호를 주기적으로 캐싱하며 이는

이 솔루션 세트는 Proofpoint의 통합 인간 중심 보안 플랫폼의 일부이며 사람에게서 비롯되는 위험 중 네 가지 주요 영역을 완화합니다.

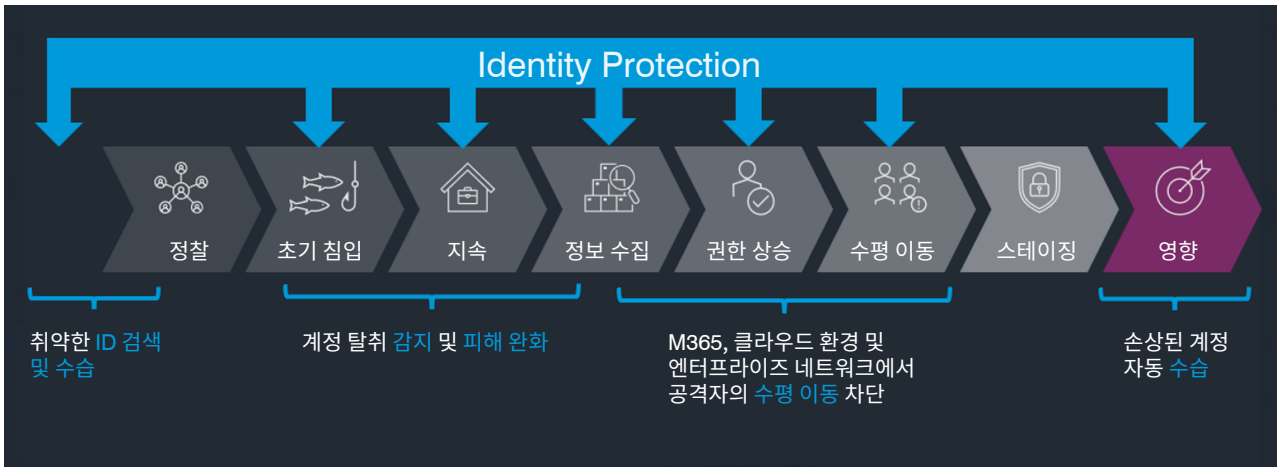

그림 1. Identity Protection은 전체 공격 사슬(attack chain)을 포괄하는 여러 보안 제어를 제공합니다.

쉽게 추출될 수 있습니다. 원격 지원 세션 후에 도메인 관리자 자격 증명이 시스템 메모리에 캐싱되는 경우도 있습니다. 잘못된 Active Directory 구성으로 인해 비IT 사용자에게 관리자 권한이 잘못 부여되는 경우도 많습니다.

완벽한 단일 보안 시스템은 없습니다. 따라서 Identity Protection에서는 여러 제어 계층을 제공합니다. 여러 제어 계층을 사용하면 계정 탈취로부터 효율적으로 방어하고 IT 시스템을 보호할 수 있습니다. 이 심층 방어 접근 방식은 클라우드 자산과 온프레미스 자산에 모두 의존하는 오늘날의 하이브리드 기업에서 더욱 의미가 있습니다. Active Directory, PAM, 클라우드 기반 ID 공급자 서비스와 같은 ID 관리 시스템이 점점 표적이 되고 있습니다.

검색, 우선순위 지정, 수정

Identity Protection은 계정 탈취 공격 이전에 취약한 ID를 검색하여 우선순위를 지정하고 수정합니다.

- **검색 -** Active Directory, Entra ID, AWS Identity Center, PAM, 엔드포인트 및 기타 ID 리포지토리에서 취약한 ID를 지속적으로 검색합니다.
- **우선순위 지정** - 위험을 기준으로 ID 취약성의 우선순위를 지정하고 조직의 ID 핵심 자산을 기준으로 사용 가능한 공격 경로를 매핑합니다.
- **수정 -** 대시보드에서 직접 자동 수정을 사용하도록 설정하고 보안 정책에 부합하는 예외 규칙을 설정할 수 있습니다.

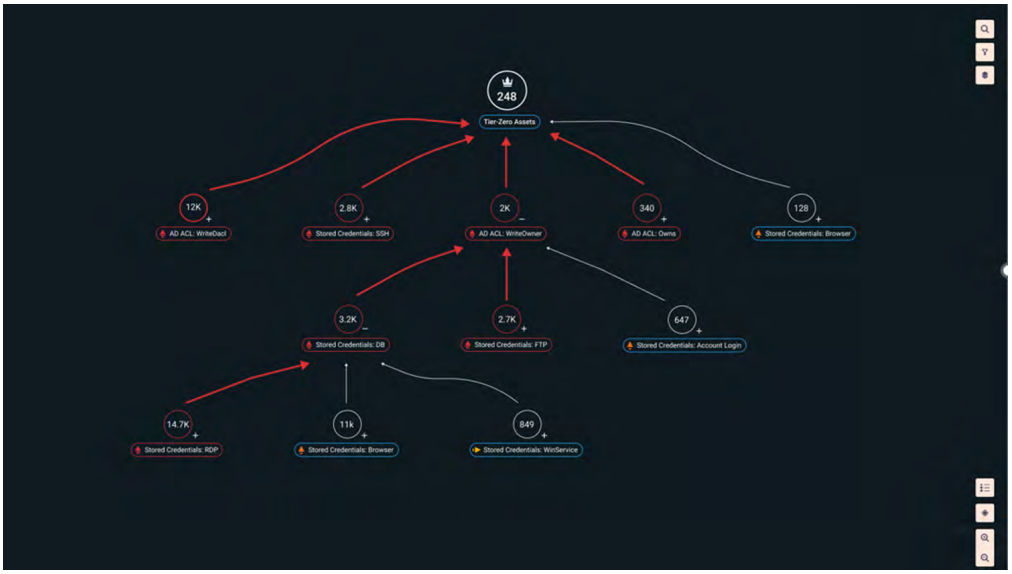

그림 2. 공격 경로 관리 보기에 조직의 묘책에 대한 익스플로잇 경로가 표시됩니다.

그림 3. 공격 시퀀스 보고서에 공격 사슬(attack chain) 전반의 위협이 표시됩니다.

손상된 계정 감지

Identity Protection은 Microsoft 365 및 Google Workspace 이메일 계정에서 손상된 계정을 찾습니다. 이러한 계정을 확인하지 않으면 전체 클라우드 응용 프로그램 환경이 광범위하게 손상될 수 있습니다. 이 솔루션은 Proofpoint Targeted Attack Protection의 위협 인텔리전스 및 데이터를 인공 지능(AI) 및 행동 분석과 상호 연결하여 계정 탈취를 나타낼 수 있는 악의적인 이벤트를 탐지합니다. 이 접근 방식은 완전한 가시성을 제공합니다. 손상된 계정과 위협 행위자가 수행한 작업을 확인할 수 있습니다. 또한 정확도 높은 판단을 내립니다.

Identity Protection은 위협 행위자의 활동에 대한 공격 시퀀스 타임라인을 표시합니다. 여기서 공격자가 계정에 액세스한 방법과 로그인하여 제어권을 확보한 후 수행한 작업을 알 수 있으므로 조사에 도움이 됩니다.

활성 위협 감지 및 대응

Identity Protection을 사용하면 공격자의 사기 공격 후 활동을 감지하여 대응할 수 있습니다. 이를 위해 기업 전반에서 에이전트 없는 위장 기법을 배포합니다. 이러한 위장 기법은 진짜처럼 보입니다. 하지만 실제로는 이메일, 캐싱된 자격 증명, 부신 RDP 세션과 같은 기만적인 리소스입니다. 위협 행위자가 이러한 리소스에 연결하면 권한 상승 및 측면 이동 시도를 감지할 수 있습니다. 걸려들면 위장 기법은 포렌식 데이터를 수집하여 활성 위협에 대한 대응을 안내합니다.

활동 타임라인 보기에서는 탈취된 계정에 대한 인사이트를 제공합니다. 모든 데이터를 클릭할 수 있습니다. 이를 통해 분석가들이 사기 공격 후 각 사고를 분석하고 조사할 수 있습니다. 공격자가 메일함 규칙을 변경하면 Identity Protection에서 자동으로 감지하여 수습 조치를 취합니다. 공격자가 BEC 또는 다른 유형의 공격을 준비하기 전에 활동을 숨기기 위해 이러한 규칙을 변경하는 경우가 있습니다. 또한 Identity Protection에서는 손상된 계정과 신뢰 관계에 있는 악용된 타사 클라우드 앱을 감지한 후 액세스 권한을 취소합니다. 공격자가 영구 액세스 권한을 얻기 위해 MFA 설정을 조작한 경우 Identity Protection에서 원래 설정을 복원합니다. 이러한 대응은 공격자의 체류 시간을 줄이는 데 도움이 됩니다. 사고의 잠재적 비즈니스 영향을 최소화하는 데에도 도움이 됩니다. 공격자가 사용자 환경에서 데이터를 유출하려고 시도하면 Identity Protection에서 이를 차단합니다.

자세히 알아보기

자세한 내용은 **proofpoint.com**을 참조하십시오.