집중 분석

계정 탈취 킬 체인

사이버 킬 체인을 발생 즉시
파악할 수 있습니까?

계정 탈취 킬 체인 사이버 공격 단계를 살펴보고
이를 방어하는 방법을 알아보세요.

1

정찰

예상되는 결과
데이터 유출, 인증정보 도난

방어하는 방법

구현:

- 웹 애플리케이션 방화벽
- 암호화
- 알려진 유출에 대한 인증정보 확인
- 강력한 보안 정책

예상되는 공격자 반응

공격자는 다른 사이트를 공격하거나 인증정보를 구매합니다. 다크 웹에는 수십억 개의 인증정보가 존재합니다.

2

무기화

예상되는 결과
실패한 로그인 시도 소폭 증가

방어하는 방법

확인:

- 정상 사용자가 로그인했는지 확인
- 봇 관리 소프트웨어가 작동 중인지 확인
- MFA가 로그인 엔드포인트를 보호하고 있는지 확인

예상되는 공격자 반응

봇이 탐지될 경우 공격자는 봇 소프트웨어를 조정할 수 있습니다.

3

전송

예상되는 결과
트래픽 급증, 로그인 요청 폭증

방어하는 방법

검증:

- 전송률 제어
- MFA
- 사용자의 비정상 행동
- 봇 관리 소프트웨어의 고급 탐지 기능

예상되는 공격자 반응

공격이 멈추고 킬 체인이 중단됩니다. 매우 정교한 봇 공격은 일시적으로 탐지를 피할 수 있습니다.

4

악용

예상되는 결과
실제 사용자의 단일 요청, 로그인 수의 소폭 증가

방어하는 방법

검사:

- 사용자의 비정상 행동

예상되는 공격자 반응

공격자는 대규모로 공격을 일으킬 수 없습니다. 범죄자들은 소셜 네트워크에서 계정 소유자를 찾아 개별 공격 시도를 할 수 있습니다.

5

실행

예상되는 결과
계정을 탈취당했다는 고객의 신고 급증

방어하는 방법

모니터링:

- 사용자가 로그아웃할 때까지 지속적으로 사용자 리스크 모니터링

예상되는 공격자 반응

계정 보안 소프트웨어가 공격 시도를 차단하고 공격자가 공격을 포기합니다.

Akamai가 계정 탈취를 방어하는 방법을 확인하세요.

자세히 보기

Akamai

| 지원 | 2021년 6월 발행