멀티 채널 피싱으로부터 인력 보호

받은 편지함 이상으로 확대되는 계층화된 보호

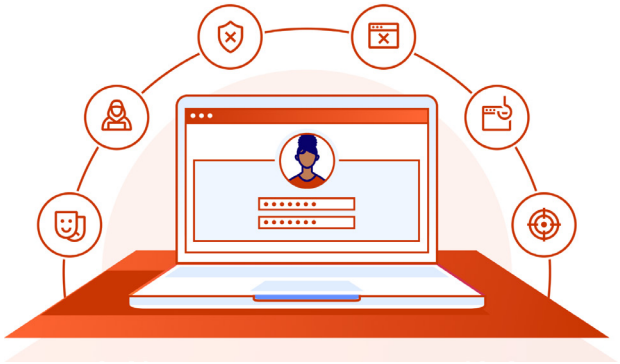
개요

더 이상 이메일에만 한정되지 않는 피싱 공격

피싱 캠페인에 가장 널리 사용되고 효과적인 전달 메커니즘은 이메일이지만, 공격자는 일상 커뮤니케이션 및 협업에 사용되는 다양한 채널(즉, 애플리케이션)을 통해 사용자를 겨냥하고 악용하기 위한 영리한 전술을 점점 더 많이 사용하고 있습니다. 이러한 공격은 교묘하게 난독화된 링크를 이용하여 사용자를 속이고, 악성 콘텐츠 및 안전하지 않은 환경으로 대상을 전환시키는 경우가 많습니다.

더 많은 채널 = 더 많은 직원 악용 방법

공격자는 이메일 내부 및 다른 협업 애플리케이션에 있는 속임수 링크를 통해 직원을 겨냥하여 기존 감지 방식을 우회하는 동시에 진위 여부에 대한 인식을 높이는 방식으로 사용자의 참여를 유도할 수 있습니다. 따라서 직원이 악성 웹 콘텐츠를 클릭하거나, 자격 증명을 공개하거나, 중요한 정보를 유출할 가능성이 높아집니다. 받은 편지함을 통해 공격이 발생하는 경우에는 이메일 보안이 도움이 될 수 있지만, 이러한 공격이 다른 애플리케이션으로 확산되면 공격을 차단하기 위해 보다 광범위한 보안 솔루션이 필요합니다.



과제

기존 이메일 필터링을 우회하는 멀티 채널 위협

멀티 채널 공격은 복잡한 링크 난독화 및 다양한 협업 애플리케이션을 활용하여 사용자가 악의적인 콘텐츠를 클릭하거나 중요한 정보를 유출하도록 유도합니다. 이러한 유형의 공격을 차단하기 어려운 이유는 다음과 같습니다.

- **링크 난독화**(URL 리디렉션/축약기)
- **이미지 기반 URL**(QR 코드)
- **지연 공격**(전달 후 활성화)
- **업무 애플리케이션 전반에서의** 분산된 참여

89%

멀티 채널 위협을 우려하고 있는 보안 의사 결정권자의 비율[1]

#1

감지량 기준으로 상위에 해당하는 피싱 위협인 악의적인 링크[2]

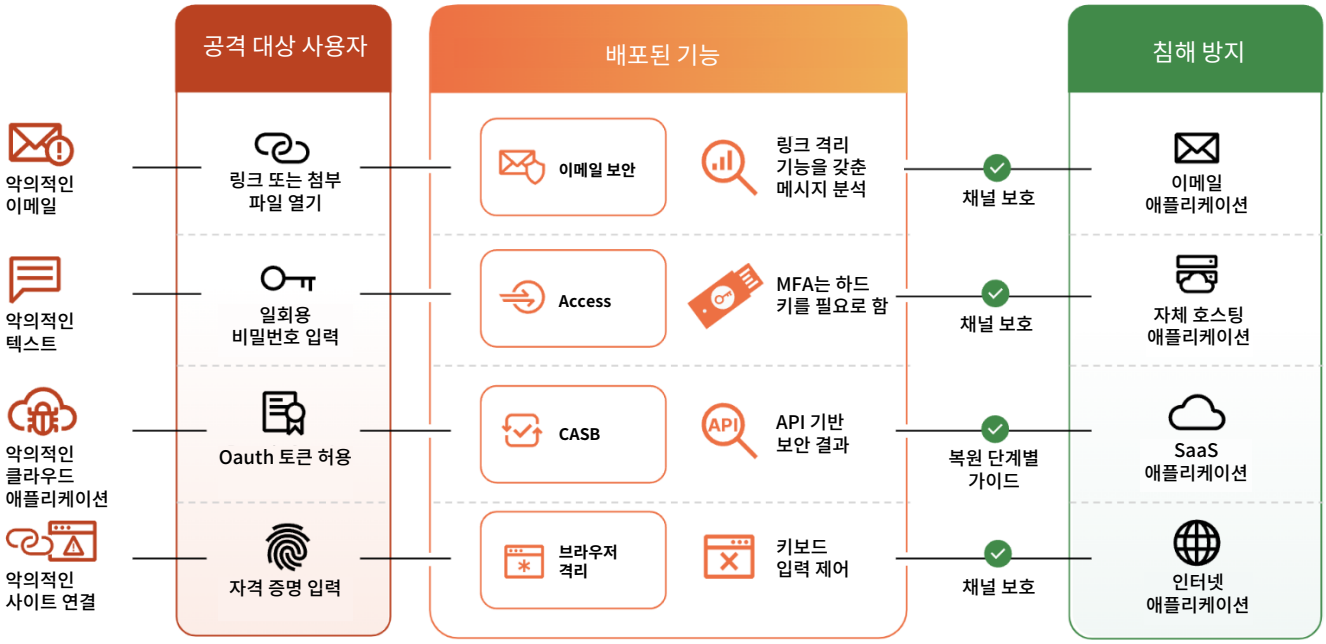
81%

지난 12개월 동안 멀티 채널 공격을 경험한 조직의 비율[1]

솔루션

모든 피싱 노출 지점에서의 통합 보안

멀티 채널 공격을 차단하려면 직원의 워크플로우 및 애플리케이션 내부 상호 작용에 존재하는 모든 범위의 취약점에 대응할 수 있는 플랫폼이 필요합니다. 이것이 바로 Cloudflare에서 직원 및 애플리케이션 전반을 원활하게 보호하는 데 중점을 둔 가장 완벽한 피싱 솔루션을 제공하는 이유입니다. 조직에서는 Cloudflare One 플랫폼을 활용하여 기본적으로 통합된 ES(이메일 보안) + Zero Trust 서비스를 활용하여 이메일, 자체 호스팅 애플리케이션, SaaS 애플리케이션, 인터넷 애플리케이션에 계층화된 보호 기능을 배포하여 사기성 결제와 데이터 유출을 차단하는 심층 방어를 제공할 수 있습니다.



이메일 기반 위협을 선제적으로 차단

AI/ML 기반 콘텐츠 분석을 통해 비즈니스 이메일 손상(BEC), 맬웨어, 이메일에서 발생한 기타 위협 등을 감지하여 자동으로 보호합니다.

자격 증명 도난으로 발생하는 유출 방지

자격 증명이 도난되거나 손상된 경우 최후의 방어선 역할을 수행하는 조건부 액세스 + 하드 키 요건으로 유출을 방지합니다.

우회된 링크 기반 공격의 차단 및 격리

널리 사용되는 메시징 애플리케이션을 통해 포착하기 어렵도록 교묘하게 난독화된 링크를 사용하여 직원을 유도하는 표적 공격으로부터 사용자를 보호합니다.

이메일 기반 위협 차단(ES)

가장 많이 사용되면서 가장 악용되기 쉬운 비즈니스 애플리케이션이 이메일이라는 점을 생각하면, 이메일을 통해 사용자들의 믿음을 악의적으로 이용하려는 피싱 공격으로부터 사용자를 보호하는 일이 그 어느 때보다 중요해졌습니다. 조직에서는 현재 사용하고 있는 이메일 보호 기능을 Cloudflare로 강화하거나 교체하여 임베딩된 이메일 링크, 첨부 파일, 손상되거나 가장된 계정을 이용하여 중요한 정보를 훔치고 금융 사기를 시도하는 정교한 피싱 공격을 자동으로 완화할 수 있습니다.

Cloudflare의 경량 클라우드 네이티브 솔루션은 단 몇 분이면 배포하여 Microsoft 및 Google에서 제공하는 기본 이메일 기능을 보완할 수 있습니다. Cloudflare에서는 강화된 자동화 및 최소한의 조정으로 최적의 결과를 이끌어내므로 지속적인 관리에 필요한 시간과 노력이 크게 줄어듭니다.

비즈니스 이메일 손상(BEC)
AI/ML 기반 콘텐츠 분석은 모든 메시지를 해체하여 대화 내역, 작성 패턴, 감정, 기타 변수를 평가하여 발신자의 진위 여부를 결정합니다.

랜섬웨어 및 악의적 첨부 파일
페이로드에 대한 ML 감지 모델, 무서명 감지, 컴퓨터 비전, 원격 추출, 기타 형태의 분석은 암호화되거나 암호화되지 않은 악의적인 페이로드를 식별하는 데 사용됩니다.

악의적인 이메일 링크
복잡한 URL을 해체하고 세부 분석하는 고급 기술을 적응형 링크 격리와 결합하여 직원에게 안전하고 원활한 웹 경험을 보장합니다.

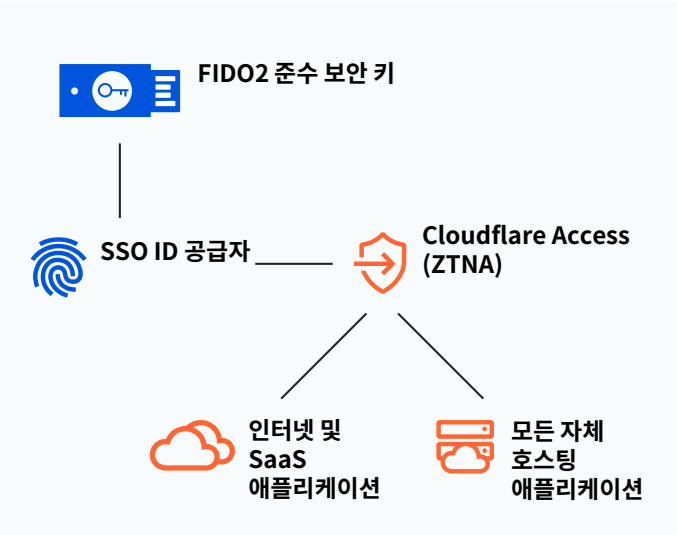
OAuth 피싱 공격 완화(CASB)

OAuth 피싱은 합법적인 ID 공급자와 권한 부여 워크플로우를 이용하여 사용자가 악성 애플리케이션에 권한을 부여하도록 유도합니다. Cloudflare One 플랫폼은 해당 애플리케이션을 감지하는 기능을 제공하며, 이러한 위협을 빠르게 완화할 수 있는 복원 가이드를 제공합니다.

손상된 자격 증명으로 발생하는 유출 방지(ZTNA)

많은 조직에서는 직원의 자격 증명이 잘못된 사람의 손에 넘어가지 않도록 광범위한 예방 조치를 시행하고 있지만, 그러한 예방 조치가 100% 완벽하지는 않다는 것이 뼈아픈 진실입니다. 운이 따르지 않는 경우 자격 증명이 도난되거나 자신도 모르는 사이에 유출되기 때문에, 전면적인 유출을 방지하기 위한 최후의 방어선이 반드시 있어야 합니다.

Cloudflare Access는 자체 호스팅 또는 비웹 리소스를 비롯하여 모든 리소스에서 집계 계층 역할을 수행하므로, 조직에서는 피싱 방지 MFA를 위해 FIDO2 준수 인증을 일관되게 시행할 수 있게 됩니다. 따라서 직원의 자격 증명이 손상되더라도 조직에서는 자사 데이터를 계속 보호할 수 있게 됩니다.



링크 기반 공격 격리(ES + RBI + SWG)

링크 기반 공격은 자격 증명을 도용하고, 맬웨어/랜섬웨어를 로딩하며, 중요한 정보를 추출하기 위해 자주 사용되는 방법이 되었습니다. 이메일, 채팅, SMS, 소셜 및 클라우드 드라이브의 조합으로 이러한 링크를 전달하면 표적 피싱 공격으로부터 직원과 데이터를 모두 보호하기 위한 프로세스가 더욱 복잡해집니다.

Cloudflare 브라우저 격리는 사용자의 로컬 장치가 아닌 당사의 글로벌 클라우드 네트워크에서 모든 웹 코드를 원격으로 렌더링하여 링크 기반 피싱 공격을 해결합니다. 이는 맬웨어와 브라우저 zero-day를 완화하는 동시에 사용자 작업을 미세하게 조정하여(예: 키보드 입력 비활성화) 자격 증명 수집 및 데이터 유출을 방지합니다.

직원의 업무 속도 저하 없이 피싱 위험 제거

Cloudflare에서는 고유한 네트워크 벡터 렌더링(NVR) 기술을 이용하여 구축된 차세대 브라우저 격리 기능을 통합함으로써 잠재적인 악성 링크를 격리하는, 원활하고 안전하며 확장 가능한 솔루션을 제공할 수 있습니다. 대역폭을 많이 사용하는 기술과 달리 NVR은 안전한 그리기 명령을 장치로 스트리밍합니다. 따라서 최종 사용자 경험에 영향을 미치지 않고 악의적인 웹 콘텐츠의 위험을 제거할 수 있습니다. NVR 및 Cloudflare의 대기 시간이 짧은 네트워크 덕분에, 조직은 멀티 채널 위협을 격리하는 동시에 직원에게 중단 없는 생산성을 보장할 수 있습니다.

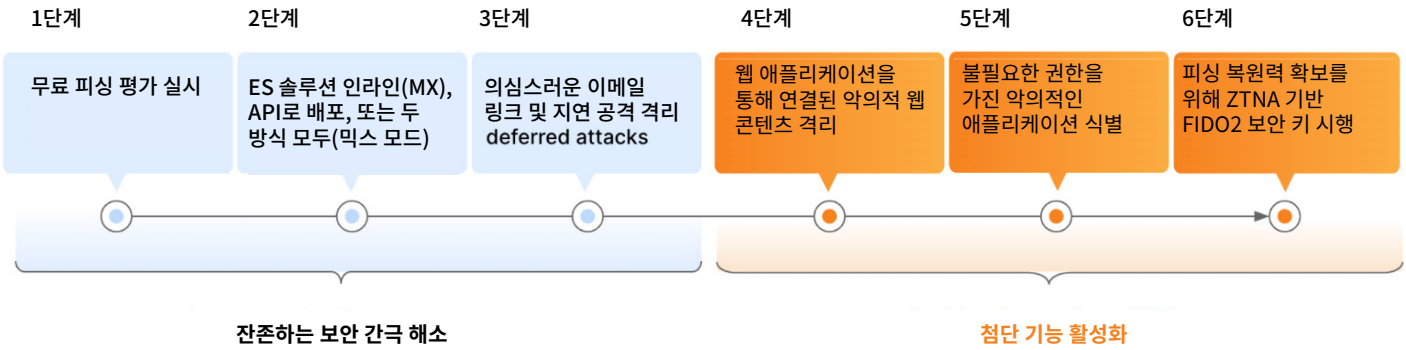
이점

완벽한 멀티 채널 보호

피싱 캠페인이 이메일을 넘어 빠르게 확장되면서, 조직에서 빠르고 간단한 경로로 완전한 멀티 채널 보호를 제공하는 피싱 솔루션을 구현하는 것이 그 어느 때보다도 시급해졌습니다.

조직에서는 Cloudflare One 플랫폼을 사용하여 먼저 업계 최고의 이메일 보안을 배포하여 가장 중요한 피싱 채널에 빠르게 대처한 후, 추가로 Zero Trust 서비스를 쉽게 활성화하여 모든 채널에 보호 기능을 확장함으로써 알려진 신흥 피싱 위협을 효과적으로 차단할 수 있습니다.

- **효율이 좋은 로우 터치 보호 기능:** 업계 최고의 감지 기능을 사용하여 최소한의 조정만으로 피싱 위협을 최소화합니다.
- **더 큰 통합, 더 낮은 비용:** 모든 피싱 사용 사례를 해결하는 완전 통합 단일 플랫폼으로 지출을 줄입니다.
- **빠른 배포, 손쉬운 관리:** 즉각적인 보호를 보장하는 동시에 지속적인 관리에 필요한 시간과 노력을 줄입니다.



평가 및 비교

현재 사용하고 있는 이메일 보호 기능을 평가하고 어떤 위협을 놓치고 있는지 확인

몇 분 동안 무료 레트로 스캔(O365 받은 편지함)을 실행하여 지난 14일 동안 어떤 피싱 위협이 전달되었는지 확인하거나, PRA(피싱 위험 평가)를 요청하여 받은 편지함에서 피싱을 받고 있는지 모니터링합니다. 즉시 사용 가능하며 조정이 필요 없는 다른 공급자와 비교해보고 어떤 이메일 보안 솔루션이 가장 빠르고 가장 간편한 보호 기능을 제공하는지 평가해 보세요.

어떤 피싱 위협이 방어를 뚫고 침투하는지 확인하세요

레트로 스캔 실행 | PRA 요청하기

CLOUDFLARE

1. 2023 Forrester Opportunity Snapshot: 출처
2. 2023 피싱 위협 보고서 출처