이메일 링크 격리

이메일 링크를 격리하여 공격 표면을 줄이고 운영을 간소화하세요

브라우저 격리 보호 및 제어를 적용하여 피싱 위험을 줄이세요

과제: 정교한 다중 채널 피싱

다중 채널 피싱에는 필터링 규칙을 능숙하게 회피할 수 있는 방식으로 이루어지는 이메일 전송과 웹 전송이 포함됩니다. 일반적인 유형은 다음과 같습니다.

- **지연된 피싱:** 이메일에 내의 무해한 최초 링크는 전달된 이후, 악의적인 목적지를 통해 무기가 됩니다.
- **클라우드 서비스 피싱:** 위험한 HTTPS 링크는 일반적인 클라우드 서비스 (예: Google Drive, Box)와 매우 유사합니다

이러한 위협을 차단하려면 절대 신뢰하지 않고 항상 확인하는 Zero Trust의 정밀 조사를 모든 링크에 적용하는 최신 이메일 보호 기능을 갖추고 있어야 합니다.

솔루션: 이메일 링크 격리

원격 브라우저 격리(RBI)
기능을 클라우드 이메일 보안(CES)과 통합하면
정밀 조사를 적용하여 피싱 방지를
강화할 수 있습니다. Cloudflare Area 1
고객은
Cloudflare 브라우저 격리
기능을 사용하여 이러한
다중 채널 위협을 방어할 수 있습니다.

관리자는 격리된 웹 페이지에서 사용자 인터렉션을 제어하여(키보드 입력 및 파일 업로드 제한) 자격 증명 수집이나 기밀 데이터 도난과 같은 피싱의 영향을 방지할 수 있습니다.

또한, 격리된 브라우저에서 이메일 링크를 열면 모든 모든 코드를 로컬 장치에서 멀리 떨어진 클라우드에서 실행하여 맬웨어를 무력화할 수 있습니다.

분석가의 견해:

"외부에서 확인되는 이메일 기반 URL은 직원을 속이는 데 자주 사용됩니다. 이러한 이메일을 격리하면 피싱 공격 성공률을 줄일 수 있습니다."

"대부분의 공격은 웹 브라우징 또는 사용자가 악의적인 사이트를 방문하도록 유도하는 이메일 링크를 통해 공용 인터넷으로 전달됩니다. 최종 사용자의 데스크톱에서 브라우저를 제거(또는 더 강력하게 격리)하기만 하면 랜섬웨어 공격에 맞서 보호하고 기업 보안 상태를 크게 개선할 수 있습니다."

"특히 불확실성을 낮추려 하는 조직이라면, 재무 팀와 같이 위험도가 높은 특정 사용자에게 적합한 브라우저 격리 솔루션이나 이메일 기반 URL 렌더링과 같은 사용 사례를 평가해 시범적으로 운영해 보세요."[1]

Gartner

자세히 알아보기

CES 및 RBI 통합의 비즈니스 이점

피싱 보호 강화

이메일 격리는 피싱 링크의 유해한 코드가 로컬에서 실행되지 않도록 막아주며, 데이터 보호 제어를 적용하여 중요한 정보가 공격자의 손에 들어가지 않도록 방지합니다.

IT 및 보안 생산성 활용

몇 번의 클릭으로 모든 웹 사이트에 이메일 격리를 켜세요.

IT 팀과 보안 팀은 사용자 생산성을 저하할 만큼 '과도하게 차단할' 위험과, 위협을 허용할 만큼 '차단이 부족할' 위험이 있는 필터링 정책을 구성하는 번거로움에서 벗어날 수 있습니다.

사용 사례 예시: 지연된 피싱 차단

문제: 지연된 피싱은 감지되지 않습니다

지연된 피싱 캠페인에 적절한 전략과 동기가 갖춰지면, 기존의 보호 조치를 피해갈 수 있습니다.

캠페인 설정: 공격자는 새로 만든 도메인을 사용하여 진짜 같은 이메일을 보내거나 적절한 이메일 인증(SPF, DKIM, DMAR)과 무해한 웹 페이지를 사용하여 공격을 시작할 수 있습니다.

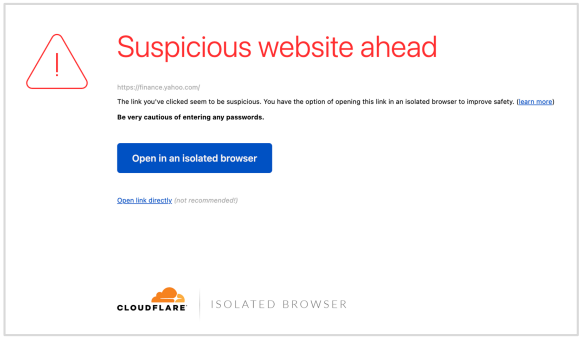
수신함에 전달 성공: 이러한 이메일은 보안 이메일 게이트웨이, 인증 기반 필터 또는 평판 기반 신호 및 기타 결정론적 기술에 의존하는 기타 서비스에서 감지되지 않습니다.

악의적인 링크로 변경: 이메일이 성공적으로 전달되면 공격자는 링크를 직접 제어하는 웹 페이지로 변경해 악의적인 목적지로 바꿔버릴 수 있습니다. 예를 들어, 자격 증명을 수집하기 위해 가짜 로그인 페이지를 사용하는 경우가 흔합니다.

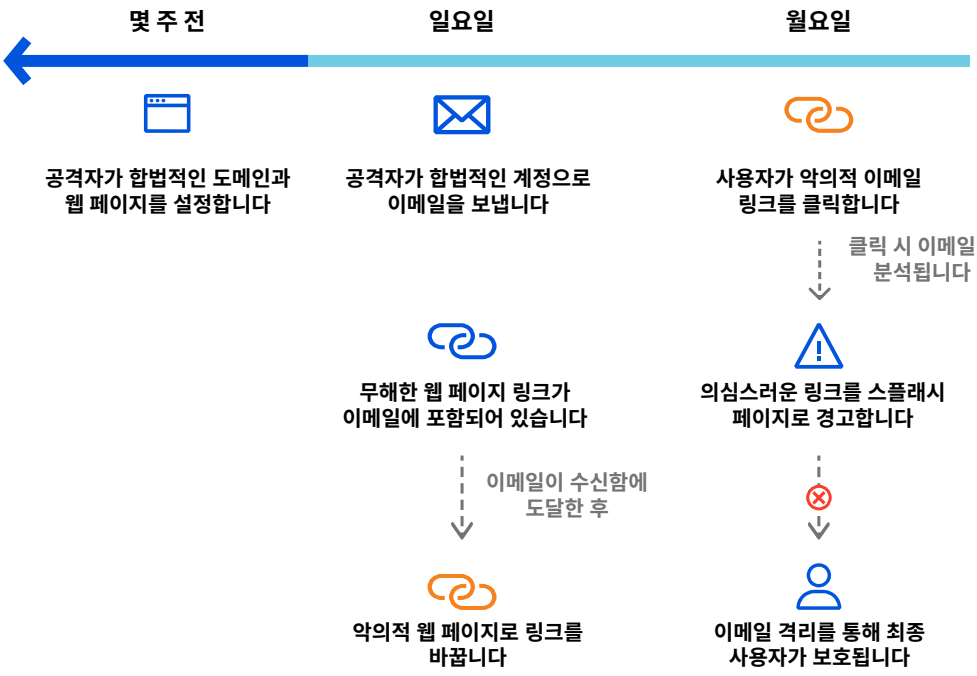
솔루션: 전달 후 의심스러운 링크 격리

이메일 링크 격리는 전달 후 보호라는 중요한 계층을 제공합니다. Cloudflare는 사용자가 클릭한 이메일에서 모든 링크를 분석합니다. 링크가 의심스럽거나 위험한 것으로 판단되면, Cloudflare는 경고 스플래시 페이지*(아래 참조)*를 표시하고 사용자가 웹 페이지를 탐색하면 웹 페이지를 격리합니다.

관리자는 로컬 장치에서 악성 코드가 실행되지 않도록 하고 파일 업로드 및 다운로드 제한, 사용자 키보드 입력 방지 또는 읽기 전용 모드로 웹 페이지 열기 등 데이터 보호 제어를 적용할 수 있습니다.



지연된 피싱 캠페인의 타임라인



Cloudflare는 클릭 시점에 각 링크를 분석합니다

안전한 링크: 사용자가 이 사이트로 투명하게 리디렉션됩니다.

악의적 링크: 탐색하지 못하도록 사용자가 차단됩니다.

의심스러운 링크: 탐색하지 않는 것이 좋으며 격리된 브라우저에서 링크를 확인하도록 권고하는 스플래시 경고 페이지가 사용자에게 표시됩니다.

Cloudflare Zero Trust와 클라우드 이메일 보안 통합

Zero Trust를 이용한 최신 보안

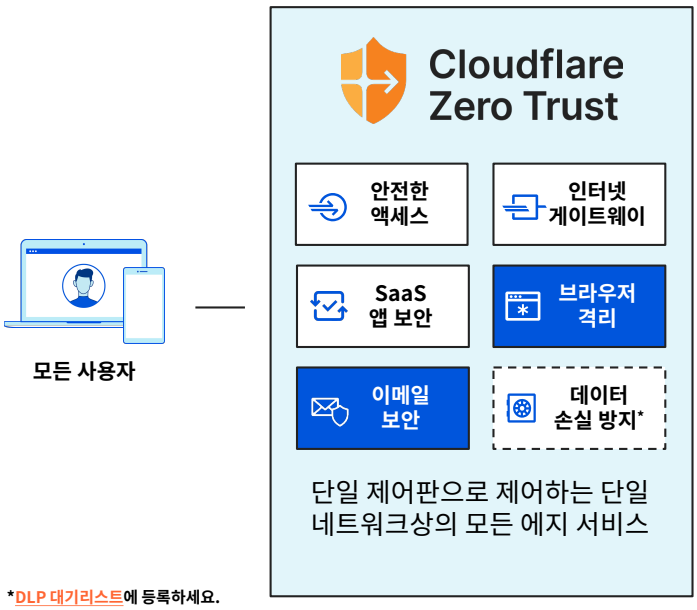
Cloudflare Zero Trust는 원격 근무자와 사무실 근무자가 기업 애플리케이션과 공용 인터넷에 접속할 때 가시성을 높이고 복잡성을 제거하며 위험을 줄입니다.

2022년 4월 1일, Cloudflare는 당사의 Zero Trust 플랫폼을 통해 이메일, 웹, 네트워크 환경의 피싱 공격으로부터 사용자를 더욱 강력하게 보호하겠다는 비전으로 Area 1 Security 인수를 마무리했습니다. 여기에서 자세히 읽어보세요.

이메일 보안: Zero Trust의 핵심

Cloudflare Area 1 이메일 보안은 이메일에서 암시적 신뢰를 제거해 피싱 및 비즈니스 이메일 손상(BEC) 공격을 선제적으로 방어하여 Zero Trust를 강화합니다.

내부 발신자라고 하더라도, 모든 발신자를 절대 신뢰하지 않습니다. 그 대신 이메일을 포함한 모든 사용자 트래픽을 검증, 필터링, 검사하며 인터넷 위협으로부터 격리합니다. 이메일 보안은 RBI, CASB 등과의 강력한 연동과 더불어 Cloudflare의 모든 Zero Trust 서비스에 통합됩니다.



*DLP 대기리스트에 등록하세요.

VPN 대체
모든 리소스에 대한 사용자 연결을 간소화하고 안전하게 보호

인터넷 보호
모든 포트 및 모든 프로토콜에서 위협으로부터 데이터를 안전하게 보호

SaaS 보안 간소화
이메일을 포함한 애플리케이션의 가시성 및 제어

보안 현대화
생산성 향상,
더욱 단순화된 운영,
공격 표면 감소

클라우드 이메일 보안(CES)

- 피싱 인시던트 대응 시간을 90% 단축하세요.
- 공격 초기 단계에 피싱을 차단할 수 있도록 미리 공격자의 인프라와 전달 메커니즘을 파악합니다.
- 커뮤니케이션의 콘텐츠, 컨텍스트, 소셜 그래프를 분석하여 이메일에서 암시적인 신뢰를 제거합니다.
- Microsoft, Google, 기타 환경과의 통합을 활용하여 기본 제공 보안을 강화하세요

원격 브라우저 격리(RBI)

- 사용자 인터렉션(예: 키보드 입력, 복사 및 붙여 넣기, 업로드/다운로드)을 제어하여 '읽기 전용 모드'에서 위험한 사이트를 열어 자격 증명 손상을 방지하세요.
- 모든 브라우저 코드를 Cloudflare 네트워크에서 실행하여 악성 코드로부터 로컬 장치를 격리하세요.
- 매끄럽고 빠른 최종 사용자 경험을 선사하세요. 일반적인 픽셀 스트리밍 대신, 전 세계 인터넷 사용자의 95%로부터 최대 50밀리초 거리에 있는 원격 브라우저에서 정확한 복제본 페이지를 제공합니다.

피싱 위험 평가 요청 문의

+82 70 4515 6893 | enterprise@cloudflare.com | www.cloudflare.com

REV: PMM-2022JUN

[1] *Gartner Hype Cycle for Network Security, 2021* /GARTNER 및 HYPE CYCLE은 Gartner, Inc. 및/또는 미국 내 계열사의 등록 상표 및 서비스 마크이며 허가 하에 본 문서에 사용되었습니다.