사칭메일 공격 목표는 사람입니다.
메일 수신자는 사칭메일을 인지할 수 없기에 메일의 내용을 믿고 행동하여 사고가 일어납니다.
사칭메일 피해 방지는 이메일 수신 전에 차단하는 것이 유일한 해결책입니다.

사회공학기법의 사칭메일 공격을 원천 차단하는

사 칭 메 일 관 리 시 스 템

우수특허 혁신제품 / 보안기능확인서 / GS1등급 / KOLAS인증

2023년

RealSecu
Security System

RealSecu
Security System

이메일 위협

이메일 사기공격(BEC) 피해
사칭메일 유형
사칭메일 대응의 오류
사칭메일 탐지 방안

이메일 사기공격(BEC) 피해

연간 2조 6천 억원

기존 운영중인 메일보안시스템은

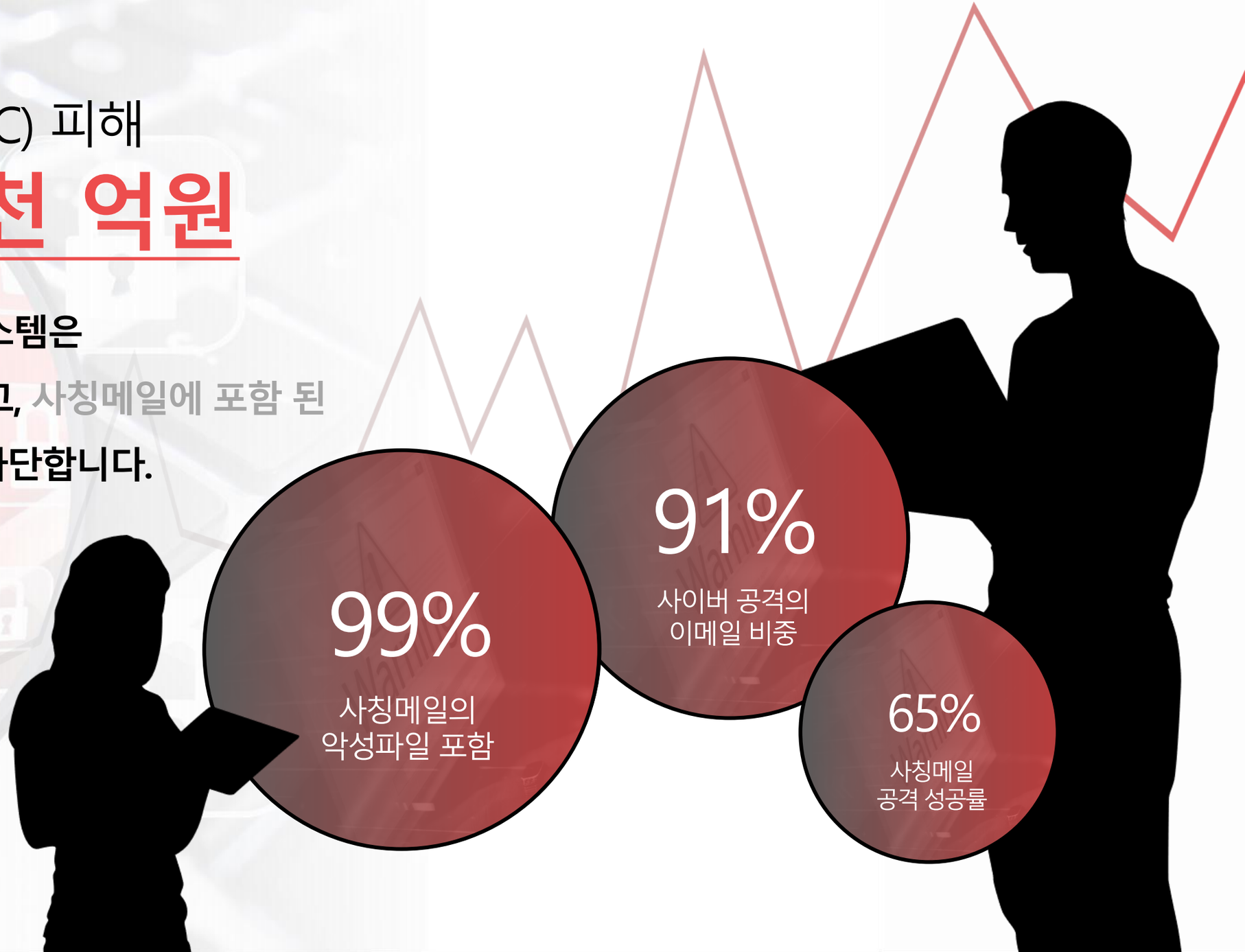
사칭메일은 탐지하지 못하고, 사칭메일에 포함 된

악성코드와 URL링크만을 차단합니다.

사이버공격의 91% 이메일을 통해 시작

사칭메일의 99% 악성파일을 포함

사칭메일 공격성공률 65%



[출처] 해킹메일동향 (KISA, 2019년)

업무와 관련된 사칭메일

제목 : 발주서 보내 드립니다.
내용 : **첨부파일** 다운 후 확인 부탁드립니다.

거래처를 사칭한 메일

제목 : 대금 결제 요청 건
내용 : 대금 결제 계좌가 변경 되었습니다.

공기관을 사칭한 메일

제목 : 위반사실통지 및 과태료 부과
내용 : 귀하의 차량이 법규 위반한 사실이 확인.

고객센터를 사칭한 메일

제목 : 계정이 해킹 당했습니다.
내용 : 아래 **링크**를 클릭하여 정보를 재설정해...

이메일 사기공격의 대상은
사람(메일 수신자)입니다.

사칭메일에 포함된 악성코드는 차단
사칭메일은 그대로 수신자에게 전달되어 사고 발생

사회공학기법의 사칭메일을 탐지하기 위해서 필요한 메일보안기술은 무엇일까?

RealSecu
Security System

이메일 사기공격(BEC)

"사람을 공격하는 메일" 사칭메일
이메일 사기공격(BEC) 방법
SPF, DKIM, DMARC 의 한계
안전한 메일 수신 플로우

사칭메일의 공격 목표는

사칭메일의 1차 목표는 사람입니다.
공격자는 메일 수신자를 사회공학기법을 통해 분석한 후
수신자가 메일의 발신자와 내용을 진짜로 믿게 만든 후
메일의 내용처럼 행동하게 합니다.

내부자를 사칭한 메일

위험군 : 그룹사, 공공기관 등 통합 메일 사용
형태 : 정기적인 내부 거래 결제 사기 등
목적 : 금전적 이득

업무를 사칭한 메일

위험군 : 이메일을 사용하는 모든 기업, 기관
형태 : 수신자의 업무에 따라 달라짐
목적 : 금전적 이득, 정보유출

거래처를 사칭한 메일

위험군 : 무역회사, 해외 비즈니스 기업
형태 : 거래처 계좌변경 유도
목적 : 금전적 이득

나를 사칭한 메일

위험군 : 이메일을 사용하는 모든 사용자
형태 : 나의 계정을 해킹하여 보냈다고 협박
목적 : 금전적 이득

막대한 피해가 잇따르는 사칭메일 공격

사칭메일로
거래대금 사기를 당한 L사

피해금액 **240억** 원

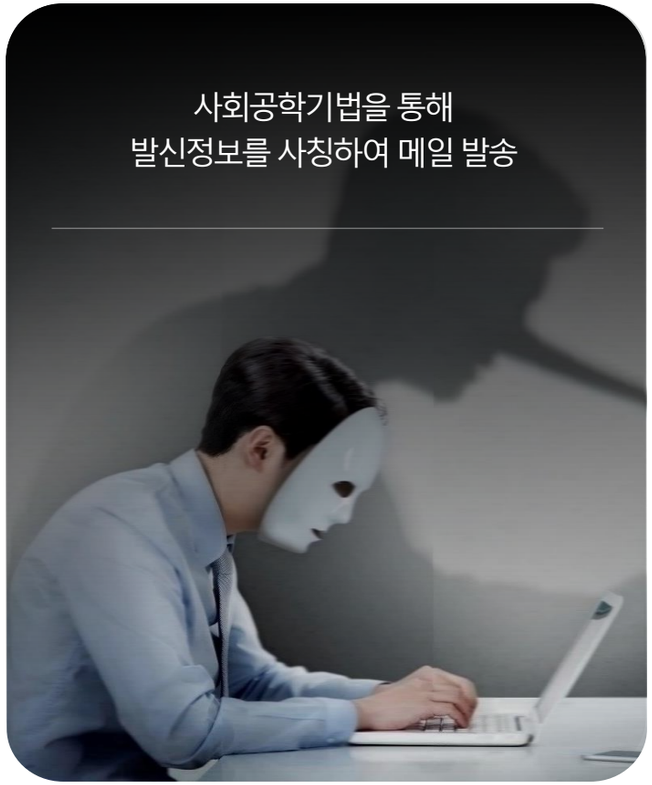
사칭메일로
거래대금 사기를 당한 M사

피해금액 **60억** 원

이메일 사기공격은 해커가 만든 사설메일서버를 이용
사회공학기법을 통해 발신정보를 사칭하여 수신자에게 발송

해커는 악의적인 목적으로
사설메일서버(발신스크립트)를 구축

사회공학기법을 통해
발신정보를 사칭하여 메일 발송



대부분의 사칭메일에는
악성코드가 포함되어 수신

사설메일서버 구축 → 사회공학기법 적용 → 사칭메일 수신

SPF, DKIM, DMARC 보안 기술은 전세계 모든 메일서버에 적용되어야 정상적인 운영 가능

1

SPF

메일서버등록제

Sender Policy Framework

2

DKIM

도메인 키 인증 메일

Domain Keys Identified Mail

3

DMARC

도메인 기반 이메일 인증

Domain based Message Authentication, Reporting & Conformance

- 사칭메일, 스피어피싱, 스캠 차단
- 무역대금 송금 사기 메일 차단
- 업무를 사칭한 메일 차단
- 계열사·협력사를 사칭한 메일 차단
- 출처가 불분명한 메일 차단

- 이메일 사기공격(BEC) 차단 불가

- 악성코드 차단 불가
- 이메일 사기공격(BEC) 차단 불가

RealSecu
Security System

리얼메일

보안지침
개요
핵심기술
흐름도
프로세스
기술비교
주요기능
부가기능
구성방안
제품유형
구축사례
기대효과

리얼메일 - 사칭메일관리시스템

RealMail

국정원	주요 내용
정보보안 기본지침	**제77조(전자우편 보안)** ①각급기관의 장은 전자우편을 컴퓨터바이러스·트로이목마 등 악성코드로부터 보호하기 위하여 백신 소프트웨어 설치, **해킹메일 차단시스템 구축 등 보안대책을 수립·시행**하여야 한다. ②각급기관의 장은 기관 전자우편을 구축·운용할 경우 다른 전자우편과 자료를 안전하게 소통하기 위하여 전자우편시스템에 암호화 기술을 적용하여야 한다. ③각급기관의 장은 기관 전자우편을 구축·운용할 경우 수신된 **전자우편의 발신지 IP주소 및 국가명이 표시되고 해킹메일로 의심될 경우 해킹메일 원본을 전송하여 신고할 수 있는 기능을 갖추어야 한다.** ④개별사용자는 수신된 전자우편에 포함된 첨부파일이 자동 실행되지 아니하도록 기능을 설정하고 **첨부파일을 다운로드할 경우 최신 백신 소프트웨어로 악성코드 은닉여부를 검사**하여야 한다. ⑤개별사용자는 **출처가 불분명하거나 의심되는 제목의 전자우편은 열람하지 말고 해킹메일로 의심될 경우 즉시 정보보안담당관에게 신고**하여야 한다. 정보보안담당관은 해킹메일로 판단될 경우 국가정보원장과 관계 중앙행정기관의 장에게 통보하여야 한다. ⑥각급기관의 장은 **전자우편 발신자 조작 등을 통한 기관 사칭 전자우편의 유포를 차단하기 위하여 보안대책을 수립·시행**하여야 한다.

과학기술정보통신부, 한국인터넷진흥원은 " **'22년 사이버 보안 위협 분석과 '23년 사이버 보안 위협 전망"**을 발표

22년 분석

정부기관을 사칭한 해킹메일을 유포하는 등 해킹 목적에 따라 대형사고로 이어질 수 있는 공격들이 발생하고 있어 **기관 사칭 해킹메일에 각별한 주의 필요**

23년 전망

사회공학적 기법을 통해 악성코드가 지속적으로 유포될 것이며, **전자우편** 뿐만 아니라 누리소통망 등 개인화된 채널을 활용한 **공격도 증가**

기대효과

- 거래처 대금사기 메일 차단
- 계열사 대금사기 메일 차단
- 내부자 대금사기 메일 차단
- '나'를 사칭한 메일 차단
- 업무 사칭 메일 차단
- 기타 '협박' 등 사칭 메일 차단

키워드

- 스피어피싱
- 사칭메일
- 무역 대금 사기
- 이메일 사기공격(BEC)
- 스캠
- 출처가 불분명한 메일 공격
- 악성메일모의훈련
- APT공격

리얼메일 - 사칭메일관리시스템

RealSecu Security System

RealMail

사회공학기법의 이메일 사기공격(BEC) 중 **사칭메일, 스피어피싱, 스캠** 등을 직접 검증하고 차단하는 **차세대 이메일보안솔루션**입니다. **발신자 검증 기술과 SMTP응답코드**를 분석하여 **이메일 사기공격을 직접 검증**하는 **Zero Trust기반**의 **최초의 사칭메일관리시스템**입니다.

주요 특징

- **사칭메일 관리시스템** 세계 최초
- **보안기능 확인서** 메일보안 최초
- **우수특허 혁신제품** 메일보안 최초
- **이메일 사기 공격(BEC)차단** 국내 최초
- **출처가 불분명한 메일 차단** 국내 최초
- **제로 트러스트 화이트 보안기술** 사칭메일보안 최초

인증서

GS1등급

KOLAS인증

보안기능확인서

SMTP응답코드

발신자 검증 알고리즘

기대효과

- 거래처 대금사기 메일 차단
- 계열사 대금사기 메일 차단
- 내부자 대금사기 메일 차단
- '나'를 사칭한 메일 차단
- 업무 사칭 메일 차단
- 기타 '협박' 등 사칭 메일 차단

키워드

- 스피어피싱
- 사칭메일
- 무역 대금 사기
- 이메일 사기공격(BEC)
- 스캠
- 출처가 불분명한 메일 공격
- 악성메일모의훈련
- APT공격

리얼메일 - 사칭메일관리시스템

RealSecu Security System

RealMail

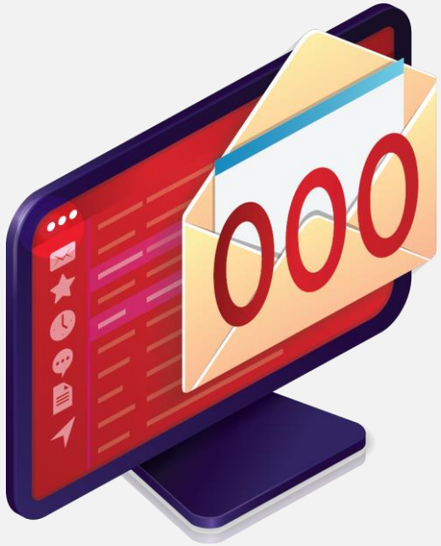
다수의 특허기술 중 **발신자 검증기술과 SMTP응답코드를 분석**을 통해 **이메일 사기공격(BEC)을 원천적으로 차단** 할 수 있습니다.

기대효과

- 거래처 대금사기 메일 차단
- 계열사 대금사기 메일 차단
- 내부자 대금사기 메일 차단
- '나'를 사칭한 메일 차단
- 업무 사칭 메일 차단
- 기타 '협박' 등 사칭 메일 차단

키워드

- 스피어피싱
- 사칭메일
- 무역 대금 사기
- 이메일 사기공격(BEC)
- 스캠
- 출처가 불분명한 메일 공격
- 악성메일모의훈련
- APT공격



SMTP 응답코드란?

- 이메일의 수신과 발신에 대한 유실을 방지하기 위해 개발된 3자리 숫자 코드
- 리얼메일은 발신 측 정보를 정확히 검증하기 위한 단서 (특허 등록)

정상메일서버

정상메일

- id@domain 그리고 메일서버는 세계에서 하나 뿐 인, 유일한 것이다
- id@domain은 정상메일서버에서 발송 된 유일한 메일이다
- 정상 메일은 수신자의 필요성에 따라 아래와 같이 다양하게 분류된다

일반 메일 | 업무 메일 | 뉴스 레터 | 홍보 메일
스팸 메일 | 불필요한 메일 | 알 수 없는 메일

사설메일서버

사설메일

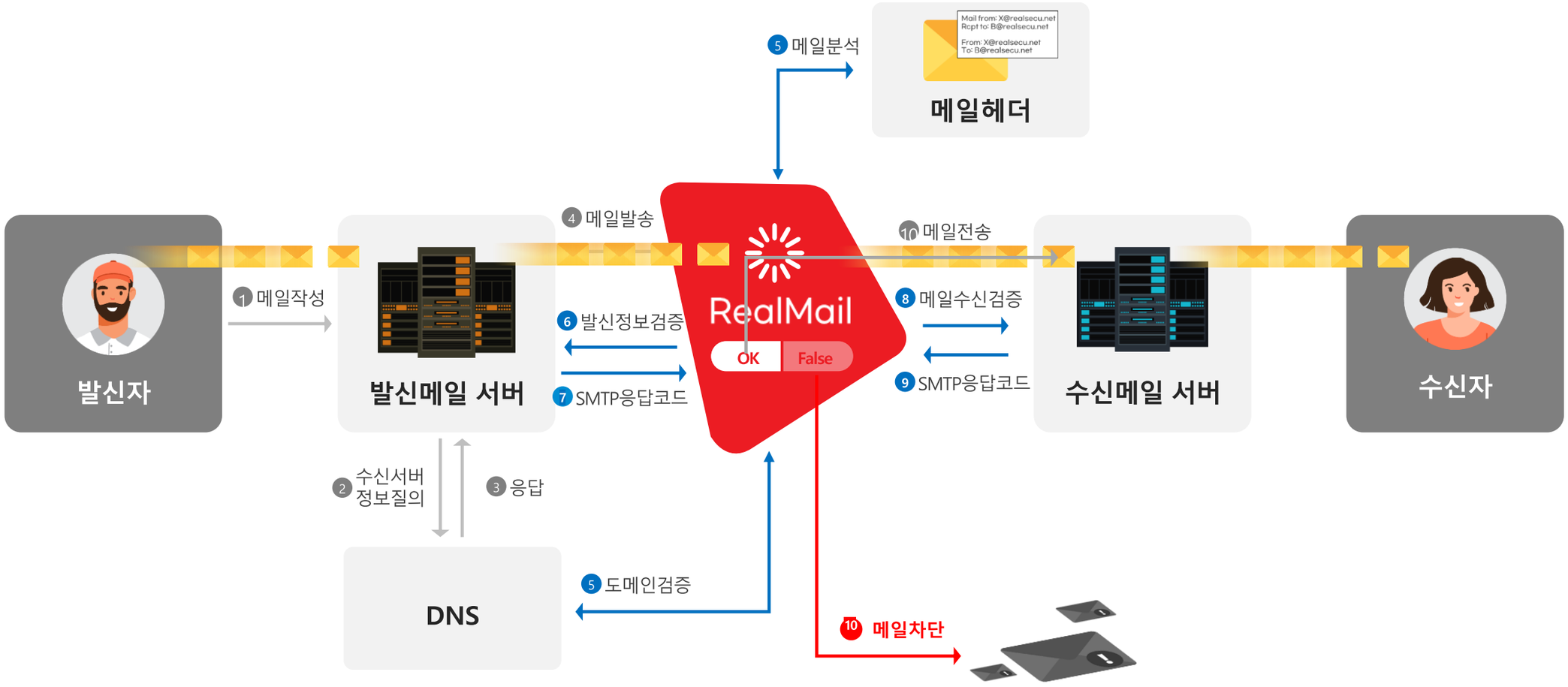
- 사칭메일은 정상메일처럼 보이게 사칭한 중복 메일이다
- 출처가 불분명한 메일은 DNS에서 확인할 수 없는 사설메일이다
- 사설 메일은 수신자의 생각에 따라 아래와 같이 다양하게 분류된다

업무 메일 | 스피어피싱 | 유사도메인 | 사칭 메일 | 스캠
스팸 메일 | 악성 스팸 메일 | 불법광고 메일 | 출처가 불분명한 메일

리얼메일 - 사칭메일관리시스템

RealMail

Zero Trust기반의 수신된 **모든 메일의 발신측 정보를 실시간으로 재검증**하여 **수신여부를 결정**합니다. **발신측 정보가 정확히 확인된 메일만 수신자에게 전달**합니다.



기대효과

- 거래처 대금사기 메일 차단
- 계열사 대금사기 메일 차단
- 내부자 대금사기 메일 차단
- '나'를 사칭한 메일 차단
- 업무 사칭 메일 차단
- 기타 '협박' 등 사칭 메일 차단

키워드

- 스피어피싱
- 사칭메일
- 무역 대금 사기
- 이메일 사기공격(BEC)
- 스캠
- 출처가 불분명한 메일 공격
- 악성메일모의훈련
- APT공격

리얼메일 - 사칭메일관리시스템

RealMail

사회공학기법의 **이메일 사기공격(BEC)을 차단**하는 **수신 메일 처리 프로세스** 입니다.

STEP 1 수신 차단

- RBL 차단
- 키워드필터링
- 국가별 IP 차단
- SPF, DKIM, DMARC 차단

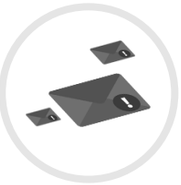
STEP 2 메일 분석

- 메일 헤더 분석
- DNS 정보 분석
- 세션 계정, 세션 도메인 분석
- 메일 릴레이 연계 분석
- 알고리즘 연관 분석

STEP 3 메일 검증

- 도메인 검증
- 사칭메일 검증
- 사설메일 검증
- 출처가 불분명한 메일 검증
- 수신메일 계정 검증
- 메일서버 설정 검증
- 메일서버 서비스 검증

수신



차단

기대효과

- 거래처 대금사기 메일 차단
- 계열사 대금사기 메일 차단
- 내부자 대금사기 메일 차단
- '나'를 사칭한 메일 차단
- 업무 사칭 메일 차단
- 기타 '협박' 등 사칭 메일 차단

키워드

- 스피어피싱
- 사칭메일
- 무역 대금 사기
- 이메일 사기공격(BEC)
- 스캠
- 출처가 불분명한 메일 공격
- 악성메일모의훈련
- APT공격

리얼메일 - 사칭메일관리시스템

RealSecu Security System

RealMail

메일보안시스템들은 **각각의** 솔루션들이 가지고 있는 분명한 **개발목적**이 있습니다.

	리얼메일	스팸메일차단시스템	샌드박스시스템
개발목적	**사칭메일 차단**	스팸메일 차단	악성코드 차단
차단기준	메일의 발신정보, 수신정보	메일의 내용과 첨부파일	메일의 내용과 첨부파일
핵심기술	SMTP응답코드, 발신자 검증 알고리즘 (특허기술)	패턴, 키워드	행위 기반, 가상화 기술
검사범위	패킷, 세션, 헤더, SMTP, DNS, 메일본문 등	패킷, 세션, 헤더, SMTP, DNS, 메일본문 등	패킷, 세션, 헤더, SMTP, DNS, 메일본문 등
주요기능	• 사칭메일 공격 차단 • 스피어피싱 공격 차단 • 이메일 사기 공격 차단 • 출처가 불분명한 메일 공격 차단 • 발신전용 메일 차단 • 사설메일 차단 • 메일 본문 이미지 변환 • 차단 메일 리스트 제공 • 국가별 메일 IP 리스트 지원	• RBL 차단 • 불법 Relay 차단 • 메일 유효성 검사 • SMTP 세션 제어 • 바이러스 탐지 및 차단 • 키워드 필터링 • 메일서버 보호	• 시그니처 기반의 파일 분석 및 차단 • 행위기반의 파일 분석 및 차단 • 이상행위 식별 및 진단 • 악성 URL에 대한 분석 및 차단 • 압축파일 검사 • 악성파일에 대한 머신러닝 분석 • 암호 파일 검사
부가기능	컨텐츠 무해화(CDR)	내부정보 유출탐지	CDR
기대효과	**이메일 사기공격(BEC) 원천 차단**	불필요한 메일 차단	멀웨어, 랜섬웨어 차단

기대효과

- 거래처 대금사기 메일 차단
- 계열사 대금사기 메일 차단
- 내부자 대금사기 메일 차단
- '나'를 사칭한 메일 차단
- 업무 사칭 메일 차단
- 기타 '협박' 등 사칭 메일 차단

키워드

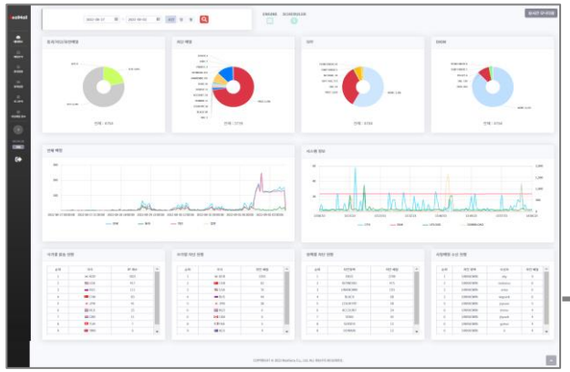
- 스피어피싱
- 사칭메일
- 무역 대금 사기
- 이메일 사기공격(BEC)
- 스캠
- 출처가 불분명한 메일 공격
- 악성메일모의훈련
- APT공격

리얼메일 - 사칭메일관리시스템

RealMail

발신측 정보를 확인할 수 있는 **직관적인 UI**와 모든 기능을 쉽고 간편하게 설정하고 관리할 수 있는 다양한 기능을 제공합니다.

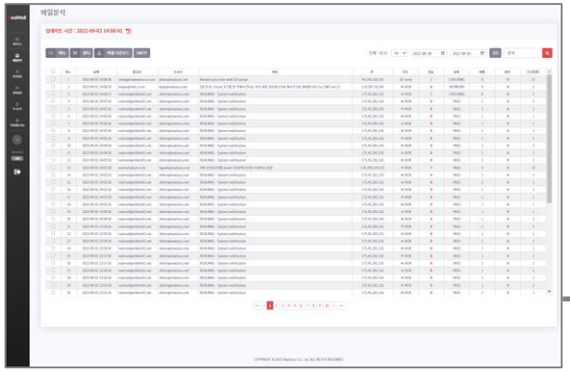
리얼메일 대시보드



- 직관적인 차트와 그래프를 통한 수신 메일 현황 파악

전체메일
차단메일
시스템정보
국가별 발신정보
국가별 차단정보
정책별 차단정보
사칭메일 정보

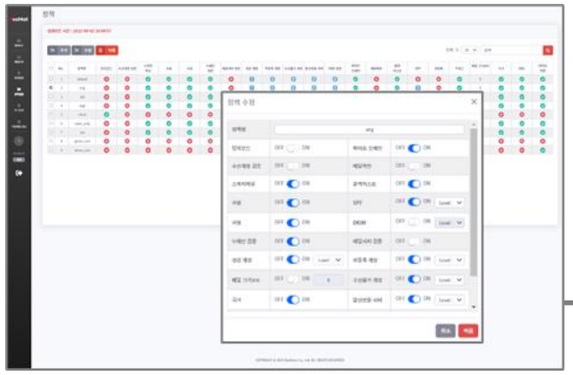
메일 분석 및 관리



- 수신메일에 대한 발신정보 분석 기능 제공 및 관리

발신자 검증
메일 헤더
재전송
화이트,블랙 추가
필터설정
엑셀다운로드
SMTP

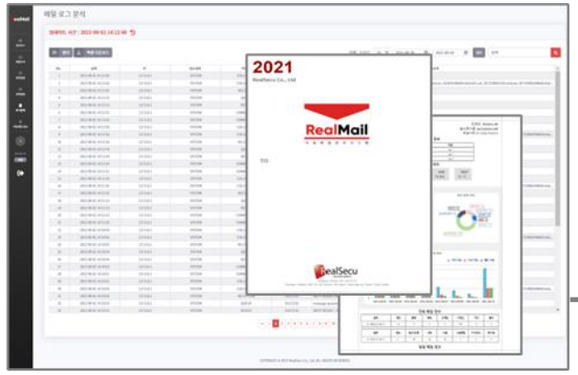
정책 설정 및 관리



- 그룹별 정책을 설정하여 효율적인 업무 지원

정책 추가, 수정
키워드리스트
국가별 정책
시스템 설정
관리자 설정
그룹 설정
차단메일리스트

로그분석 및 보고서



- 다양한 로그 분석 및 보고서 생성 기능 제공

시스템 로그분석
메일 로그분석
보고서 생성
매뉴얼 및 정보

기대효과

- 거래처 대금사기 메일 차단
- 계열사 대금사기 메일 차단
- 내부자 대금사기 메일 차단
- '나'를 사칭한 메일 차단
- 업무 사칭 메일 차단
- 기타 '협박' 등 사칭 메일 차단

키워드

- 스피어피싱
- 사칭메일
- 무역 대금 사기
- 이메일 사기공격(BEC)
- 스캠
- 출처가 불분명한 메일 공격
- 악성메일모의훈련
- APT공격

리얼메일 - 사칭메일관리시스템

RealMail

이메일에 포함된 **첨부파일(문서) 내 숨겨진 악성 콘텐츠의 위협을 정확히 제거하고 재구성**하여 안전한 첨부파일(문서)을 보장한다. **(누리랩 기술제휴)**

리얼메일 연동

첨부파일
(문서)

1 식별 및 분류

- 파일 포맷 식별 (문서, 뷰어, 이미지 등)
- 압축(다중) 파일 식별
- DRM 적용 파일 식별
- 암호화 문서 식별
- 파일 손상 여부 식별

60여종, 수백여가지 형태의 다양한 포맷의 파일 검출

2 탐지 및 차단(연동)

정상 파일(문서)

악성 파일(문서)

3 CDR(재조립)

- 악성코드 유사도 검증
- CDR(무해화) 처리

정상 파일
(문서 재구성)

WHITELIST

* 추가 기능 라이선스 필요

기대효과

- 거래처 대금사기 메일 차단
- 계열사 대금사기 메일 차단
- 내부자 대금사기 메일 차단
- '나'를 사칭한 메일 차단
- 업무 사칭 메일 차단
- 기타 '협박' 등 사칭 메일 차단

키워드

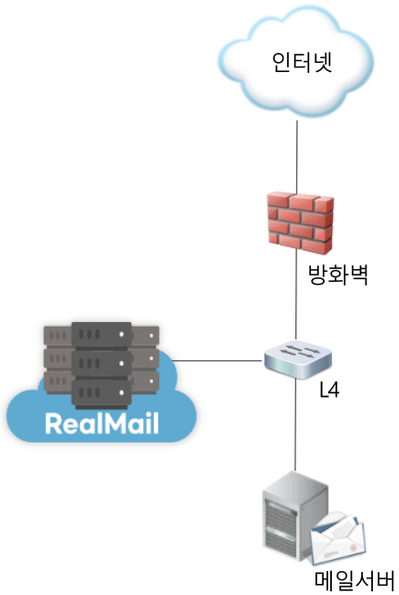
- 스피어피싱
- 사칭메일
- 무역 대금 사기
- 이메일 사기공격(BEC)
- 스캠
- 출처가 불분명한 메일 공격
- 악성메일모의훈련
- APT공격

리얼메일 - 사칭메일관리시스템

RealMail

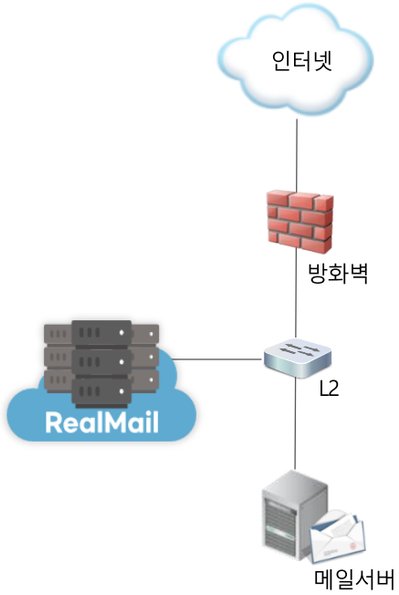
메일시스템의 네트워크 환경에 따라 **다양한 형태의 구성을 지원**합니다. (Bridge, Proxy, Cloud Service)

Bridge



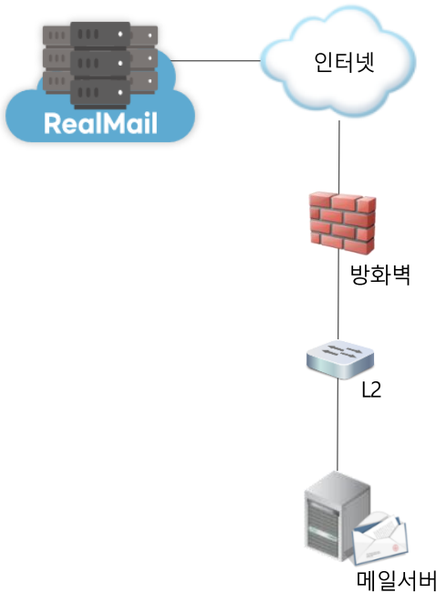
- L4를 통한 단일 또는 이중화 지원
- 리얼메일 장애 시 메일 수신은 이상 없이 지원
- DNS 설정 변경 최소화
- 시스템 설정 변경 최소화
- 내부 메일서버 운영 시

Proxy



- MX레코드 변경으로 메일 수신 우선 순위 조정
- 시스템 설정 변경 최소화
- 내부 메일서버 운영 시
- 외부메일서비스 운영 시

Cloud Service



- MX레코드 변경으로 메일 수신 우선 순위 조정
- 시스템 설정 변경 최소화
- 내부 메일서버 운영 시
- 외부메일서비스 운영 시

기대효과

- 거래처 대금사기 메일 차단
- 계열사 대금사기 메일 차단
- 내부자 대금사기 메일 차단
- '나'를 사칭한 메일 차단
- 업무 사칭 메일 차단
- 기타 '협박' 등 사칭 메일 차단

키워드

- 스피어피싱
- 사칭메일
- 무역 대금 사기
- 이메일 사기공격(BEC)
- 스캠
- 출처가 불분명한 메일 공격
- 악성메일모의훈련
- APT공격

리얼메일 - 사칭메일관리시스템

RealSecu Security System

RealMail

기대효과

- 거래처 대금사기 메일 차단
- 계열사 대금사기 메일 차단
- 내부자 대금사기 메일 차단
- '나'를 사칭한 메일 차단
- 업무 사칭 메일 차단
- 기타 '협박' 등 사칭 메일 차단

키워드

- 스피어피싱
- 사칭메일
- 무역 대금 사기
- 이메일 사기공격(BEC)
- 스캠
- 출처가 불분명한 메일 공격
- 악성메일모의훈련
- APT공격

리얼메일은 구축형과 서비스형을 제공합니다.

구축형

H/W	인력	단점
H/W 필요	관리인력 필요	도입비용 및 유지비용 증가

다양한 구축	데이터 관리	보안정책 관리
고객별 맞춤형 구축 제공 및 커스터마이징	자체 데이터 관리로 기업 데이터 보안 강화	사내 네트워크 보안 및 메일보안 정책 적용

메일 처리량(일)	30만 통	40만 통	50만 통
최대 처리량(일)	40만 통	50만 통	70만 통
H/W 사양 (X86계열)	Xeon 8 Core 이상 (3.2 GHz이상) RAM : 128GB 이상 SSD : 256GB HDD : 2 TB 이상	Xeon 12 Core 이상 (3.2 GHz이상) RAM : 256GB 이상 SSD : 256GB HDD : 2 TB 이상	Xeon 16 Core 이상 (3.2 GHz이상) RAM : 256GB 이상 SSD : 256GB HDD : 2 TB 이상

* CDR 적용 시 H/W업그레이드 필요함

서비스형(클라우드)

H/W	인력	단점
H/W 불필요	관리인력 불필요	맞춤형 기능 제공 불가

도입비용 없음	저렴한 비용	정기 업데이트
Cloud 서비스에 대한 도입비용 없음	트래픽량과 기간에 따라 비용 지불	신규 기능 자동 업데이트

CDR	라이선스 적용 불가
Cloud 비용	100 User 이상. 월 과금은 메일 트래픽량
SOHO 비용	100 User 미만, 월 과금은 도메인 수와 User수에 대한 정액제

리얼메일 - 사칭메일관리시스템

RealSecu Security System

RealMail

기대효과

- 거래처 대금사기 메일 차단
- 계열사 대금사기 메일 차단
- 내부자 대금사기 메일 차단
- '나'를 사칭한 메일 차단
- 업무 사칭 메일 차단
- 기타 '협박' 등 사칭 메일 차단

키워드

- 스피어피싱
- 사칭메일
- 무역 대금 사기
- 이메일 사기공격(BEC)
- 스캠
- 출처가 불분명한 메일 공격
- 악성메일모의훈련
- APT공격

HUMAX HOLDINGS

사칭메일 공격으로부터 내부정보 유출과 자금이체 사기 방지

기존 메일보안시스템에서는 탐지할 수 없는 사칭메일, 스피어피싱을

효과적으로 차단하는 사칭메일관리시스템 "리얼메일"

- 메일보안 환경

  : 스팸메일차단시스템과 이메일APT시스템 운영 중

  : 지속적인 사칭메일 공격 발생

- 구축내역


Case Study 휴맥스홀딩스, 리얼시큐 '리얼메일' 도입

지능적 사칭메일 차단해 글로벌 비즈니스 보호 … 제로 트러스트 원칙의 메일보안 체계 구축

사칭메일 정확한 탐지로 안전한 이메일 커뮤니케이션 보장

휴맥스그룹의 지주사인 휴맥스홀딩스(대표 변대규)는 '세계 1위 콘텐츠 소비 플랫폼(Contents Consuming Platform)' 기업으로 성장한다는 비전을 갖고 국내와 해외 휴맥스 그룹 계열사의 성장을 지원하고 있다. 휴맥스홀딩스는 그룹의 모든 회사들이 기업의 존재 목적에 충실하면서 끊임없는 혁신과 사회적 부의 창출을 통해 지속가능한 기업으로 성장하도록 도와주며, 모든 구성원들이 회사와 함께 좋은 리더로 성장해 나갈 수 있는 기반을 마련하기 위해 노력하고 있다.

_ 글·김선해 기자 iyamm@datanet.co.kr _사진·김구룡 기자 photoi@naver.com

사칭메일 관리시스템을 도입한 배경은

휴맥스홀딩스는 글로벌 기업으로, 전 세계 많은 국가, 많은 기업으로부터 메일을 수신하고 있다. 그중 신뢰할 수 있는 사람이나 기업 기관으로 위장한 사칭메일로 인한 위협에 대응해야 할 필요가 있었다.

사칭메일은 기존 메일보안 솔루션을 우회하고, 임직원의 습관이나 업무 특성을 악용하는 사회공학 기법을 사용하기 때문에 패턴시그니처 기반 메일보안 솔루션으로 차단할 수 없다. 특히 스캠, BEC와 같이 악성코드, 악성문서 없이 공격하는 시도를 차단하는 기술을 제공하는 별도의 메일보안 솔루션이 필요했다.

RealSecu Security System | HUMAX HOLDINGS

시스템 도입 시 가장 중요하게 검토한 것은

안정성과 정확성이다. 이메일은 업무의 중요한 수단이기 때문에 보안으로 인해 업무에 지장이 있어서는 안 된다. 정상 메일이 제대로 수신되지 않거나, 대규모 메일을 분석하느라 수신에 시간이 오래 걸려 시급한 주문을 제때로 전달받지 못하면 막대한 피해를 입을 수도 있기 때문이다. 그래서 업무에 영향을 주지 않는 빠르고 안정적인 속도와 오탐이 없는 정확도가 매우 중요한 검토 사항이었다.

리얼시큐의 리얼메일을 선택한 이유는

정확도와 안정성이 높기 때문이다. 실제 메일서버에서 테스트한 결과 정확하게 사칭메일을 찾아 차단하는 것을 확인했으며, 메일서버에 영향을 주지 않아 업무에 지장 없이 메일 보안을 적용할 수 있었다.

악성메일 대응에 대해 고민하는 기업 기관에 조언을 해 준다면

아무리 잘 설계된 보안 정책과 기술이 있다 해도 결국 뚫릴 수밖에 없다. 대규모 보안 사고가 나기 전에 수많은 침해 시도가 발견된다. 그렇기에 촘촘한 그물망 방식의 보안 정책을 통해 지능적인 공격시도에 대응할 필요가 있다. 제로 트러스트 원칙의 보안 정책으로 지능적이며 집요한 사칭메일 공격으로부터 비즈니스를 보호해야 한다.

리얼메일 - 사칭메일관리시스템

RealSecu Security System

RealMail

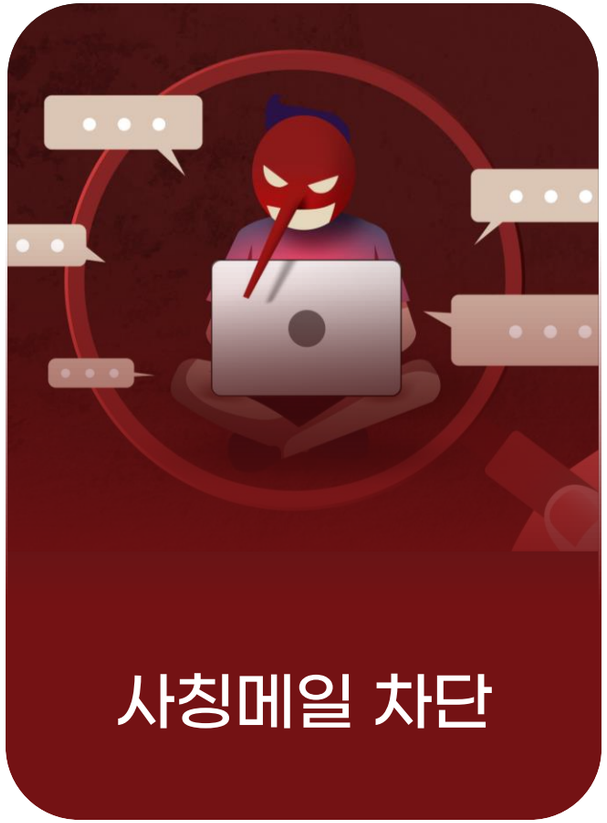
기대효과

- 거래처 대금사기 메일 차단
- 계열사 대금사기 메일 차단
- 내부자 대금사기 메일 차단
- '나'를 사칭한 메일 차단
- 업무 사칭 메일 차단
- 기타 '협박' 등 사칭 메일 차단

키워드

- 스피어피싱
- 사칭메일
- 무역 대금 사기
- 이메일 사기공격(BEC)
- 스캠
- 출처가 불분명한 메일 공격
- 악성메일모의훈련
- APT공격

사회공학기법 이메일 사기공격의 1차 목표는 수신자, 즉 사람입니다. **이메일 사기공격(BEC)은 수신자에게 전달하지 않는 것이 가장 안전합니다.**



RealSecu
Security System

사칭메일관리시스템

리얼메일은 소중한 정보자산을 지켜드립니다 !

THANK YOU FOR YOUR ATTENTION

부산광역시 해운대구 센텀북대로 60, 809
서울특별시 금천구 가산디지털1로 205-27, 811
051-552-9118
051-552-9121
realsecu@realsecu.net