



차세대 메일보안시스템

RealMail

사칭메일차단시스템

사칭메일

수신자를 속이기 위해 해커가 만든 가짜메일

- '내가 알고 있는 발신자' 가 나에게 보낸 '특별한 정보메일' 입니다.
- 사칭메일의 발신자와 메일제목은 수신자가 신뢰 할 수 있는 것으로 조작하여 **열람을 유도**합니다.
- 사칭메일의 메일내용과 첨부파일에는 **악의적인 목적이 포함**되어 있습니다.
- 사칭메일은 **메일보안시스템을 우회**하고 수신자에게 전달되어 피해를 일으킵니다.

사칭메일 형태

임직원 사칭



택배 사칭



문서 사기



경품 사기



악성코드

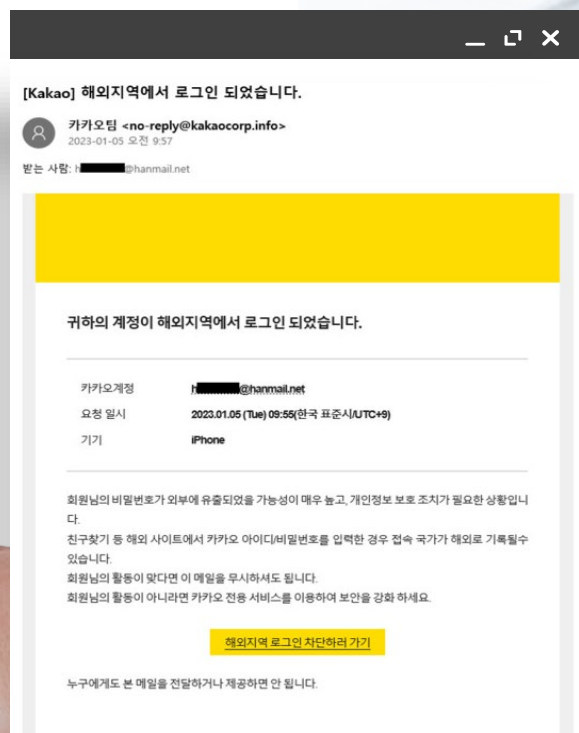


- 메일발송기를 통해 신뢰하는 발신자를 사칭하고 업무와 관련된 내용으로 만들어 발송합니다.
- 수신자는 사칭메일을 정상메일로 생각하고, 그대로 행동하여 피해가 발생합니다.
- 사칭메일에 의한 금전적인 피해는 일정한 시간이 지난 후 그 피해를 확인할 수 있습니다.
- 사칭메일은 수신자의 피해 유형에 따라 다양한 이름으로 불려져 많은 혼란을 가져옵니다.

사칭메일예시 I



사칭메일예시 II



사칭메일 피해 규모

2023년 기준

사칭메일공격으로 인한 피해금액 **27**억 달러 연간

사칭메일 피해 금액 증가 **3**배 이상 매년

랜섬웨어 대비 큰 피해 금액 발생 **80**배 이상

기관에서 사칭메일 공격 경험 **88**% 이상

데일리시큐
국내 공공종합병원 78%, 이메일 사기 및 도메인 스푸핑 공격에 노출
사이버보안 기업 프루프포인트는 국내 공공종합병원(국립중앙의료원 자료 기준)을 대상으로 진행한 이메일 이중 프로토콜(IMAP) 분석 결과를 발표

보안뉴스
2024년 2분기 피싱 메일 현황... 결제·구매로 주의 끌고, 가짜 페이지로 정보 입력 유도
2024년 2분기에는 가짜 페이지(Fake Page) 첨부파일을 악용한 피싱 메일 공격이 활발했다. NTPA: 드오르 제자디 가짜 페이지는 유명 브랜드가 트러거

전자신문
국정원이 알려주는 해킹메일 대응법은?... "모르는 사람 메일 무시·로그인 보안 강화"
생성형 인공지능(AI) 등 신기술 도입으로 인해 갈수록 해킹 메일 수법이 고도화하고 있어 대응책 수립은 물론 변화가 중요하다

ExpressVPN
2024년 전 세계 사이버 공격 피해 비용
2023년 사이버 공격으로 인한 전 세계 피해액은 8조 달러에 달할 것으로 예상되며, 2024년에는 9조 5천억 달러, 2025년에는 10조 5천억 달러로 증가할...

DigitalDaily
"복구 도와드릴게요"... IT 대란 파고드는 사이버 공격자들
[디지털데일리 김보민기자] 전 세계를 강타한 정보기술(IT) 대란이 사이버 공격에 대한 우려로 번지고 있다. 복구를 원하는 기관과 기업에 피싱 메일...
2024. 7. 22.

사칭메일 공격 순서



사칭메일은 메일내용과 첨부파일 분석으로 차단할 수 없습니다.

사칭메일을 발송한 '메일발송기'를 탐지해야 합니다.

이제 사칭메일 차단은 선택이 아닌 필수입니다.



사칭메일, 사기메일, 피싱, 스피어피싱, 출처가 불분명한 메일을 발송하는 해커의 메일발송기를 탐지하는 차세대 메일보안 시스템입니다.

제로트러스트 기반의 '머신러닝', '메일분류 알고리즘', '이메일 역추적기술', '메일서버 검증'을 통해 모든 발신측 정보를 실시간으로 검증합니다.

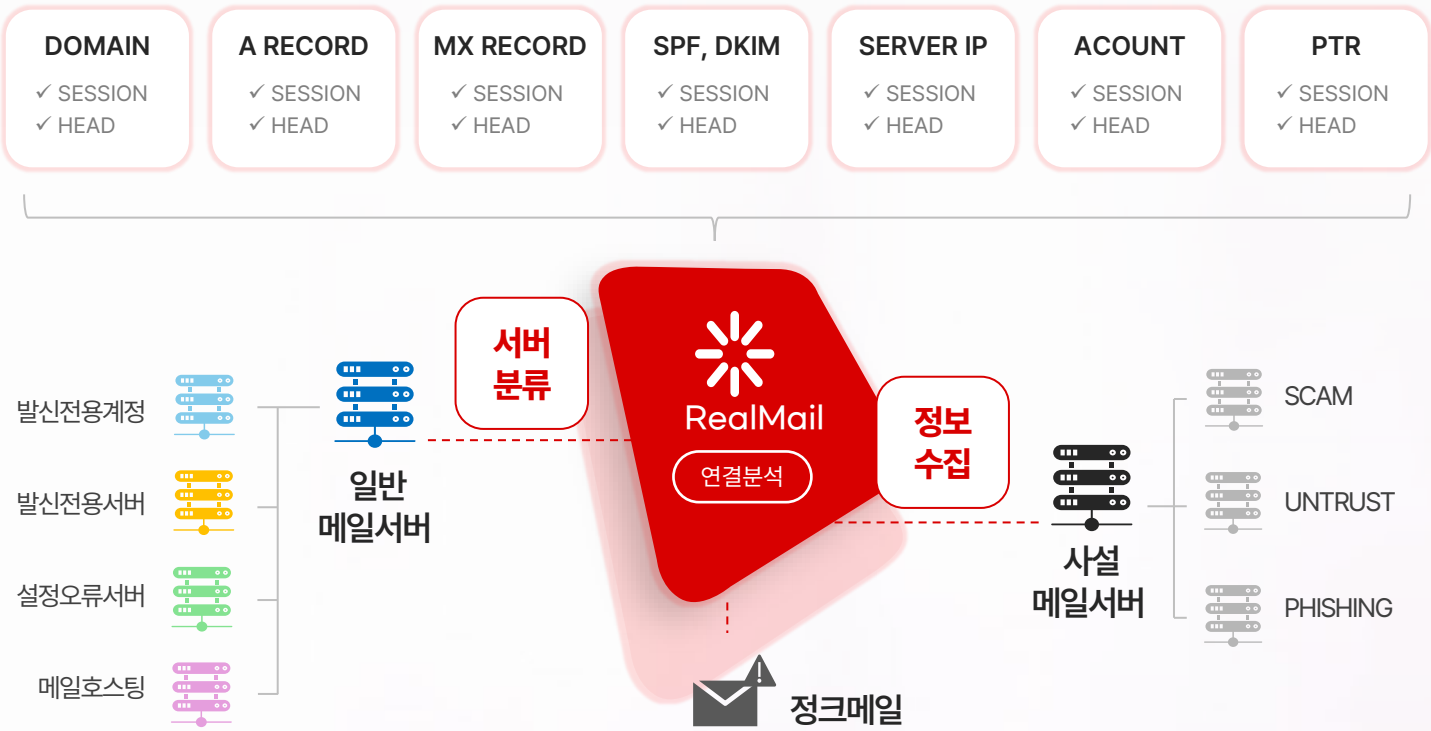


	사칭메일차단시스템	메일보안시스템
운영 목적	사칭메일 차단	스팸메일 차단
기반 기술	제로 트러스트 기반, 화이트 보안	가상화 / 블랙 보안
차단 기준	발신메일 서버	메일내용, 첨부파일
기대 효과	가짜메일 차단	악성메일 차단
차단 위치	발신 측	수신 측

RealMail 핵심 기술

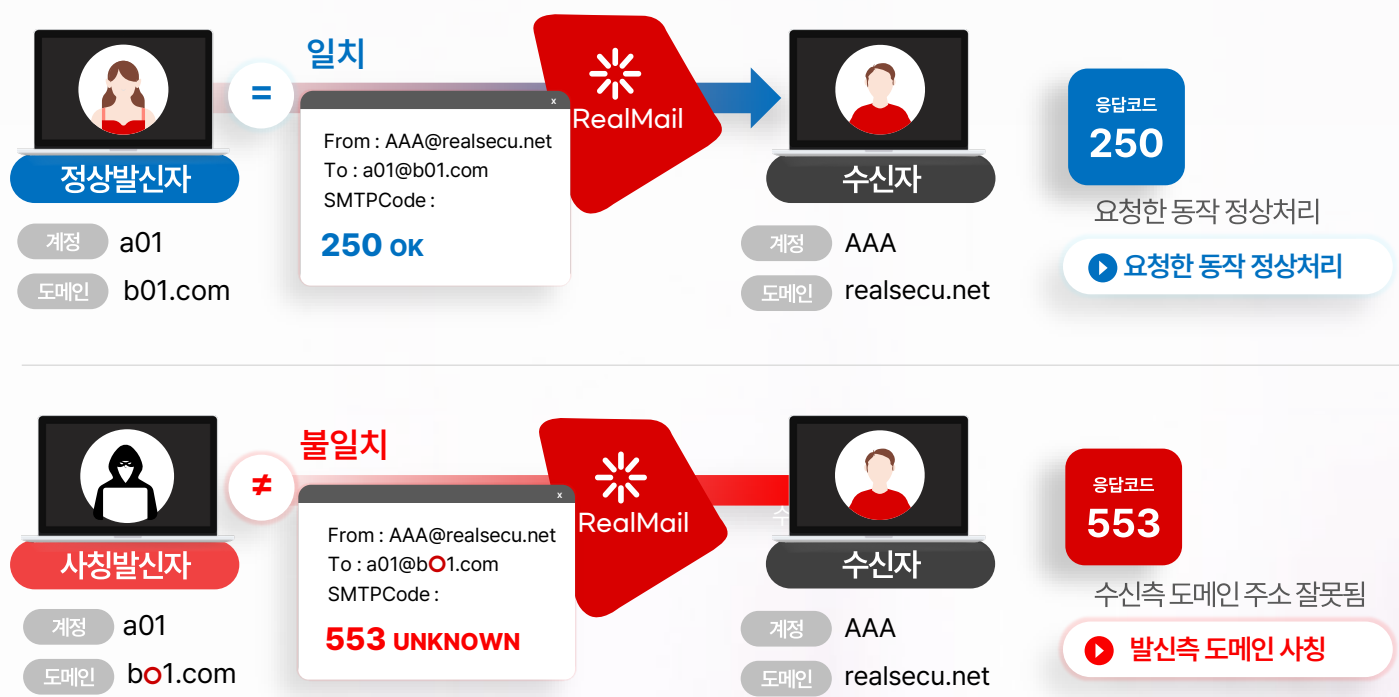
분석기술

메일분석 알고리즘, 머신러닝



검증기술

이메일 역추적, SMTP에러코드



* SMTP에러코드: 이메일 전달 과정에서 발생할 수 있는 통신 에러에 대비하여 발신자에게 그 원인을 알려주는 프로토콜 메시지이다.

주요 기능



SCAM



UNTRUST



PHISHING



JUNK



SPAM



VIRUS



Blacklist /
Whitelist



Multi-RBL



SRF/DKIM/
DMARC



수신계정 없는
메일 차단



메일 본문
이미지 변환



불필요한 국가
발신메일 차단



APT
(SandBox)



CDR
(컨텐츠 무해화)

모델

RealMail Appliance	RealMail 500	RealMail 1000	RealMail 3000	RealMail 5000	RealMail 10000
Mail Concurrent	200	300	300	400	500
Mail Throughput	25,000	100,000	200,000	400,000	700,000
HW Spec	4 Core 32 GB 960GB*2ea	8 Core 64 GB 960GB*2ea	12 Core 64 GB 1.92TB*2ea	16 Core 128 GB 3.84TB*2ea	20 Core 256 GB 3.84TB*2ea

* Mail Throughput - 일일메일 처리량 / Mail Concurrent - 동시 메일 처리량

UI

메일발송기를 통한 가짜메일을 차단하기 위해 개발된 **사칭메일차단시스템**

PHISHING / SCAM / UNTRUST / JUNK

JUNK
15

PHISHING
54

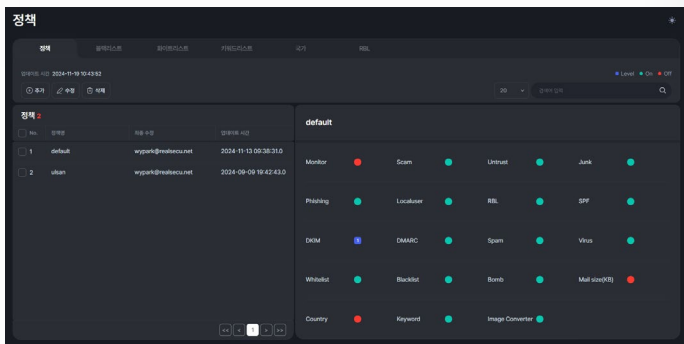
UNTRUST
0

SCAM
2



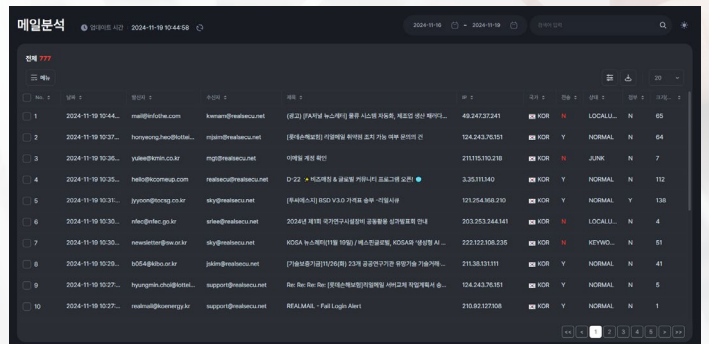
RealMail 대시보드 메인 화면. 상단에는 'JUNK 15', 'PHISHING 54', 'UNTRUST 0', 'SCAM 2' 등의 카운트 카드가 표시되어 있습니다. 중앙에는 시스템 정보 그래프와 국가별 발송 현황, 차단 현황, 정책별 차단 현황, BEC 공격 현황 등의 데이터 테이블이 포함되어 있습니다.

정책 설정



정책 설정 화면. '정책' 탭이 선택되어 있으며, 'default' 정책의 구성이 표시되어 있습니다. 각 정책 항목에는 'Monitor', 'Scam', 'Untrust', 'Junk', 'Phishing', 'Localuser', 'RBL', 'SPF', 'DKIM', 'DMARC', 'Spam', 'Virus', 'Whitelist', 'Blacklist', 'Bomb', 'Mail size(KB)', 'Country', 'Keyword', 'Image Converter' 등의 체크박스나 상태 표시가 있습니다.

메일 분석



메일 분석 화면. '메일분석' 탭이 선택되어 있으며, 분석된 메일 목록이 표시되어 있습니다. 목록에는 '일련 번호', '일련 번호', '발신자', '수신자', '제목', '발신 시간', '수신 시간', '상태', '종류', '등급' 등의 정보가 포함되어 있습니다.

차세대 메일보안시스템

RealMail

사칭메일차단시스템

 RealSecu

www.realsecu.net