국정원 인증, 혁신제품 지정, GS1등급

RealMail

사칭메일관리시스템

RealSecu
Security System

사칭메일, 스피어피싱, 출처가 불분명한 메일

사회공학기술과 정보공학기술의 결합, BEC 공격

2022년 하반기 국내 스팸메일 총 수신량957만 건

국내발 : 3만 건, 국외발 954만 건

(KISA, 22년 하반기 스팸 유통 현황)

- 사이버 공격의 92%가 이메일을 통해서 시작 (FireEye. 2021)
- 이메일 공격 중 사칭메일 공격90%, 악성코드 공격 10% (FireEye, 2020)
- 멀웨어 유포의 92% 이상이 이메일을 통해발생 (Trend Micro, 2021)
- 랜섬웨어 원인의 55% 이상이 이메일을 통해 감염 (Datto, 2020)

사칭메일	스피어피싱	스캠	웨일링	BEC
누구나 신뢰하는 발신자	수신자만이 알고 있는 발신자	수신자를 협박하는 메일	CEO(임원) 등 업무 지시	이력서, 발주서, 대금요청

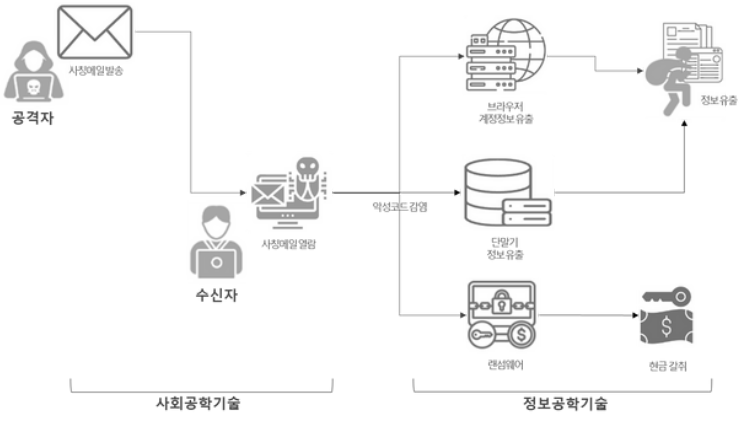
BEC공격의 이해

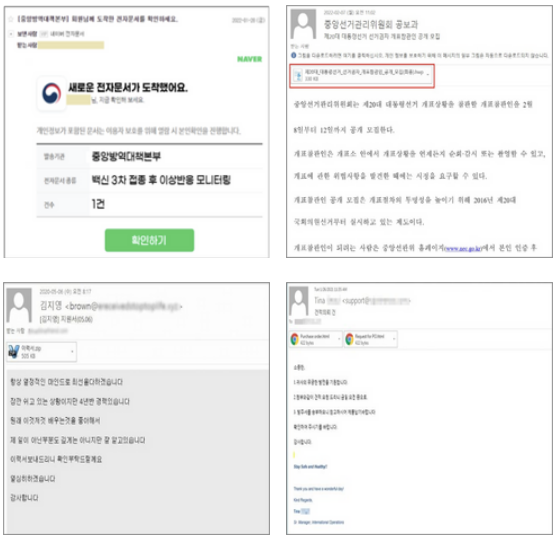
- 사칭메일은 수신자를 속이고 메일을 열람하도록 조작하여 만들어진 사기메일, 가짜메일입니다
- 발신자와 메일 내용에 따라 **'송금 사기', '협력사 사칭', '이력서 사칭', '견적서 사칭', '자문 요청 사기'** 등 다양하게 불립니다 **(사회공학기술)**
- 침해사고에 따라 **'송금 사기', '랜섬웨어 감염', '멀웨어 감염', '계정 탈취', '내부정보 유출'** 등 다양하게 불립니다**(정보공학기술)**
- BEC공격은 **'금전적인 이득'** 이 목적입니다

BEC공격 시나리오

#1 - 사회적 이슈, 비즈니스 내용을 사칭

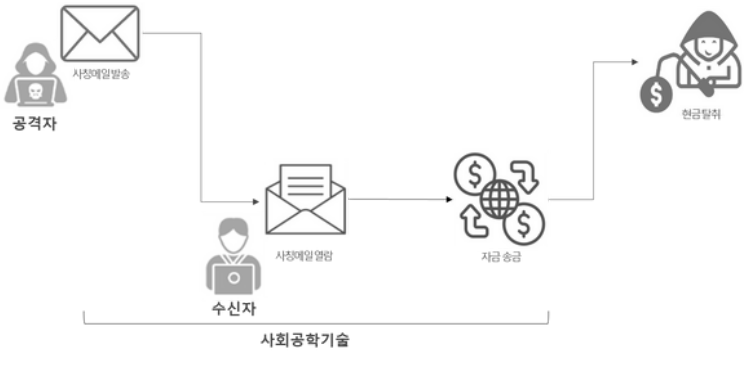
'코로나19 백신 접종 안내', '입사 지원 합니다.', '발주서를 첨부합니다.' 등

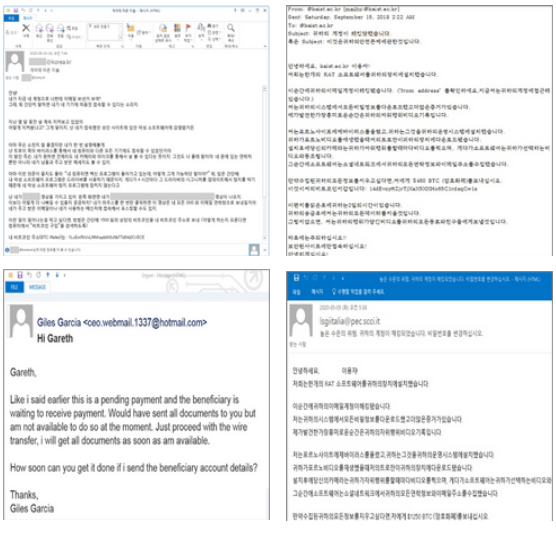




#2 - 스캠, 웨일링, 협박

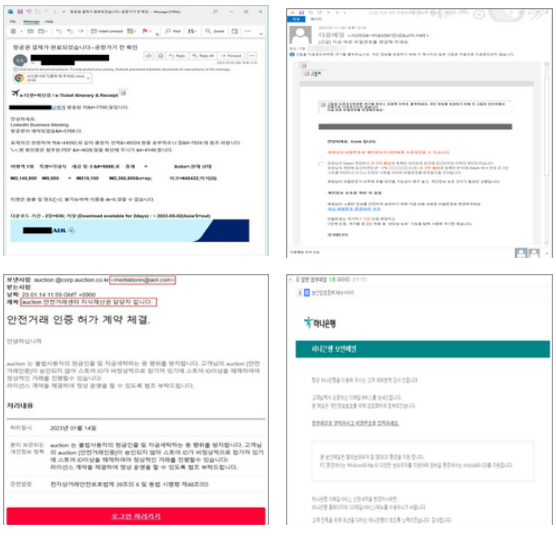
'귀하의 계정이 해킹되었습니다.', '대금 지급에 대한 계좌 변경', 'CEO의 업무 지시' 등





#3 - 금융기관, 고객센터, 관리자 사칭

'보안메일을 확인하세요.', '비밀번호를 변경해 주세요', 'e-티켓을 확인해 주세요' 등



국정원 인증과 우수특허 혁신기술로인정받은 사칭메일관리시스템

RealMail

리얼메일은 사칭메일, 피싱메일, 스피어피싱 등 을 탐지하여 멀웨어, 랜섬웨어, 악성링크를 원천 차단하는 **새로운 메일보안솔루션**입니다.

BEC공격은 사용자가 수신메일을 신뢰하도록 조작한 **사기메일, 가짜메일**입니다.

리얼메일은 **Zero Trust기술**로 **사설메일서버를 통해 만들어진 가짜 메일을 탐지**하여, **BEC공격을 차단**하는 **사칭메일관리시스템**입니다.

컴플라이언스

정보보호 기본지침

제 77조 (전자우편 보안)
. 출처가 불분명한 메일 열람 금지

정보통신망법

제 6장 (정보통신망의 안정성 확보)
. 정보통신망의 안정성 및 신뢰성 확보

국가사이버안전관리규정

제 9조 (사이버안전대책의 수립)
. 사이버안전대책을 수립,시행

기대효과

BEC공격 차단

사칭메일, 피싱메일
스피어피싱, 유사도메인
스캠, 웨일링

불법 메일 차단

불법 성인 광고
불법 도박 광고
협박 메일

메일보안 강화

출처가 불분명한 메일 차단
발신자가 조작 된 위험 메일 차단
사용자 부주의 메일 사고 방지

주요기능

사칭메일 차단

- 상급기관을 사칭한 메일
- 계열사(협력사)를 사칭한 메일
- 임원(관리자)을 사칭한 메일
- 자신을 사칭한 협박 메일
- 업무 관련 사기 메일
- 무역 대금 사기 메일

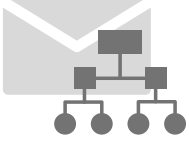
피싱메일 차단

- 사회적인 이슈를 이용한 피싱 메일
- 자문 요청 피싱 메일
- 은행 거래 통지 피싱 메일
- 설문조사 피싱 메일
- 배송/택배 배송 피싱 메일
- 발주서, 이력서 등 피싱 메일

메일서버 검증

- 발신 전용 메일 서버 검증
- 수/발신이 다른 메일 서버 검증
- 메일 서버 설정 검증
- 발신 계정의 진위 여부 검증
- 수신자 계정 검증
- 휴면 계정 검증

수신메일 분류



- 국가별 발신 메일 분류
- 발신 전용 메일 분류
- 발신 전용 계정(no-reply) 분류
- 수/발신이 다른 메일 분류
- 메일서버 설정에 따른 분류
- 메일 분류 알고리즘 특허

컨텐츠 무해화

(별도의라이선스 필요)

- 파일 위/변조 탐지
- 컨텐츠 및 파일 무결성
- 파일에 대한 실시간 무해화
- 60여 가지의 파일 포맷
- 멀웨어, 랜섬웨어 공격 차단
- Zero-Day 공격 차단

메일 보안

- SPF, DKIM, DMARC 적용
- 멀티 RBL 적용
- 국가 별 메일 차단
- 키워드 필터링
- 미리보기 및 이미지 변환
- 출처가 불분명한 메일 차단

관리자 기능

- 실시간 메일 모니터링
- 수신자에게 메일 재전송 기능
- 수신메일에 대한 다양한 분석
- 특정 기간 별 통계 분석
- 수신 메일 저장, 백업
- 보안정책 및 DB 백업

부가 기능

- Bridge, Proxy 구성 지원
- 이중화(HA) 구성 지원
- White/Black 자동 등록
- 그룹 별 정책 지원
- 이메일 역추적 검사
- 메일 헤더 검사

SPEC

메일처리량 (일)	30만 통 이하	60만 통 이하	60만 통 이상
H/W	CPU : Xeon 3.2 Ghz, 8 Core 이상 RAM : 128 GB 이상 Storage : SSD 250G, HDD : 1 T 이상	CPU : Xeon 3.2 Ghz, 12 Core 이상 RAM : 128 GB 이상 Storage : SSD 250G, HDD : 1 T 이상	CPU : Xeon 3.2 Ghz, 16 Core 이상 RAM : 128 GB 이상 Storage : SSD 250G, HDD : 1 T 이상
S/W	CentOS 7.9.2009 / Kernel 3.10.0-1062 / MariaDB 10.4.25 / Chrome (브라우저)		
기타	CDR 적용 시 H/W 사양 별도 산정		

서울특별시 금천구 가산디지털1로 205-27, 811호(가산동, A1타워)
부산광역시 해운대구 센텀북대로 60, 804 (재송동, 센텀IS타워)
Tel : 051-552-9118 | sale@realsecu.net | www.realsecu.net