Digital Transformation Partner

kt Secure 지능형위협메일차단

서비스 소개

kt Enterprise

Intro - 기업 대상 메일 위협

증가하는 악성 이메일 공격으로 심화 중인 기업 피해

최근 이메일을 통한 해킹수법이 고도화되고 지능화 되며, 기업 대상 이메일을 통한 사이버공격 피해가 매년 빠르게 증가하고 있습니다.
'22년 침해사고 분석 결과, 악성코드 공격의 75%가 이메일을 통해 전파되며,
특정 기업을 타겟한 사칭·위장 메일 또한 고도화 되어 기업에 막대한 금전적·영업적 피해를 끼치고 있습니다.

고객사칭 이메일 랜섬웨어 감염으로
콜센터 3일 업무정지
('19.12)

사칭메일 유포
고객 개인정보 수만 건 유출
('19.12)

위장메일에 오송금
61억원 금전적 손실
('20.03)

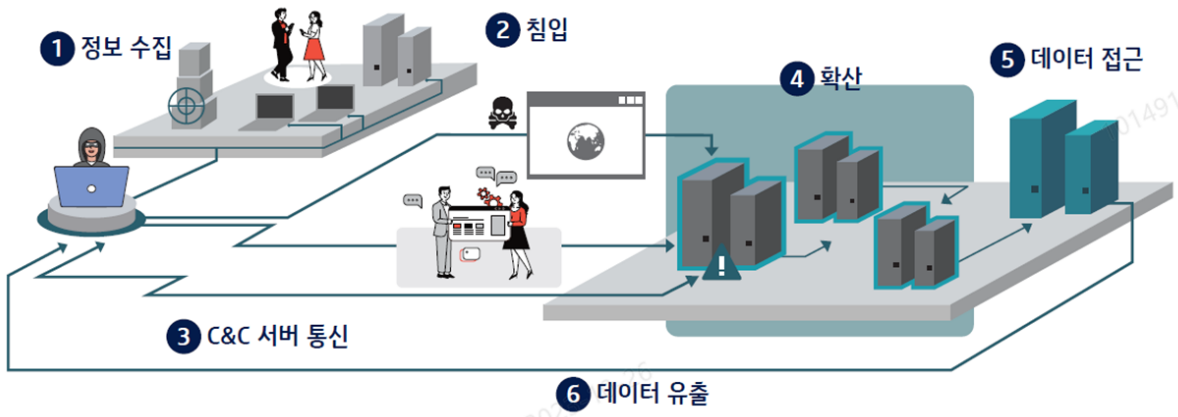
코로나19 發 해킹
중형 기업 총 1,100억원 피해
('21.08)

Intro - 메일 공격의 지능화 · 고도화

기존 솔루션 만으로는 방어할 수 없는 APT 공격

APT는 지능적이고 지속적인 공격(Advanced Persistent Threat)의 약자로, 최근 국내에서 연이어 발생했던 APT 공격 사례로는 은행 전산망 마비, 카드사, 포털사이트, 대형게임사 대상 개인정보 유출 및 랜섬웨어 배포 등이 있었습니다.

APT 공격 경로



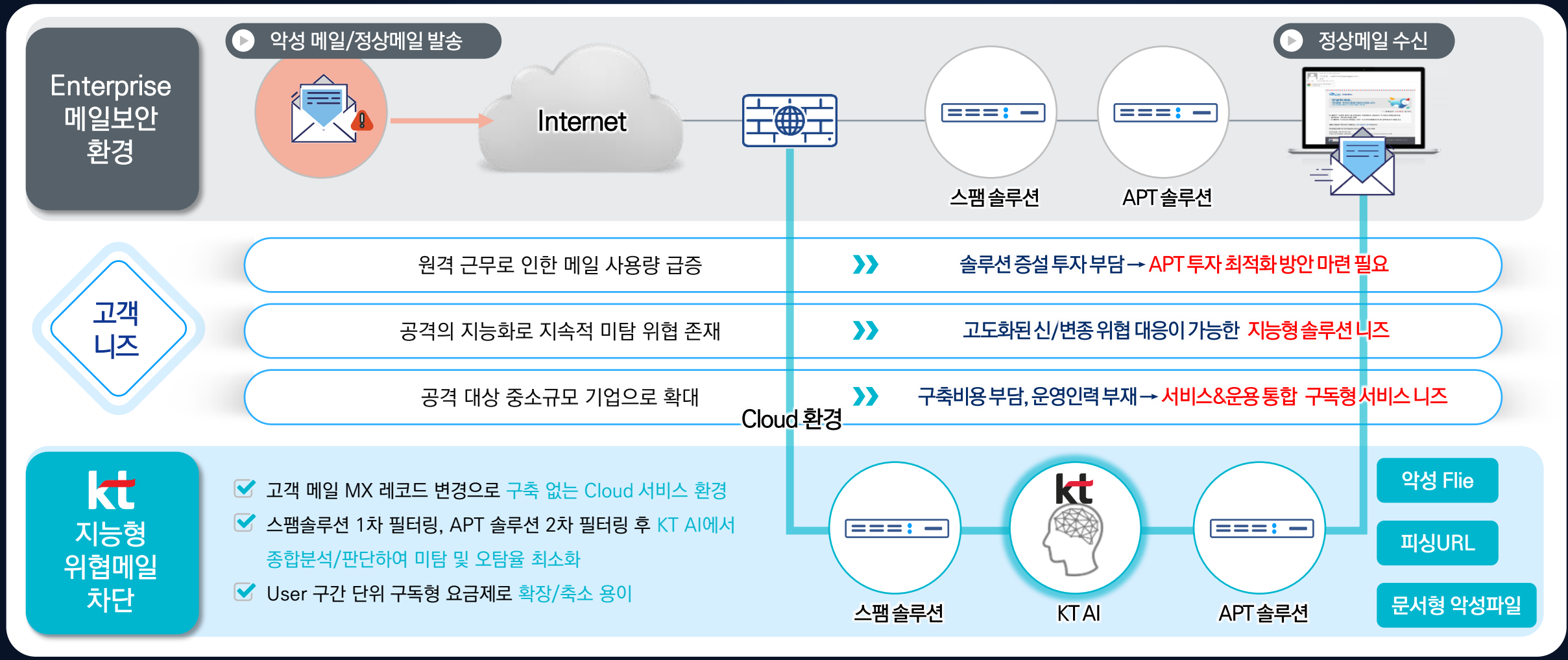
1. 정보 수집: 타깃 정보 수집 후 사칭 이메일로 위장하여 악성코드 배포
2. 침입: 의심없이 첨부파일 열람, 악성코드 감염
3. C&C서버 통신: 백도어 프로그램 설치하여 해커서버와 통신, 원격에서 명령 전파
4. 확산: 내부 PC로 악성코드 전파, 사내 접근 권한 탈취하여 점차 높은 권한 획득
5. 데이터 접근 및 유출: CORE 데이터 접근, 유출 및 파괴

Secure 지능형위협메일차단 서비스란?

KT Bigdata 기반의 AI탐지엔진을 적용하여,
지능화 · 고도화 된 신종 위협 메일로부터
기업 자산을 안전하게 지킬 수 있으며
별도 장비구축 없이 서비스형으로 이용할 수 있는
구독형 AI 메일보안 솔루션입니다.

KT 지능형위협메일차단 서비스 소개

KT Bigdata 기반 AI 분석 기술로 더욱 강력해진 기업 위협 메일 차단 솔루션, KT 지능형위협메일차단 서비스



서비스 구성

서비스 레벨에 따라 Basic, Premium 선택 가능

Basic

Basic 서비스

SPAM솔루션(Working Hour 대응)
+ APT 1종

Premium

Premium 서비스

SPAM솔루션(24H/365D 대응)
+ APT 1종

+

Option

*** 샌드박스란**

가상환경을 만들어 그 안에서 악성파일을 실행시켜보고, 무슨 행위를 하는지 지켜본 다음 악성여부를 판단하는 솔루션입니다.

APT 1종 추가

APT 1종 추가로 멀티샌드박스 적용

적용 기술 ① AI PE 탐지/차단

악성파일을 이미지 변환 후 탐지하는 방식으로, 기존 Sandbox(동적분석)대비 변종 악성코드 탐지속도 180배 향상, 벡터 기반 유사도 측정 방식으로 다양한 변종 공격도 높은 정확도로 탐지

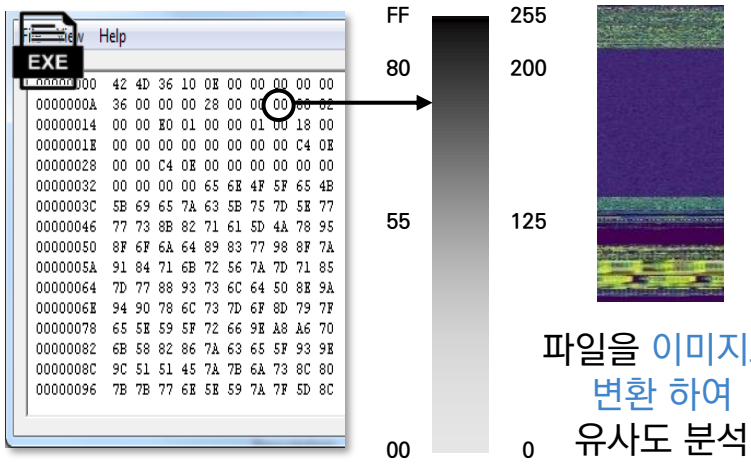
PE 이미지 변환 통한 AI 탐지 방식 적용

AI가 가장 잘하는 이미지 분류 탐지 방식 적용

행위 없이 이미지 AI 판단으로 탐지속도 향상

딥러닝(128 Layer)기반의 백터 치환 유사성 비교

이미지 변환 처리 방식으로 행위를 기다릴 필요 없이
빠르게 악성여부 판단



파일을 이미지로 변환 하여
유사도 분석

노란색 표본에 가까울 수록 악성 확률 高

(19년 5월 7일)
갠드크랩5.2 (랜섬웨어)

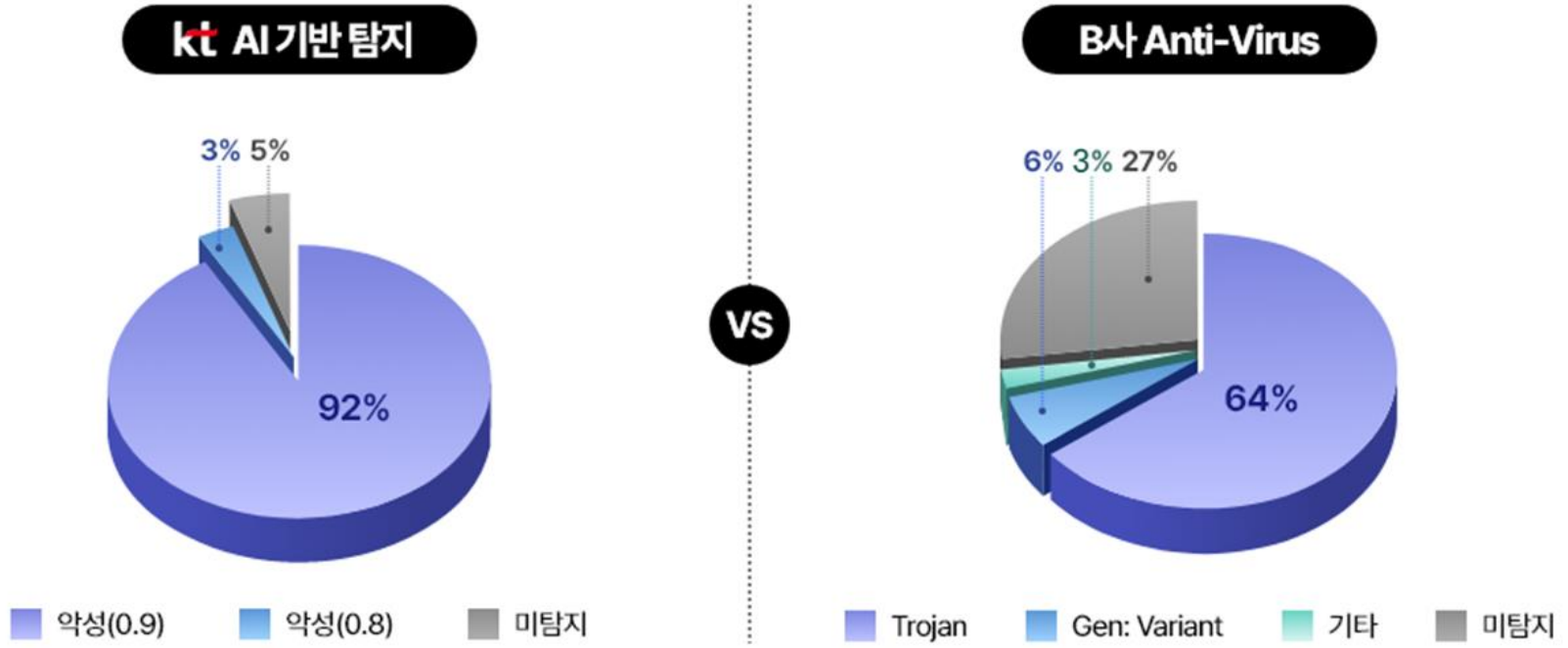
(19년 5월 28일)
소디노키비 (랜섬웨어)

(19년 5월 31일)
소디노키비 (랜섬웨어)

적용 기술 ① AI PE 탐지/차단

- 국내 특화 DB 적용으로 KT AI 모델(95%)은 글로벌 B사 Anti-virus(73%) 대비 22% 높은 악성 탐지율 확인

KT 이메일 서비스로 유입된 악성코드 2,286개 대상 탐지율 비교



- 괄호 안 Score가 1.0에 가까울수록 악성파일과의 유사도가 높은 탐지건으로, 악성파일로 분류

적용 기술 ② AI 변종 피싱 URL 탐지

✔ 피싱 사이트 유사성 분석 AI모델로 기존 시그니처에서 대응할 수 없는 변종 피싱 URL 탐지

기존 방식의 한계

해커의 공격 수법

- 동일한 피싱 사이트로 유도하는 공격 수행시, 매번 다른 URL 주소와 본문 내용으로 메일 전송

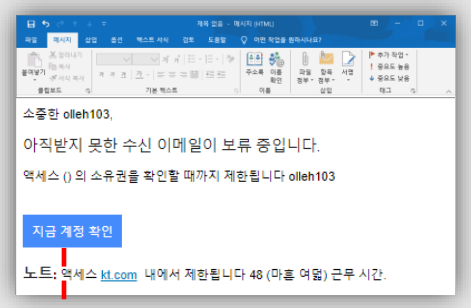
기존 시그니처의 한계

- 위협 문자열 등록 후 해당 문자열이 매칭되는 경우 위협으로 판정하는 기법은 공격자가 내용을 변경하여 전송하는 경우 탐지 불가

AI 를 통한 변종 공격 탐지

기존 패턴 기반 탐지

Subject :
귀하의 사서함 저장 공간이 부족합니다

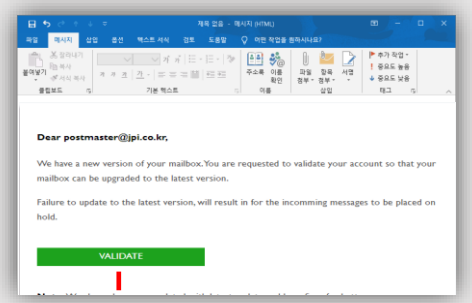


https://www.eas*a*p.com.tw/wp-content/uploads/fusion-scripts/mode/cloud.php

≠

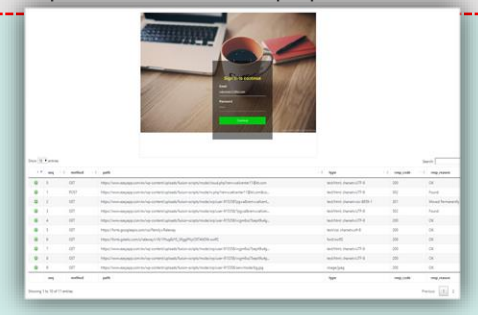
본문 내용과 URL 주소는 매번 변형되어
패턴 기반으로 탐지 불가

Subject :
Validate Mailbox Now



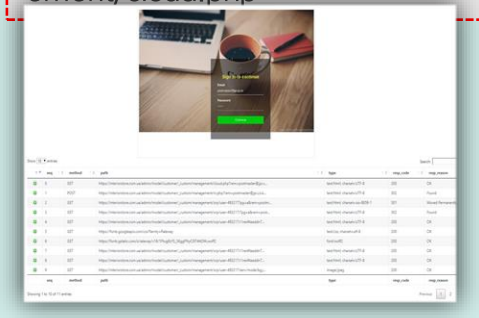
https://in*erio*s*ore.com.ua/admin/model/customer/_custom/management/cloud.php

AI 기반 탐지



=

사람이 해당 사이트를 클릭해서 유사성을 파악하는 것과 유사한 구조로,
동일 사이트로 판별

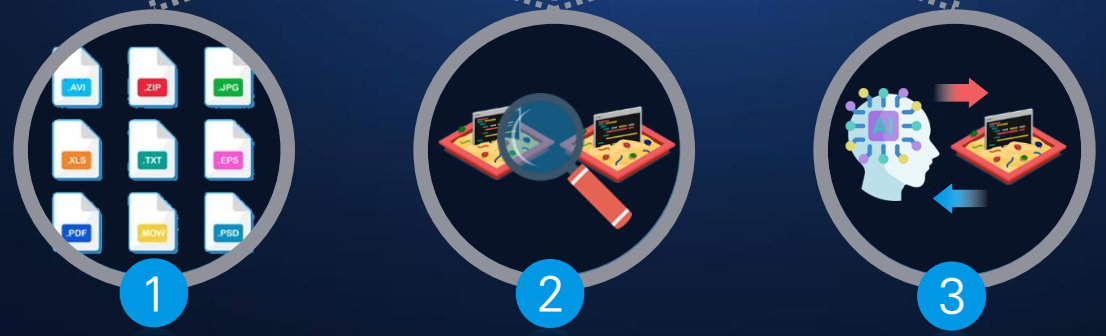


적용 기술 ③ 멀티 샌드박스 탐지/차단

✔ 멀티 샌드박스 구성 및 특성에 따라 최적의 동적 행위 분석 및 스코어링을 통한 악성 판단 자동화 구현으로 오탐지 최소화

kt 지능형 위협메일 차단

APT #1 APT #2 APT #3



01 실제 PC 유사 환경 파일 실행

- WIN 7, 10, 11 지원
- MS Office, 한글 HWP 포함 (공식 라이선스)
- Edge, Chrome 브라우저
- 실제 파일 실행 스크린샷 제공

02 프로세스 행위 분석

- 행위 정보 (악성/일반)
  파일, 프로세스, 레지스트리, 스레드, 디스크, 디렉터리, 디버깅, 후킹, 라이브러리, 메모리, 익스플로잇, 암호화 등
- 웜, 트로이목마
- 다운로더, 스파이웨어 등

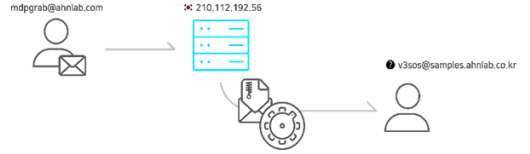
03 네트워크 행위 분석

- API 호출 / C&C 서버 호출
- TCP/UDP/HTTP/HTTPS
- URL 분석 / 이상 트래픽 식별
- PACP 파일 다운로드 제공

04 Dropped 파일 분석

- 이벤트로 인해 생성된 파일 정보
- 특정 파일 핀포인트 분석 제공

05 공격 흐름도 분석



06 분석 요약 / 레포트 제공

- 위험도: High, Medium, Low, Grey 등
- 진단명, 감염 경로, 탐지 대상, 공격자
- 백신 진단 내역
- 탐지 원인 및 대응방안 제공

특성에 맞춘 샌드박스	오탐지 최소화	회피기술 무효화
URL, PE, 압축파일, Script, 문서파일 별 샌드박스 분리 검사	멀티 샌드박스 결과를 활용한 스코어링, 종합 판정	AI 분석과 행위 분석 교차 검증 진단 회피 기술 무효화

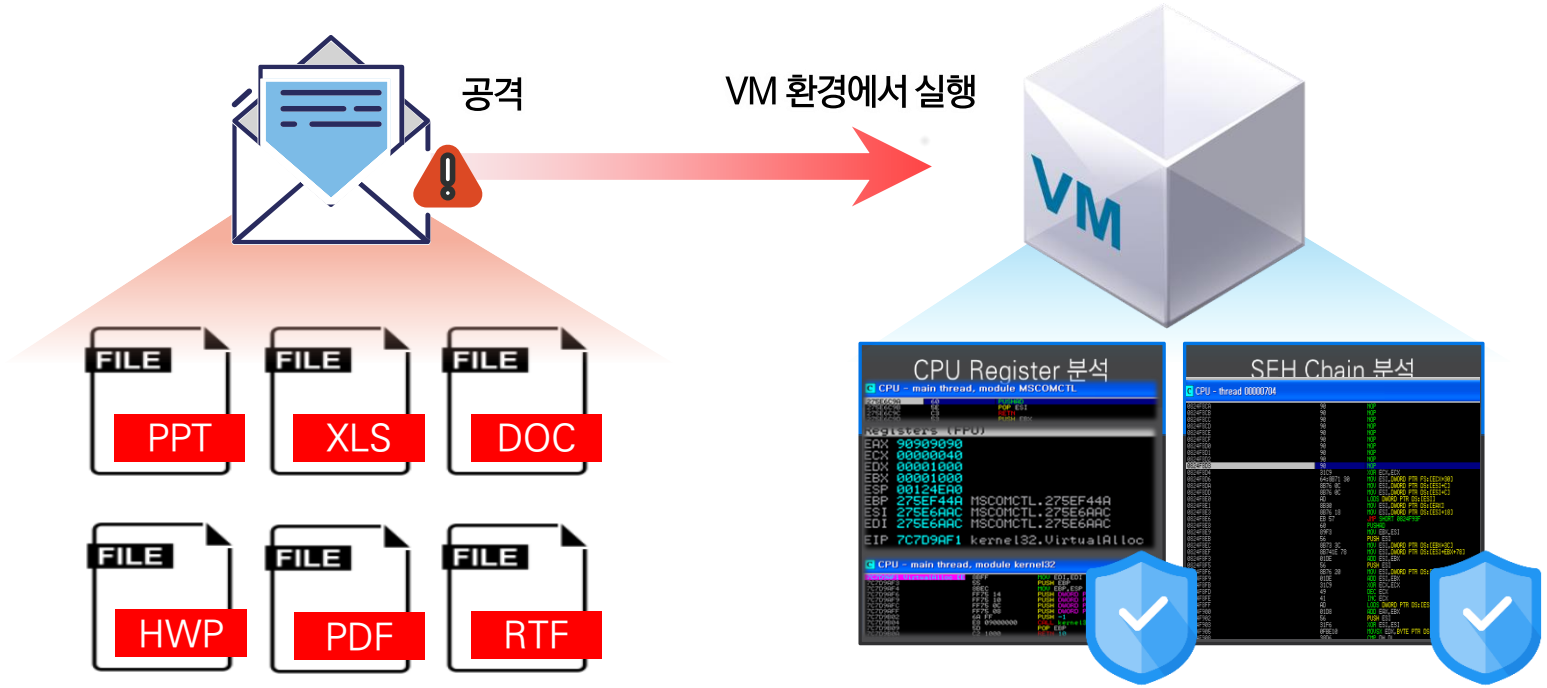
적용 기술 ④ 문서형 악성파일 탐지기술 적용

문서형 파일에 대한 어셈블리 레벨 분석으로 알려지지 않은 악성코드를 정확하게 탐지

어셈블리 레벨 진단을 통한 문서파일 탐지

문서 형태의 악성 파일 발송

가상환경에서 실행된 기계어를 어셈블리 레벨에서 진단하여 악성 파일 탐지



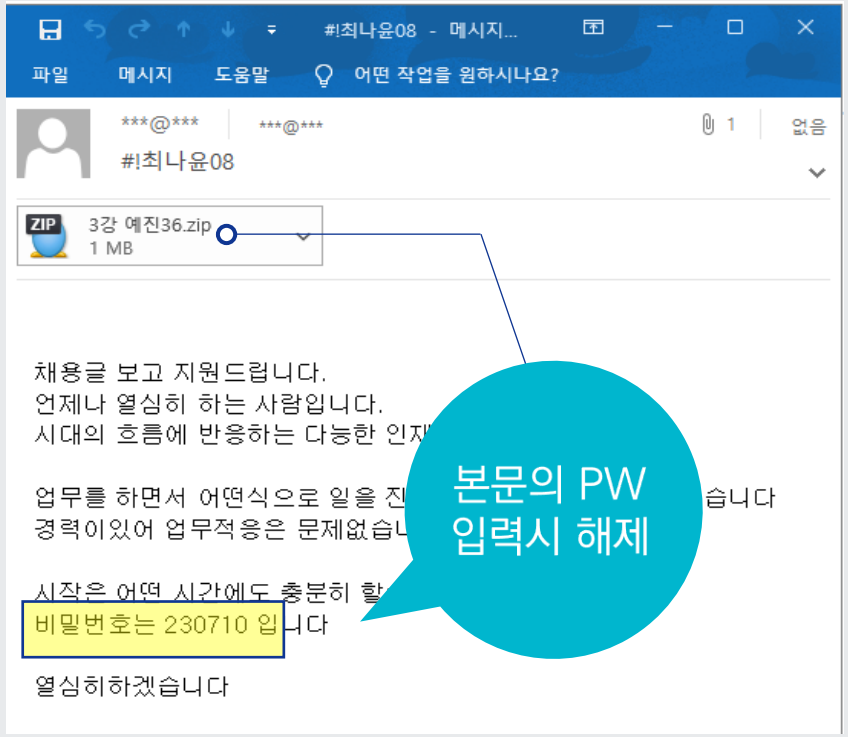
- MS-Office, PDF, RTF, HWP(한글) 정식버전 문서에 대한 분석 지원
- 가상환경 회피 기술인 Sleep 모드 탐지 가능
- 문서 내 숨겨진 문서에 대한 악성코드 탐지가 가능
- 문서 내 삽입 된 이미지에 대한 악성코드 탐지, 분석이 가능

4. KT의 AI 보안모델

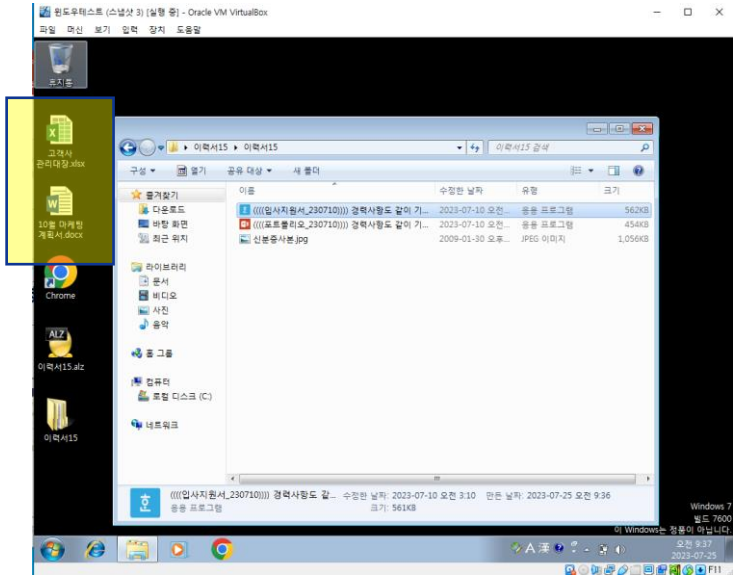
- 입사지원서를 사칭 LocKBit 랜섬웨어 최근 활발하게 유포 中, 보안솔루션 회피를 위해 암호화 압축 파일을 사용

Attack Case 01 – Lock bit 랜섬웨어

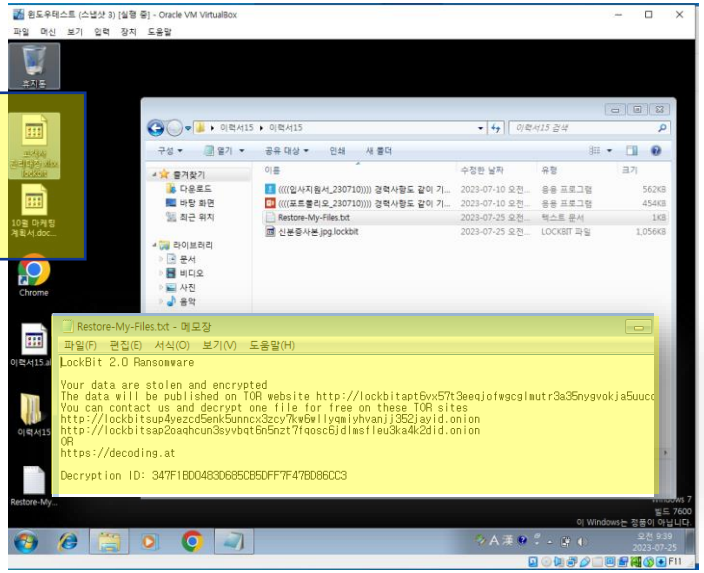
- K社 PoC결과 1개월간 총 4건의 랜섬웨어 공격을 차단
- KT AI 보안 플랫폼은 비밀번호 자동 추출 및 적용, 압축해제 후 악성 여부 판단



[워드 문서로 위장한 LockBit 랜섬웨어 실행 전]



[실행 후: 파일 암호화 후 금전요구 노트 생성]



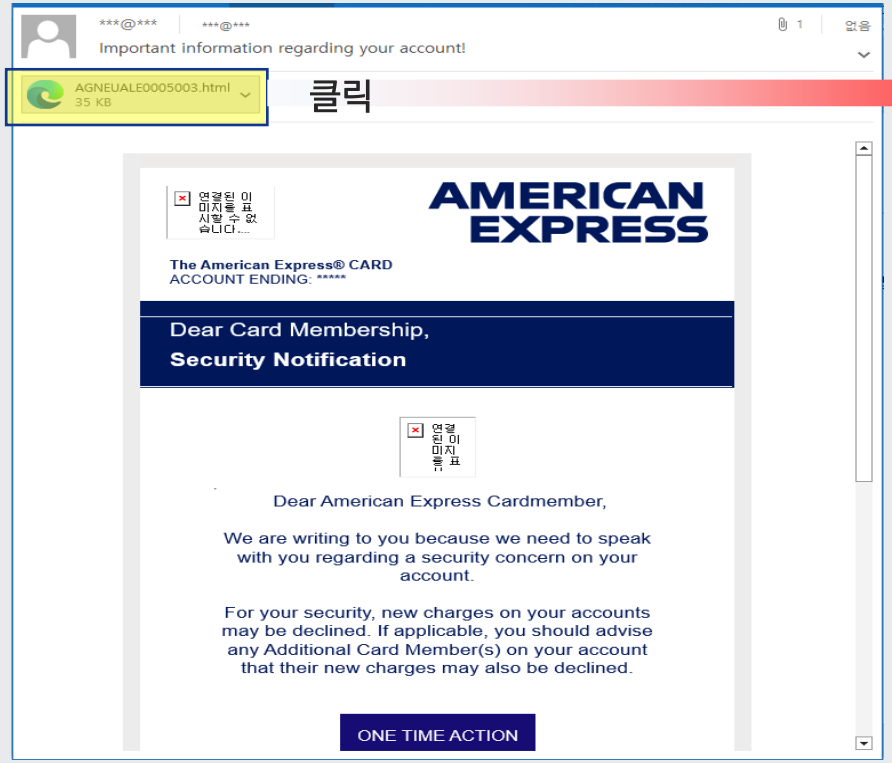
4. KT의 AI 보안모델

4-3) 공격 차단 사례- 카드회사 피싱메일 차단

HTML 파일 이용 피싱 메일, 실제 웹 페이지 동일 레이아웃과 디자인으로 사용자 개인 정보를 탈취

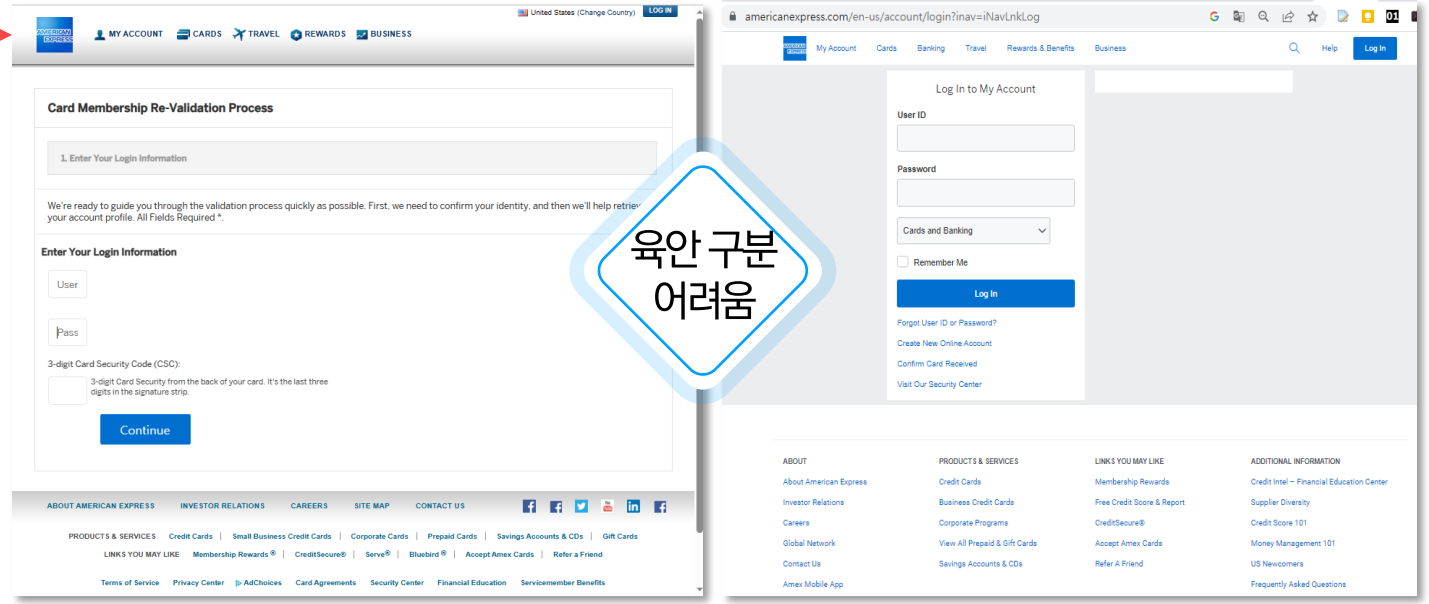
Attack Case 02 – 카드회사 피싱메일

- A社 PoC결과 개인정보 탈취 피싱 공격 다수 차단
- AI는 첨부 html 파일을 분석하여 숨겨진 악성 URL을 탐지



[개인 정보 탈취를 위해 만든 피싱 사이트]

[americanexpress.com 오리지널 사이트]



탈취된 계정정보로 소셜 엔지니어링 기법과 결합, 개인화된 정보를 더욱 위력적인 2차 공격에 활용

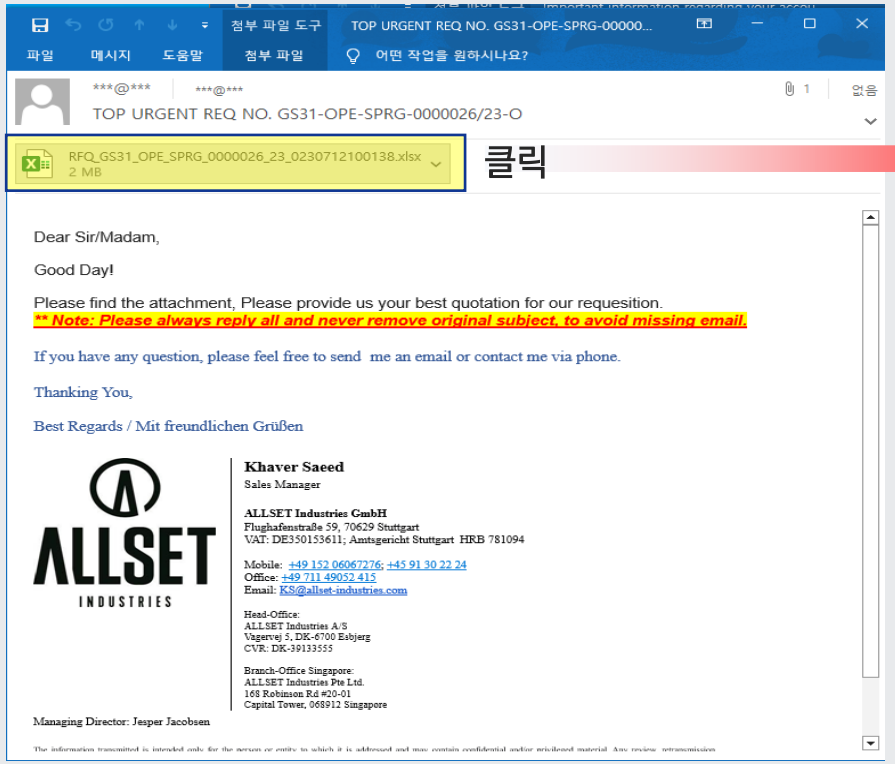
4. KT의 AI 보안모델

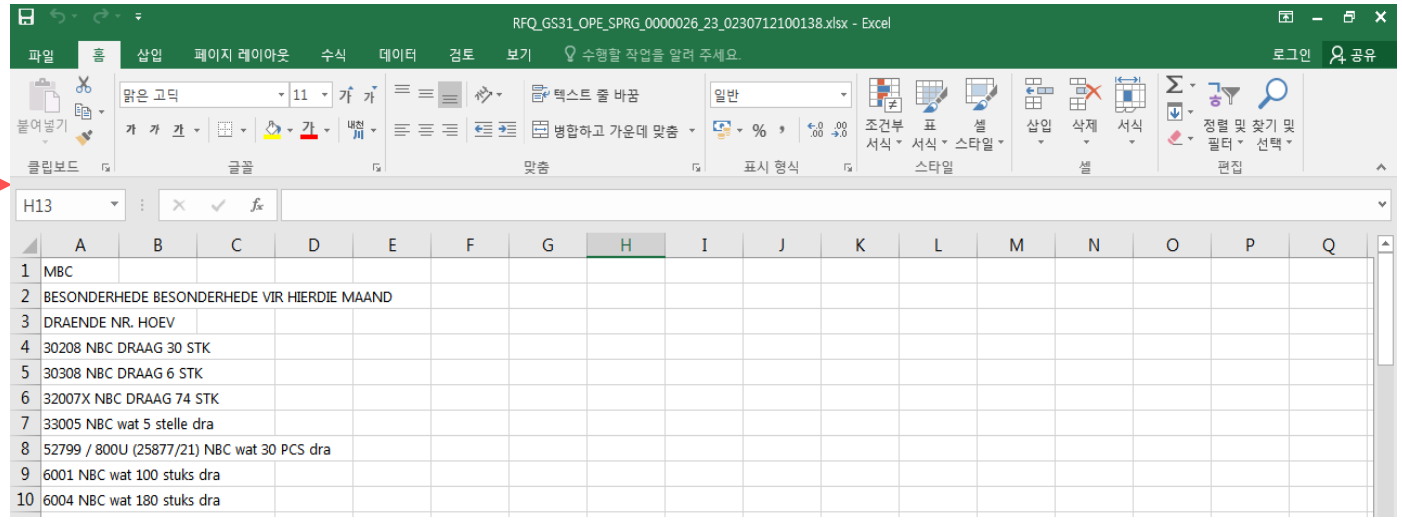
4-3) 공격 차단 사례- 문서파일을 이용한 공격

✔ 주 이용 문서(doc, pdf, hwp 등) 내에 악성스크립트를 숨겨 보안 솔루션 우회 및 성공율이 높은 APT공격

Attack Case 03 – 비실행형 악성문서

- C社 서비스 고객의 MS의 수식편집기의 취약점을 이용한 악성 문서 차단
- 정상적인 엑셀 파일처럼 위장한 비 실행형 악성파일





- MS Equation Editor 컴포넌트 취약점(CVE-2018-0798)을 악용하여 엑셀 파일을 오픈 하는 동시에 추가적인 악성코드를 다운로드 후 실행
- 해당 엑셀파일은 http://87.121.221.212:80 로 접속 시도하여 파일 다운로드 시도

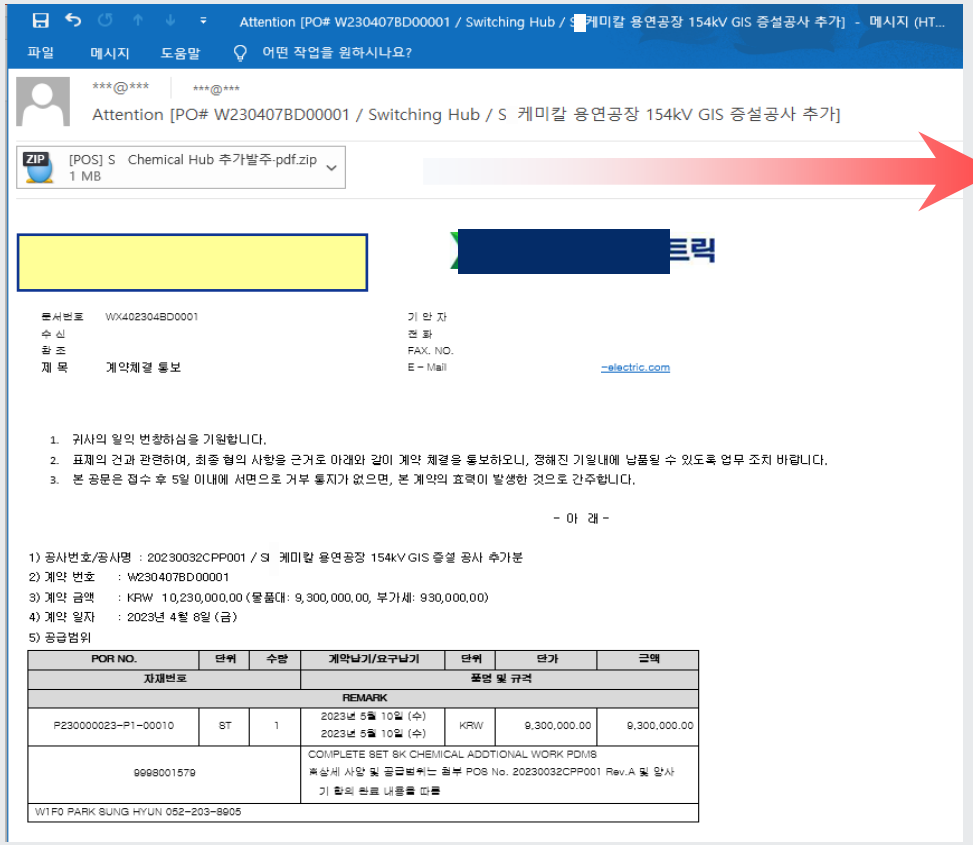
4. KT의 AI 보안모델

4-3) 공격 차단 사례- 국내 대기업 사칭 발주 메일(1)

✔ 주 이용 문서(doc, pdf, hwp 등) 내에 악성스크립트를 숨겨 보안 솔루션 우회 및 성공율이 높은 APT공격

Attack Case 04 – 대기업 사칭 메일(1)

☑ 대기업 사칭 발주 메일 – 보안솔루션 우회를 위해 디지털 서명 사용


Attention [PO# W230407BD00001 / Switching Hub / S 케미칼 용연공장 154kV GIS 증설공사 추가] - 메시지 (HT...

파일 메시지 도움말 어떤 작업을 원하시나요?

@ ***@***

Attention [PO# W230407BD00001 / Switching Hub / S 케미칼 용연공장 154kV GIS 증설공사 추가]

[POS] S Chemical Hub 추가발주-pdf.zip
1 MB

[redacted]트릭

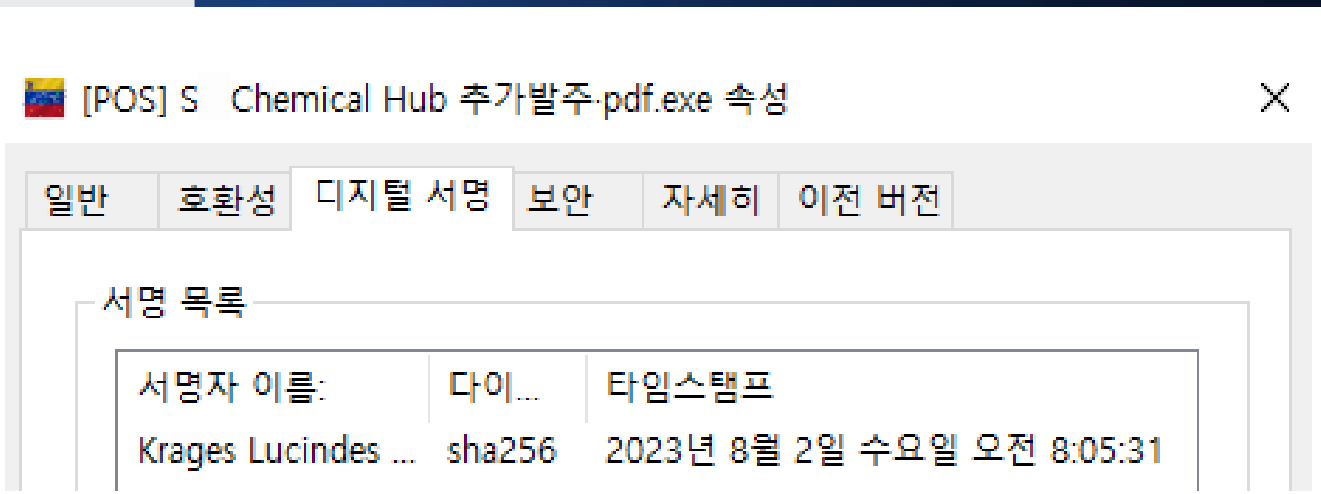
문서번호 WX402304BD0001 기 안 자
수 신 전 화
참 조 FAX. NO.
제 목 계약체결 통보 E-Mail [redacted]-electric.com

1. 귀사의 일익 번창하심을 기원합니다.
2. 표제의 건과 관련하여, 최종 협의 사항을 근거로 아래와 같이 계약 체결을 통보하오니, 정해진 기일내에 납품될 수 있도록 업무 조치 바랍니다.
3. 본 공문은 접수 후 5일 이내에 서면으로 거부 통지가 없으면, 본 계약의 효력이 발생한 것으로 간주합니다.

- 아 래 -

1) 공사번호/공사명 : 20230032CPP001 / S 케미칼 용연공장 154kV GIS 증설 공사 추가분
2) 계약 번호 : W230407BD00001
3) 계약 금액 : KRW 10,230,000,00 (물품대: 9,300,000.00, 부가세: 930,000.00)
4) 계약 일자 : 2023년 4월 8일 (금)
5) 공급범위

POR NO.	단위	수량	계약납기/요구납기	단위	단가	금액
자재번호			품명 및 규격			
REMARK						
P230000023-P1-00010	ST	1	2023년 5월 10일 (수) 2023년 5월 10일 (수)	KRW	9,300,000.00	9,300,000.00
9998001579			COMPLETE SET 8K CHEMICAL ADDTIONAL WORK PDMS ※상세 사양 및 공급범위는 첨부 POS No. 20230032CPP001 Rev.A 및 양사 기 합의 된 내용을 따름			
W1F0 PARK SUNG HYUN 052-203-8905						



☑ 보안 솔루션 우회를 위해 디지털 서명 사용
(일부 솔루션에서 서명 검증 없이 존재 유무로만 검사를 하지 않는 경우를 악용)

☑ 이메일 탐지 시점과 디지털 서명 시간의 Gap이 적은 것으로 보아 공격자는 변종 악성코드를 실시간으로 생성 및 이메일로 전송 하여 패턴 기반 탐지 우회 시도

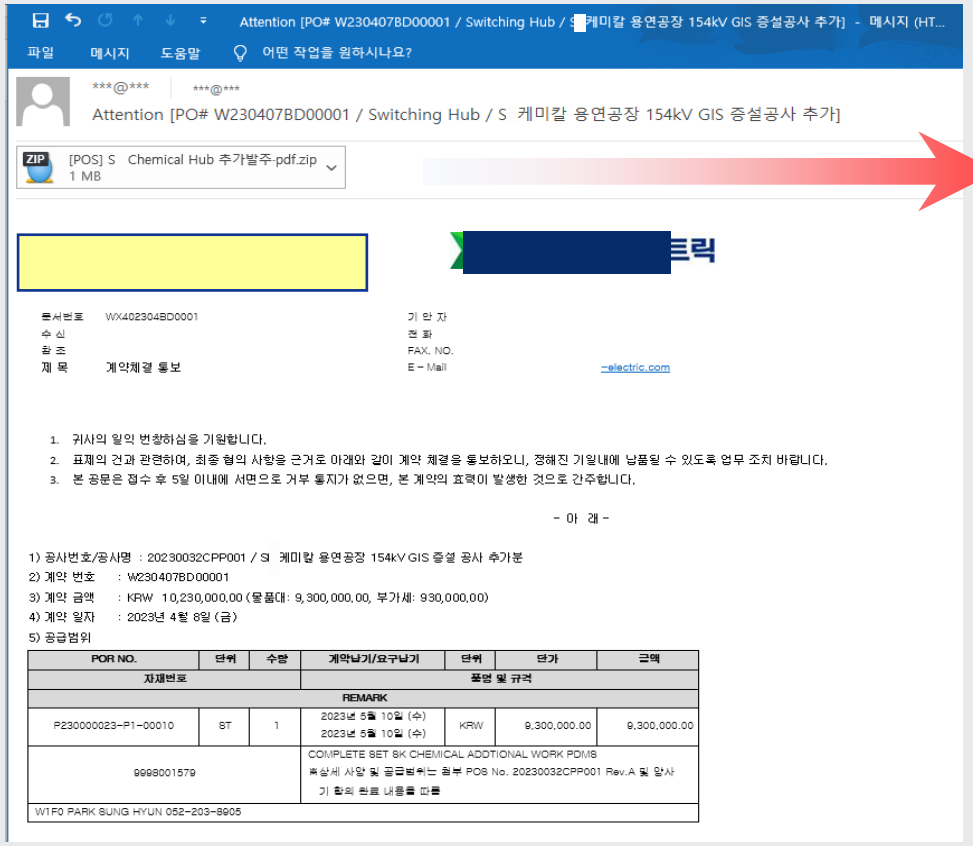
4. KT의 AI 보안모델

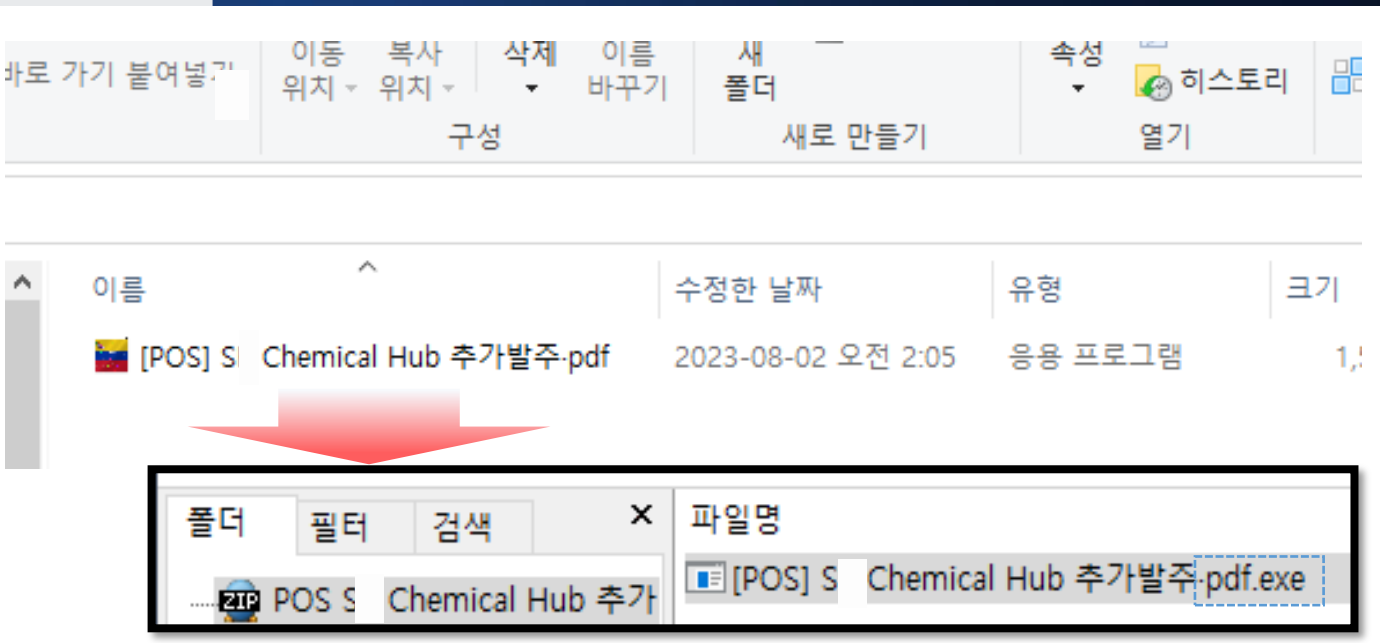
4-3) 공격 차단 사례- 국내 대기업 사칭 발주 메일(2)

주 이용 문서(doc, pdf, hwp 등) 내에 악성스크립트를 숨겨 보안 솔루션 우회 및 성공율이 높은 APT공격

Attack Case 04 – 대기업 사칭 메일(2)

대기업 사칭 발주 메일 – 이중확장자 이용하여 실행 유도





이중 확장자를 사용하여 실제 exe(PE파일) 을 pdf 파일로 위장

사용자의 부주의를 통해 악성코드 실행 유도