문서로 위장한 알려지지 않은 악성코드 방어 솔루션, 악단홀 PED

1등급 GOOD Software

TTA

AKDAN HALL PED

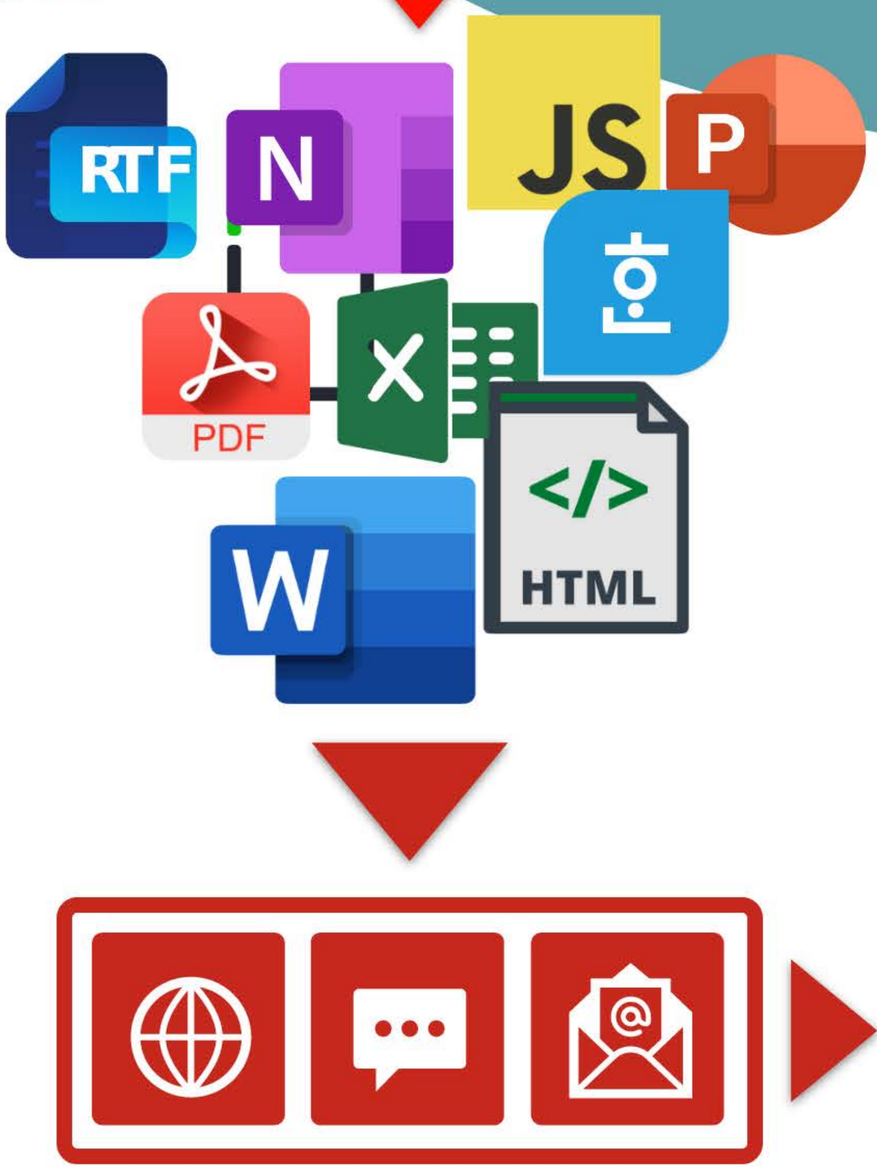
Pre-Execution Detect Solution

백신이 설치되어 있어도 알려지지 않은 악성 문서파일은 막을 수 없습니다.

작성자와 출처를 알 수 없는 문서 파일이 웹, 메신저, 이메일로 공유되고 있습니다.
아무런 의심없이 열어 보고 있다면 당신의 PC는 이미 악성코드에 감염되었을 지 모릅니다.

공격자 → **알려지지 않은** 문서형 악성코드 제작





- 이력서
- 인천광역시 코로나바이러스 대응
- 전자세금계산서
- 용산구 이태원 사고 대처상황
- 한국음악저작협회 저작권 침해 공문
- 사례비지급

사회공학적 공격



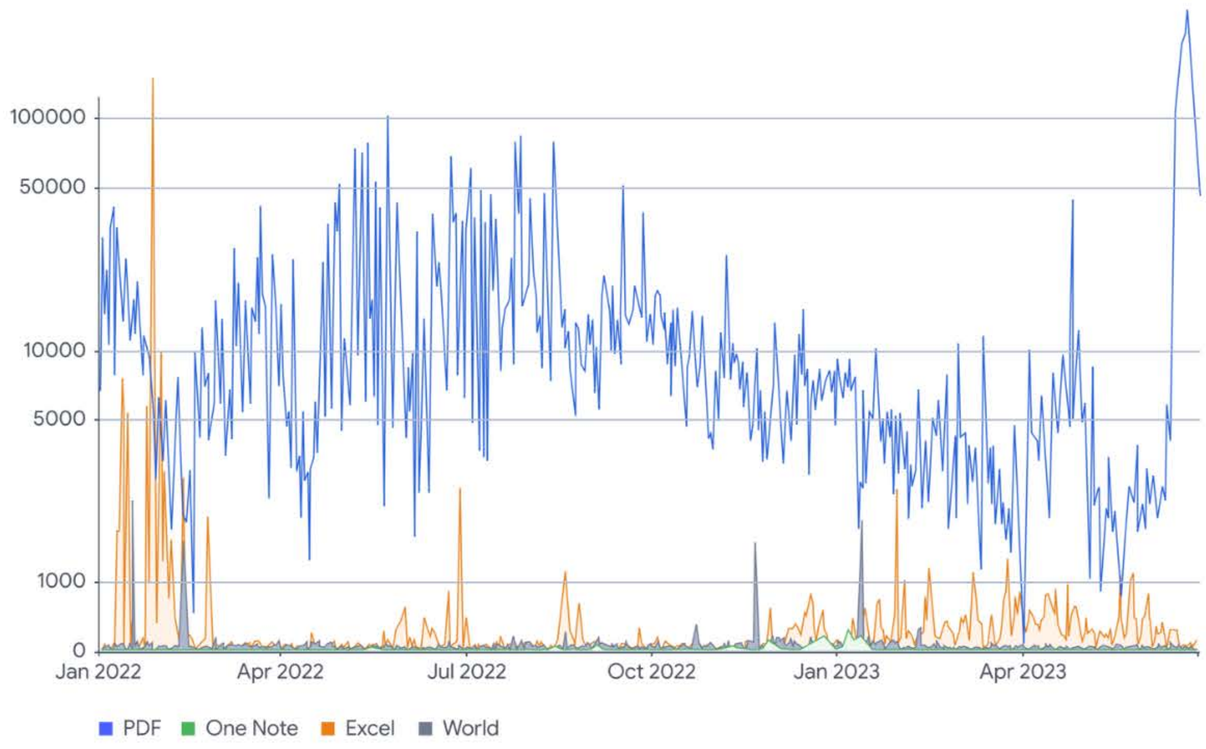
주요 특징

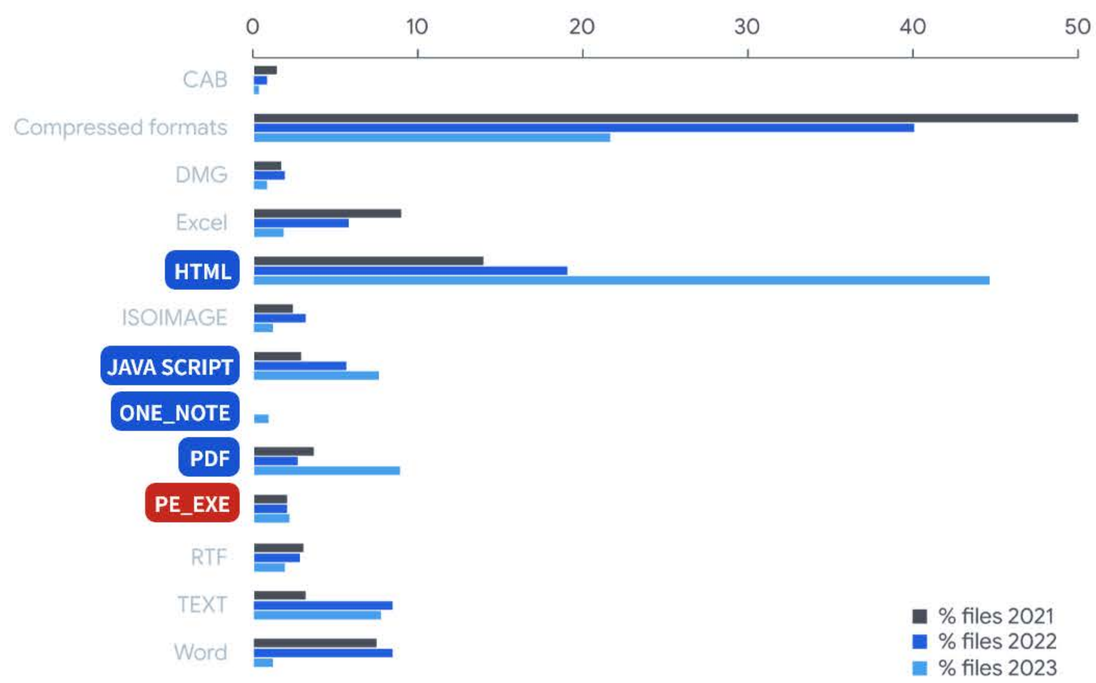
I. 클라우드 분석 서비스
II. 알려지지 않은 위협 탐지
III. 외부 유입 문서의 출처 조회
IV. 상세 분석 보고서 제공

AKDAN MALWARE ARREST TEAM

최신 악성코드 트렌드 | 실행파일 [EXE]형 악성코드는 이제 옛말입니다.

최근 3년간 추세를 보면 그 자리를 문서와 스크립트(HTML,JS)가 차지하고 있습니다.
2023년에는 원노트를 이용한 공격이 새로 등장하기도 했습니다.



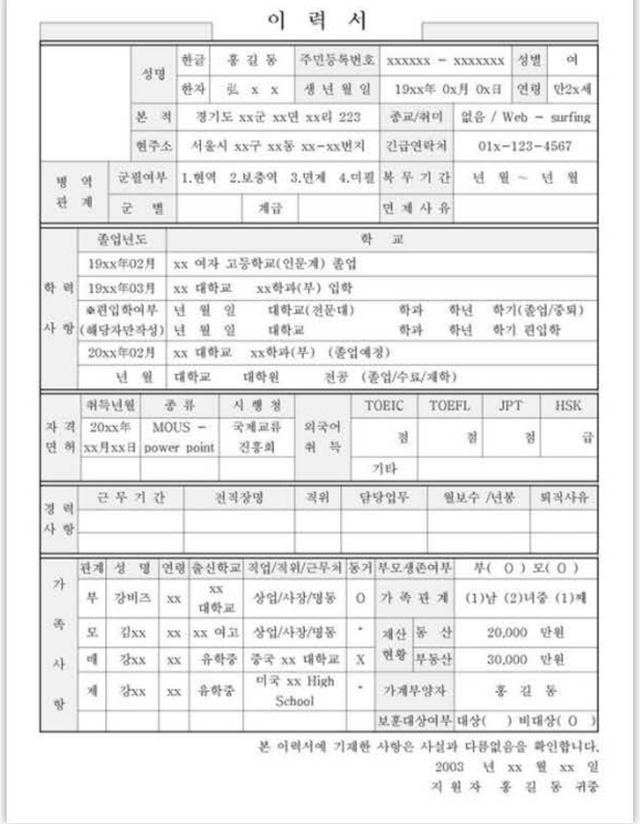


[출처] virustotal 2023emerging

심리적 허점 | 문서는 의심 받지 않습니다.

우리는 외부 문서를 별다른 의심 없이 열어보곤 합니다.
문서는 웹, 메신저, 이메일에서도 걸러지지 않는 가장 흔하게 공유되는 파일입니다.

회사 이력서



이 력 서

	성명	한글	홍 길 동	주민등록번호	xxxxxx - xxxxxxx	성별	여
		한자	弘 x x	생 년 월 일	19xx年 0x月 0x日	연령	만2x세
	본 적		경기도 xx군 xx면 xx리 223		종교/취미		없음 / Web - surfing
	현주소		서울시 xx구 xx동 xx-xx번지		긴급연락처		01x-123-4567
병 역 관 계	군필여부		1.현역 2.보충역 3.면제 4.미필		복 무 기 간		년 월 ~ 년 월
	군 별		계급		면 제 사 유		

	졸업년도	학 교
학 력 사 항	19xx年02月	xx 여자 고등학교(인문계) 졸업
	19xx年03月	xx 대학교 xx학과(부) 입학
	※편입학여부 (해당자만작성)	년 월 일 대학교(전문대) 학과 학년 학기(졸업/중퇴) 년 월 일 대학교 학과 학년 학기 편입학
	20xx年02月	xx 대학교 xx학과(부) (졸업예정)
	년 월	대학교 대학원 전공 (졸업/수료/제학)

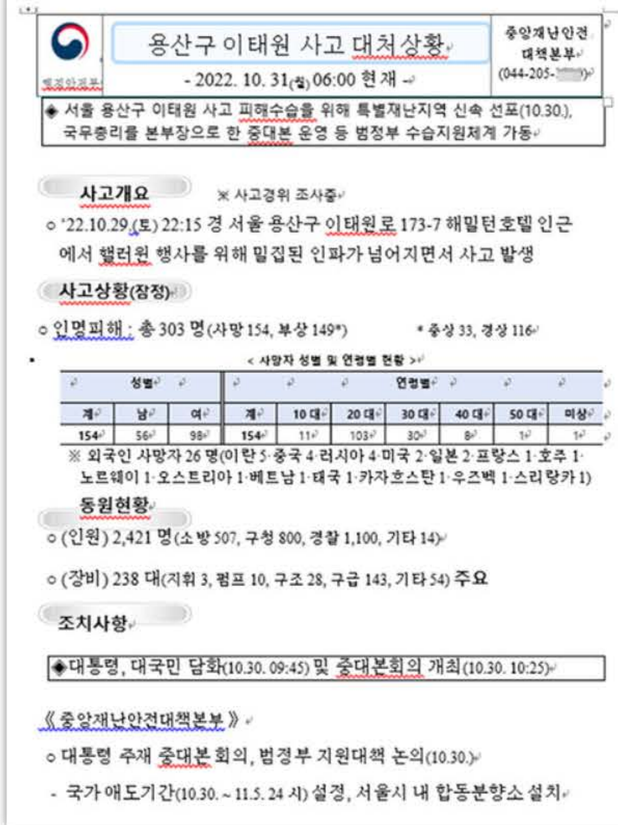
	취득년월	종 류	시 행 청	외국어 취 득	TOEIC	TOEFL	JPT	HSK
자 격 면 허	20xx年 xx月xx日	MOUS - power point	국제교류 진흥회		점	점	점	급
					기타			

경 력 사 항	근 무 기 간	전직장명	직위	담당업무	월보수 /년봉	퇴직사유

가 족 사 항	관계	성 명	연령	출신학교	직업/직위/근무처	동거	부모생존여부	부(O)모(O)
	부	강비즈	xx	xx 대학교	상업/사장/명동	O	가 족 관 계	(1)남 (2)너중 (1)째
	모	김xx	xx	xx 여고	상업/사장/명동	*	재산 현황 동 산	20,000 만원
	매	강xx	xx	유학중	중국 xx 대학교	X	부동산	30,000 만원
	제	강xx	xx	유학중	미국 xx High School	*	가계부양자	홍 길 동
							보훈대상여부	대상( ) 비대상(O)

본 이력서에 기재한 사항은 사실과 다름없음을 확인합니다.
2003 년 xx 월 xx 일
지 원 자 홍 길 동 귀중

용산구 이태원 사고 대처상황



용산구 이태원 사고 대처상황
- 2022. 10. 31(월) 06:00 현재 -

중앙재난안전 대책본부 (044-205-)

◆ 서울 용산구 이태원 사고 피해수습을 위해 특별재난지역 신속 선포(10.30.), 국무총리를 본부장으로 한 중대본 운영 등 범정부 수습지원체계 가동

사고개요 ※ 사고경위 조사중

○ '22.10.29.(토) 22:15 경 서울 용산구 이태원로 173-7 해밀턴호텔 인근에서 핼러윈 행사를 위해 밀집된 인파가 넘어지면서 사고 발생

사고상황(잠정)

○ 인명피해 : 총 303 명(사망 154, 부상 149*) * 중상 33, 경상 116

< 사망자 성별 및 연령별 현황 >

성별			연령별						
계	남	여	계	10 대	20 대	30 대	40 대	50 대	미상
154	56	98	154	11	103	30	8	1	1

※ 외국인 사망자 26 명(이란 5·중국 4·러시아 4·미국 2·일본 2·프랑스 1·호주 1·노르웨이 1·오스트리아 1·베트남 1·태국 1·카자흐스탄 1·우즈벡 1·스리랑카 1)

동원현황

○ (인원) 2,421 명(소방 507, 구청 800, 경찰 1,100, 기타 14)

○ (장비) 238 대(지휘 3, 펌프 10, 구조 28, 구급 143, 기타 54) 주요

조치사항

◆대통령, 대국민 담화(10.30. 09:45) 및 중대본회의 개최(10.30. 10:25)

《중앙재난안전대책본부》

○ 대통령 주재 중대본회의, 범정부 지원대책 논의(10.30.)

- 국가애도기간(10.30.~11.5. 24 시) 설정, 서울시 내 합동분향소 설치

홈텍스 국세청 전자세금계산서



과세 요청
국세청 (hr@putnammechanical.com) 연락처 추가

Invoice_025287.html

Hometax 국세청 홈택스

안녕하세요.
국세청 전자[세금]계산서입니다.
[전자세금계산서 발급 메일 안내]

본 메일은 국세청 홈택스를 이용하여 국일명판사 사업자가 주식회사 현대금형기술.
- 발급일자 : 2019년 05월 30일
- 본 메일이 수신인과 관련없는 경우 수신거부/해제(여기) 를 클릭하시기 바랍니다.

*메일 내용을 확인하기 위해서는 첨부파일을 클릭하십시오.

전자(세금)계산서 첨부파일이 열리지 않을 시 조치 방법
1. 첨부파일을 사용자PC에 저장
2. 저장한 첨부파일을 오른쪽마우스 클릭 후 연결프로그램에서 [Internet Explorer] 선택

국세청 National Tax Service 세종특별자치시 국세청로 8-14 국세청(정부세종2청사 국세청동) (우편번호) 30128
Copyright© National Tax Service. All rights reserved.

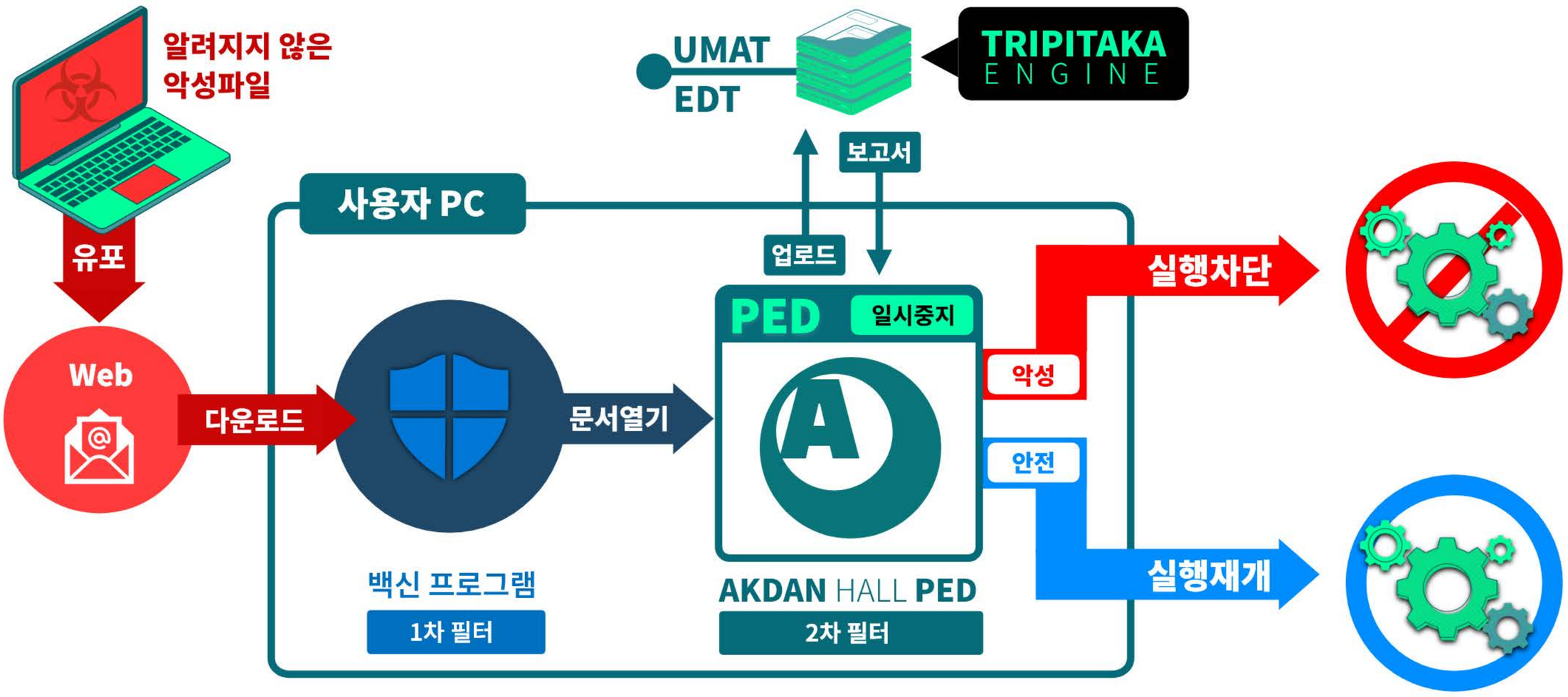
기술적 허점 | 백신도 막을 수 없습니다.

하루에 쏟아지는 악성 파일은 약 60만 개이며, 백신 패턴으로 등록되기까지 평균 205일이 소요됩니다.
백신만 맹신하다가는 알려지지 않은 악성 파일에 무방비로 노출됩니다.



악단홀 PED | 알려지지 않은 문서파일을 탐지하는 PED 방식의 PC 보안 솔루션입니다.

다운로드 시점에 검사하는 백신 이후, 악단홀이 2차로 분석합니다.
PED란, Pre-Execution Detect의 줄임말로 악성코드를 실행하기 직전에 동작을 예측하여 탐지하는 기술입니다.



트리피타카 엔진 | 클라우드에서 동작하는 악성코드 분석 엔진입니다.

메모리 오동작 탐지 트랩(UMAT)과 취약점 탐지 트랩(EDT)이 알려지지 않은 위협을 빠르고 정밀하게 추적합니다.
추출된 위협은 사용자에게 상세 분석 보고서로 제공합니다.

트리피타카 엔진 분석 시스템

EDT Exploit Detect Trap

- 오피스 버전별 취약점 트랩
- 원격파일 다운로더 트랩
- 매크로/스크립트 탐지 트랩

UMAT Unauthorized Momory Access Trap

- 콜스택 탐지
- HEAP 탐지
- SEH 탐지

→ UMAT

상세 분석 보고서



경쟁력 | 가볍다! 빠르다! 정교하다!

백신과 함께하면 더 할 나위 없는 방어 체계가 완성됩니다.

분류	백신	APT 솔루션	악단홀 PED
시그니처(알려진 악성코드)검사	✓	N/A	N/A
알려지지 않은 악성코드 검사	N/A	✓	✓
탐지속도	N/A	60초	3초*
상세 분석 보고서	N/A	✗	✓
가격	무료 / 저렴	매우 비쌈	무료 / 저렴

* TTA GS인증 및 KBeT V&V 시험결과

Everyone's SHIELD

Copyright © 2024 **AKDAN** INC. All right reserved

"AKDAN MAKES EVERYONE'S SHIELD"

"보안장인들이 모두의 방패를 만듭니다."

악성코드검거단
MALWARE ARREST TEAM

COMPANY 악성코드검거단(주)
EMAIL contact@akdan.co.kr
TEL 031-698-4155
FAX 0504-007-4155

BUSINESS LICENSE 461-81-03161
ADDRESS [13449] 경기도 성남시 수정구 대왕판교로 815
판교 제2 테크노밸리 창업존 , 465호(정보보호클러스터)
HOMEPAGE **www.akdan.co.kr**