문서파일을 이용한 고도의 사이버 공격을 탐지하는 분석엔진, 트리피타카[팔만대장경]

TRIPITAKA ENGINE

알려지지 않은 위협을 사전에 차단

파일을 실행하면 발생하는 행위를 실행 전에 추출하여 각 행위에 따른 위험도를 판단합니다.
악성코드를 사용자가 실행한 것처럼 유도하는 포워드 엔지니어링은 어떠한 공격도 탐지할 수 있습니다.

현존 동적분석 엔진

외산 샌드박스 + 상용 윈도우 + 상용 오피스

[리버스 엔지니어링]

샌드박스에서 자동 프로세스가
한 번 실행한 결과를 분석

사람의 심리와 행동을 이용한
사회공학적 공격은
[탐지불가]

차세대 동적분석 엔진

자체개발 쾌속 샌드박스(HSS)

비인가 메모리 탐지 트랩(UMAT) + 취약점 공격 탐지 트랩(EDT)

[포워드 엔지니어링]

모든 공격 경로를 탐지 트랩으로 유도하여
동시 다발적으로 추적

FEATURE

1. 문서형 악성파일과 매크로탐지
2. 숨겨진 스크립트도 추출하여 분석
3. 원격 템플릿 인젝션과 URL 감시
4. 비실행 기반의 능동 탐지

AKDAN MALWARE ARREST TEAM

Advanced Malware | 고도로 진화된 문서형 악성파일

최근에 발견되는 문서형 악성 파일은 한 가지 방식으로 동작하지 않습니다.
원격 파일 다운로더와 스크립트, 난독화, 탐지방해 기법 등 여러 공격 기술을 복합적으로 이용하여 사용자의 PC를 공략합니다.

1. **문서파일** — 취약점 공격 | 원격 템플릿 인젝션(RTI) | 매크로
2. **원격서버 URL** — 웹 서버 | 원격 템플릿 인젝션 | C&C 서버
3. **스크립트** — VB 스크립트(VBS) | 파워쉘 스크립트(PS) / 자바 스크립트(JS) | 배치 파일(BAT)
4. **난독화** — 바이너리 Hex인코딩 | Base64 인코딩 / Custom 인코딩
5. **탐지방해** — **[기존 Anti-VM 기법과 다른]** 고의시간 지연 | Random Loop 탈출 퍼즐 | 잠복 후 다음 부팅 시 실행
6. **악성코드** — 랜섬웨어 | 채굴기 | 백도어 등

위협요소 추출 → **위험도 판단**

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

Forward Engineering | 포워드 엔지니어링(FE) 탐지기술의 원리

포워드 엔지니어링 기술은 미리 만들어 둔 트랩에 악성파일을 밀어 넣어 탐지하는 방식입니다

EDT Exploit Detect Trap

주로 이용하는 공격 패턴을 수용하여 사람이 실행하는 것처럼 악성 행위를 유발합니다.
이 과정에서 원격 파일을 다운로드하고, 스크립트를 추출하며, 난독화를 해제하고 탐지방해 기법을 회피합니다.

UMAT Unauthorized Memory Access Trap

자체개발 CPU 에뮬레이터는 악성 파일이 EDT에서 활동하도록 강제합니다.
동시에 메모리 오동작을 감시하며 취약점 공격도 탐지합니다.

HSS High Speed Sandbox

악성코드 탐지에 최적화된 운영체제로 **EDT**와 **UMAT**를 초고속으로 구동합니다.
수백 가지의 실행 경로를 운행해도 소요되는 시간은 수초 이내입니다.

Support File Format | 지원하는 파일 형식

각종 오피스 문서 파일과 스크립트를 분석할 수 있습니다.

HWP	XLS	DOC	PPT
PDF	ONE	RTF	SCT
VBA	VBS	HTML	HTA
JS	PS	BAT	LNK

Technical Patent | 특허 현황

약 3년간의 연구개발 동안 국내특허 12건 (1건 등록), 해외특허 1건을 출원했습니다.



Comparison of competitors | 경쟁사 비교

포워드 엔지니어링은 향후 보안 업계를 책임질 새로운 무기입니다.

경쟁 내용	백신	리버스 엔지니어링	포워드 엔지니어링
Signature-based Detection 시그니처(알려진 악성코드) 검사	✓	N/A	N/A
Signatureless Detection 알려지지 않은 악성코드 검사	N/A	✓	✓
Detection Speed 탐지속도	N/A	60s / file	3s / file *
Necessary Resources 필요자원	N/A	500MB / file	240KB / file
Analysis Environment 분석환경	N/A	윈도우/오피스	HSS (UMAT/EDT)
External License Cost 외부 프로그램 추가구매	N/A	✓	✗
Behavior Translation 행위해석	N/A	✗	✓
Personal Solution 개인용 솔루션	✓	✗	✓
Enterprise Solution 기업/관공서 솔루션	✓	✓	✓ (설치형 엔진)

* 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)	**BUSINESS LICENSE**	461-81-03161
EMAIL	contact@akdan.co.kr	**ADDRESS**	[13449] 경기도 성남시 수정구 대왕판교로 815
TEL	031-698-4155		판교 제2 테크노밸리 창업존 , 465호(정보보호클러스터)
FAX	0504-007-4155	**HOMEPAGE**	**www.akdan.co.kr**