제 3회 해킹메일 공격 아이디어 경진대회

2023 Hacking Scenario

피싱사이트 & 엑셀 파일 - 공격 시나리오

Collaboration with KICOX (한국산업단지공단)

한국산업단지공단 홈페이지에 공개된 주요산업을 대상으로 해킹을 위한 공격용 메일 작성 시나리오입니다.
본 프로젝트는 한국산업단지공단 해킹대회임을 알립니다.

WHE

2023년도 해킹메일 공격 아이디어

Contents

목차

01

SCENARIO

공격 시나리오

한국산업단지공단의 주요산업 공격 방법

- 핵심 개요
- 대상 산업 및 최근 이슈
- 발송 메일 예시

About. 시나리오 핵심 개요

공격 시나리오의 전체적인 요약본인 핵심 개요입니다.
- 목표 기업, 공격 대상, 사칭할 발신인, 목표들로 구성되어 있습니다.

목표 기업	한국산업단지공단 - 탄소중립융자센터
공격 대상	팀장급 직급의 이한우 팀장
발신인 사칭	대리급 직급의 성혜진 대리
목표 1	이한우 팀장의 산업단지공단 누리집 개인정보 탈취 및 개인 PC해킹
목표 2	이한우 팀장으로부터 탈취한 정보 활용하여 한국산업단지공단 근무자 다수의 PC해킹 시도
목표 3	이한우 팀장의 신분을 사칭해 한국산업단지공단이 진행중인 사업에 혼란 유발

Korea Industrial Complex Corporation

한국산업단지공단
Korea Industrial Complex Corporation

Hacking Scenario

팀 WHE는 성공적인 공격 시나리오를 위해 디테일한 상황도까지 고려합니다.

이한우 팀장

공격용 메일

성혜진 대리 (사칭)

피싱 사이트

한국산업단지공단

엑셀 파일

매크로 활용

Visual Basic Editor

ID & PW 획득

근무자 PC 추가 해킹

AI사업본부

Fake Image Exploiter

Handler

사업 혼란 유발

Hacking Scenario

Key Strategy

신뢰도

대리급 부하직원
실제 파일 오류 이미지 확인

혼란한 상황

근무 시간 외 문제 발생
여러 기업의 문의 쇄도

최근 이슈 - 중요도

23.8.17 - 탄소중립 사업전환 (MOU) 이슈
최근 이슈 문제로 중요성 부각

중요한 문제가 혼란한 상황 속에 발생 & 신뢰할 수 있는 부하직원의 보고 --> 대상자가 쉽게 속을 것으로 예상.

Related Issues

팀 WHE는 성공적인 공격 시나리오를 위해 디테일한 상황도까지 고려합니다.

산단공-기보, 탄소중립 산업전환 촉진 금융지원 협력

디지털경제 | 입력 :2023/08/18 09:11

HOME > 뉴스 > 에너지수요관리

산단공·기보, 산단 탄소중립 산업전환 MOU

차기영 기자 | 승인 2023.08.17 16:54 | 댓글 0

금융지원 협력 강화

한국산업단지공단과 기술보증기금은 탄소중립 산업전환 촉진을 위한 사업화지원 업무협약을 체결하고 관계자들이 기념촬영을 하고 있다.

2023

2023.08 탄소중립 산업전환 사업화지원' 업무협약 체결

2023

2023.04 탄소중립 전환 선도 프로젝트 융자지원 사업 안내서 공지

공지사항

고객마당 > 공지사항 > 공지사항

2023년 탄소중립 전환 선도프로젝트 융자지원 사업 안내서 공개

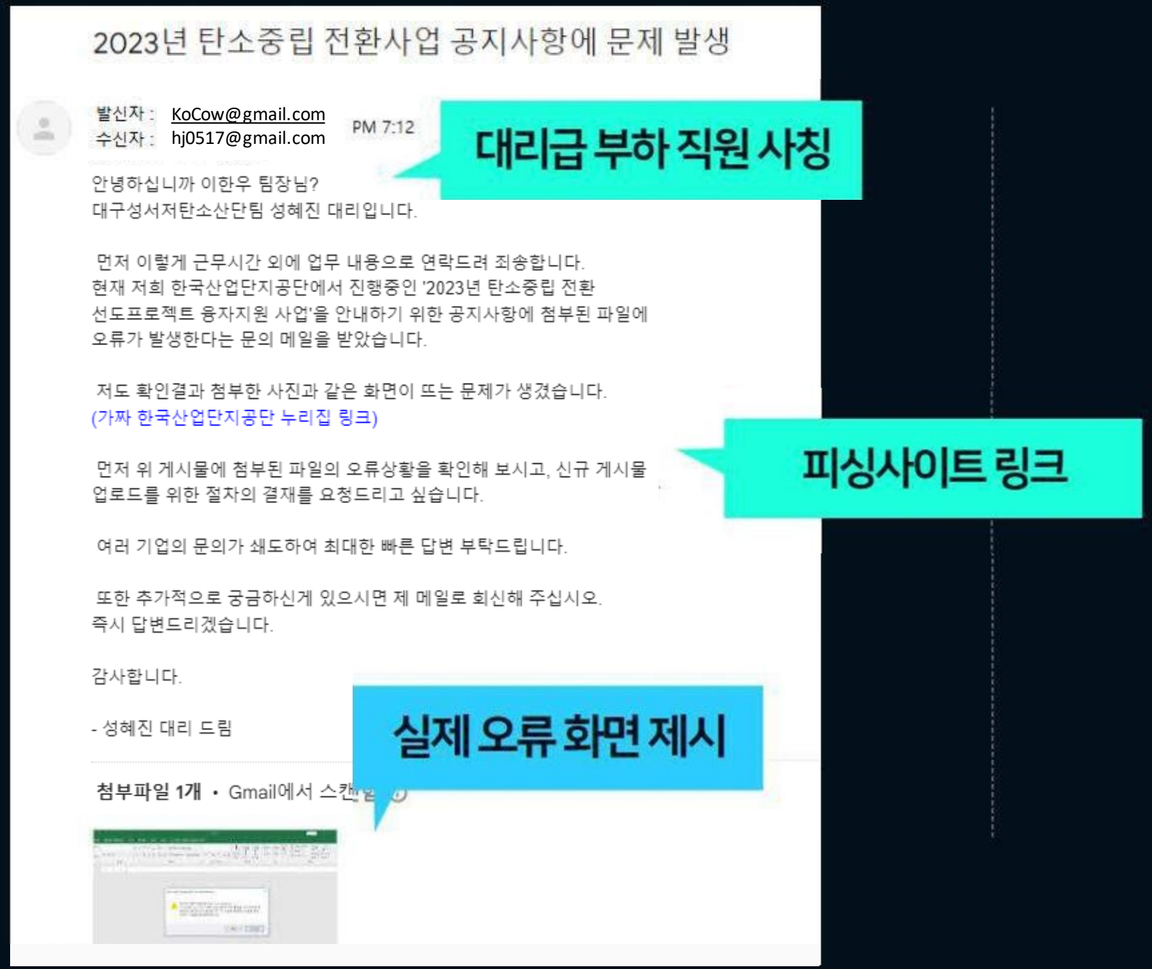
2023-04-04 10:43:22

2023년 탄소중립 전환 선도 프로젝트 참여인력 정보.xlsx | 2023년 탄소중립 전환 선도프로젝트 융자지원 사업설명회 발표자료.pdf

2023년 탄소중립 전환 선도프로젝트 융자지원 사업 안내서와 설명자료를 붙임과 같이 공개하오니,

신청을 희망하시는 기업께서는 참고하시기 바랍니다.

Mail Content



Key Point in Mail

공격 전략

KEY 1
자극적인 제목
메일 열람 유도

KEY 2
현재 이슈
'탄소중립 산업전환' 관련 사안

KEY 3
부하직원 사칭
실제 대리급 사칭

KEY 4
피싱사이트 유도
최종 목표

성공적인 공격 전략을 위해 고려한 점들과 그로 인한 효과들입니다.
팀 WHE는 성공적인 공격 시나리오를 위해 디테일한 상황도까지 고려합니다.

02

CORE TECH

핵심 기술 1

이미지 활용 해킹

- 이미지 활용 해킹
- Fake Image Exploiter

CORE TECH 1 - Image

팀 WHE는 성공적인 공격 시나리오를 위해 디테일한 상황도까지 고려합니다.

Fake Image Exploiter

작동방식

기존 image.jpg 와 payload.ps1 하나(사용자가 입력)를 가져와 실행 시 apache2에 저장된 이전 파일 2개의 다운로드를 트리거하는 새 페이로드를 구축

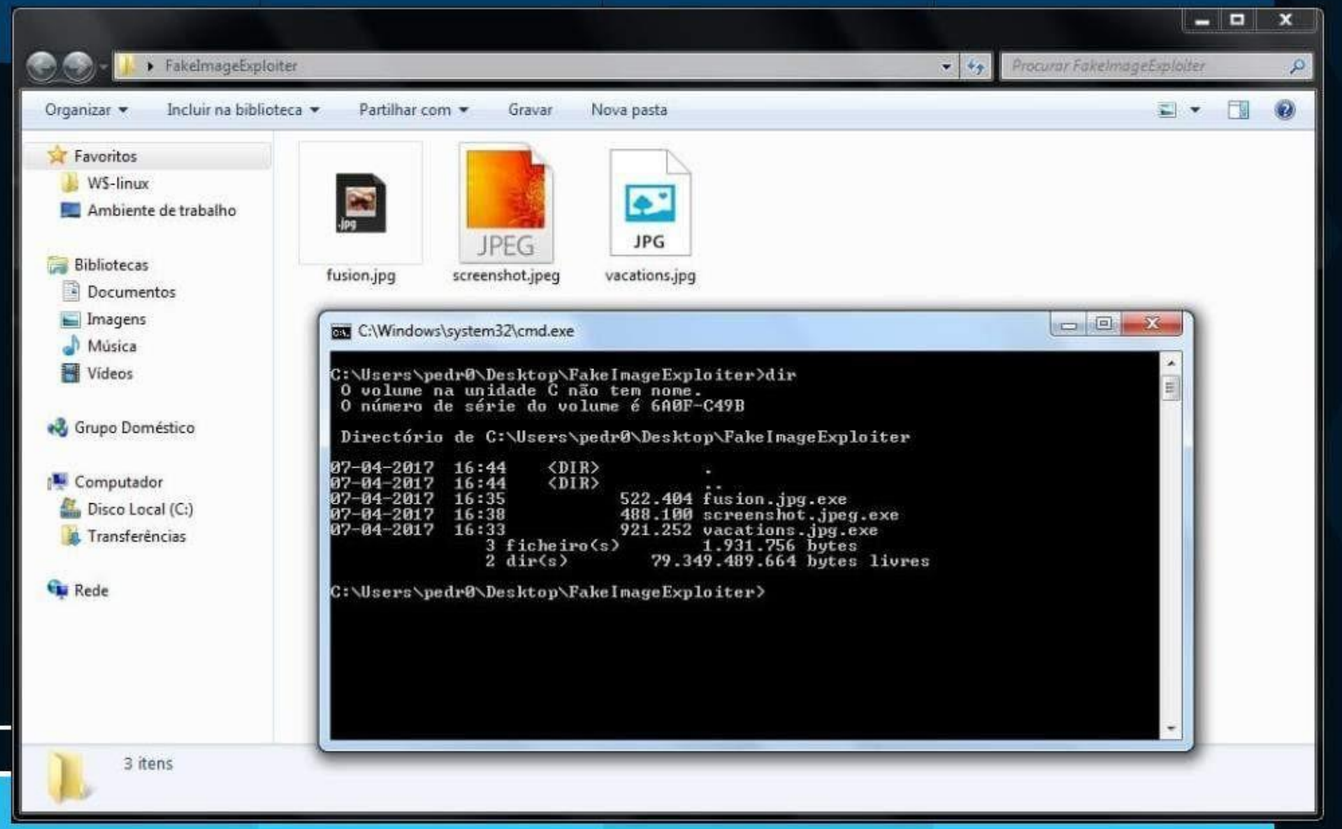
하나의 file.jpg와 일치하도록 Agent.exe 아이콘 변경.
스푸핑 '알려진 파일 형식의 확장명 숨기기' 방법을 사용하여 Agent.exe 확장자를 숨김.

모든 페이로드(사용자 입력)는 apache2 웹 서버에서 다운로드되어 대상 RAM으로 실행.
디스크에 페이로드를 써야 하는 유일한 확장 (사용자가 입력한 페이로드)은 .exe 바이너리.

핵심 기술

Fake Image Exploiter

Handler



03

CORE TECH

핵심 기술 2

피싱 사이트 & 엑셀 활용 해킹

- 피싱 사이트
- 엑셀 매크로 해킹
- Visual Basic Editor

CORE TECH 2 - Phishing

팀 WHE는 성공적인 공격 시나리오를 위해 디테일한 상황도까지 고려합니다.

피싱 사이트 제작

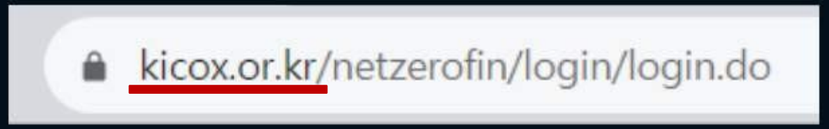
실제 '탄소중립융자센터'와 유사한 URL

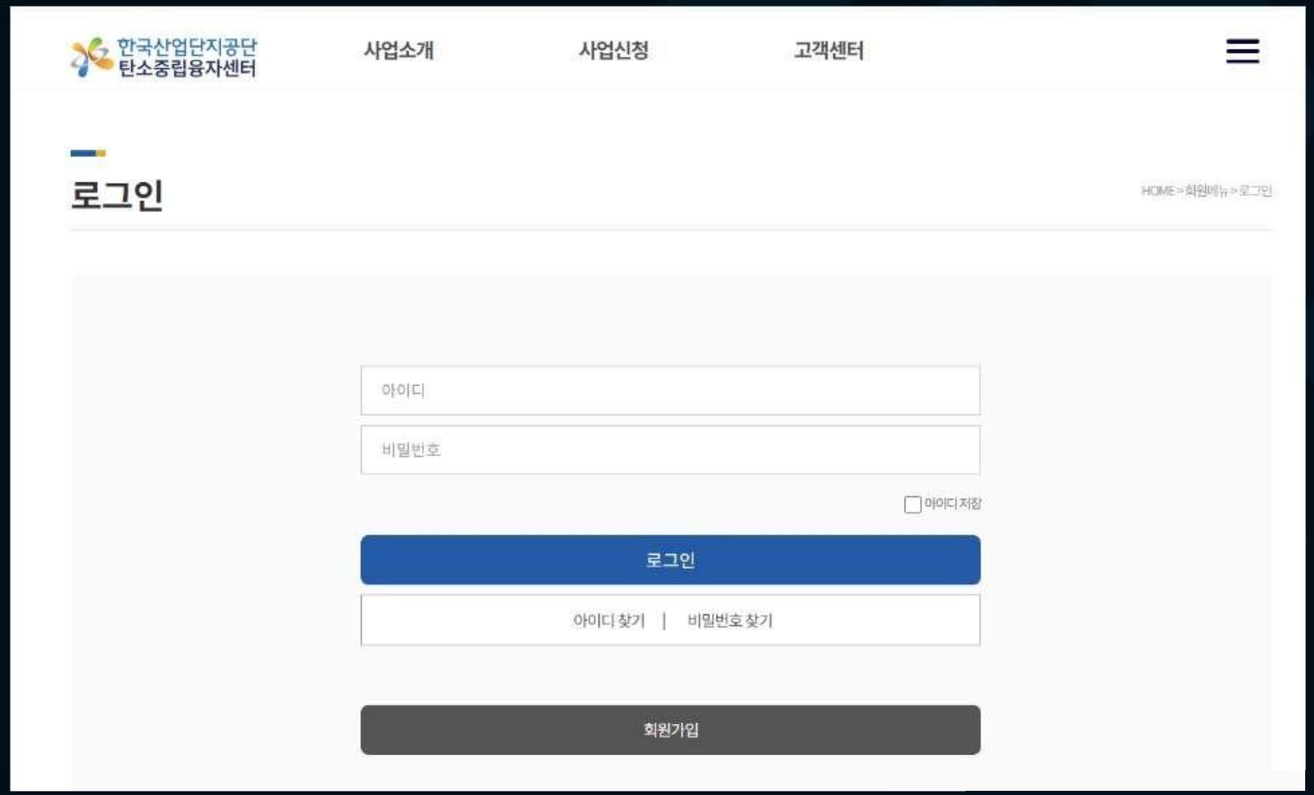
사용 용도

- 공격 대상자 ID & PW 획득
- 악성코드 파일 다운로드 경로

실제 홈페이지 (탄소중립융자센터)

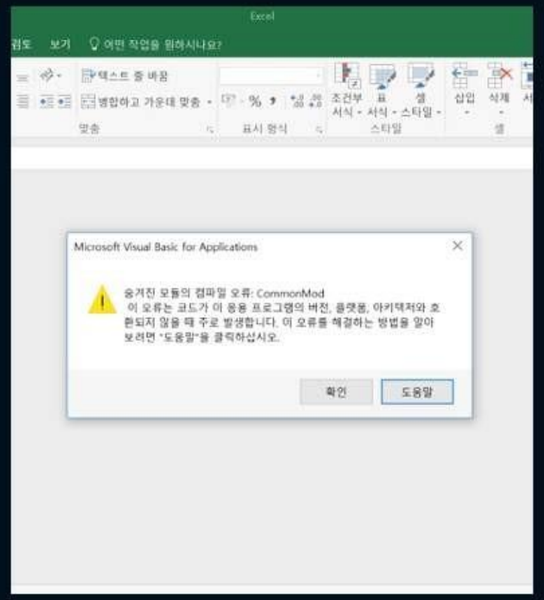
- 똑같은 구성의
- 똑같은 기능의
- 똑같은 내용의





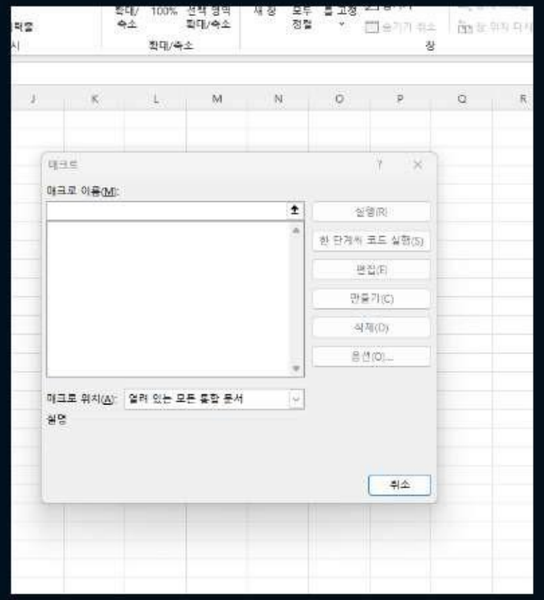
CORE TECH 2 - Excel

팀 WHE는 성공적인 공격 시나리오를 위해 디테일한 상황도까지 고려합니다.



엑셀 파일 제작

실제 홈페이지 공지사항의 파일을 바탕으로
공격 대상자를 속일 가짜 엑셀파일 제작.
오류로 보이게 조작.

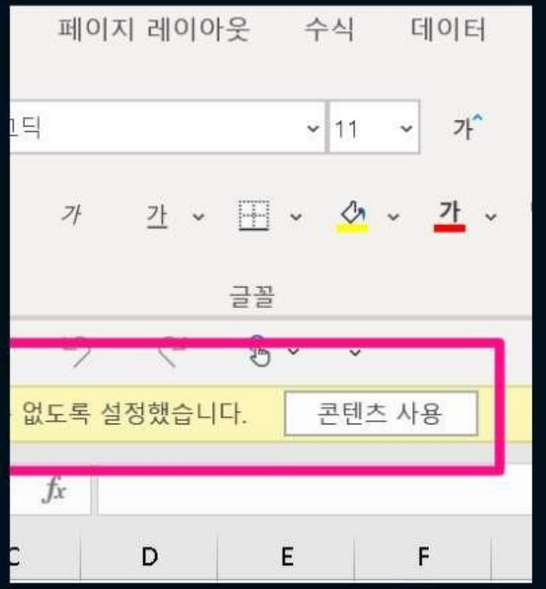


악성코드 제작

매크로를 활용하여
대상자 PC를 장악할 악성코드 설치.

파일 업로드

실제 공지사항과 동일하게 만든
피싱 사이트에 가짜 파일을 업로드



매크로 활성화 유도

악성코드 활성화를 위해
대상자가 콘텐츠 사용 허가를 하도록 유도

04

BENEFIT

기대 효과

공격 성공시 예상 피해

- 1-2차 피해
- 기타 피해

Benefit

EXPECTATION

기대 효과 (예상 피해)

팀 WHE는 성공적인 공격 시나리오를 위해 디테일한 상황도까지 고려합니다.

1차 피해

팀장 A의 PC 해킹

개인정보 유출
개인 피해

중요파일 유출
기업 피해

- 개인적 피해 + 기업 전체 피해
- 추가 피해 가능성 존재

2차 피해

악성코드 추가 유포

대규모 정보 유출
기업 피해

KICOX 전체 마비
기업 피해

- 가장 규모가 큰 피해
- 기관 전체의 마비 위험
- 추가 피해 가능성 존재

기타 피해

기타 사업에 차질

천문학적 규모의 경제적 손실 발생
기업 피해

국가기관 신뢰도 하락

- 가장 경제적 손실이 큰 피해
- 국가 자체의 신뢰 하락 우려
- 보안문제로 인해 효율성 악화 우려

WHE

우리에게 디지털 세계의 잠금은 그저 장식일 뿐.

2023년 제 3회 해킹메일 공격 아이디어 경진대회

참가자 (고등전문 A)

자료 조사 - 구암고등학교, 김기범
경상고등학교, 김진영

PPT 제작 - 구암고등학교, 김현승

발표 - 구암고등학교, 김현승
구암고등학교, 김기범
경상고등학교, 김진영

고등전문 A반 - WHE팀