

An abstract 3D composition featuring several geometric shapes. A large, dark brown cube is the central focus, with a smaller, lighter brown cube positioned above it. To the right, a dark blue cube is partially visible. Two bright yellow spheres are placed around the central cube, one above and one to the left. The background is a dark, muted blue-grey. A thin white horizontal line is positioned above the main title.

피싱 사이트를 이용한 공격

Team - K4

2022.10.15

Contents

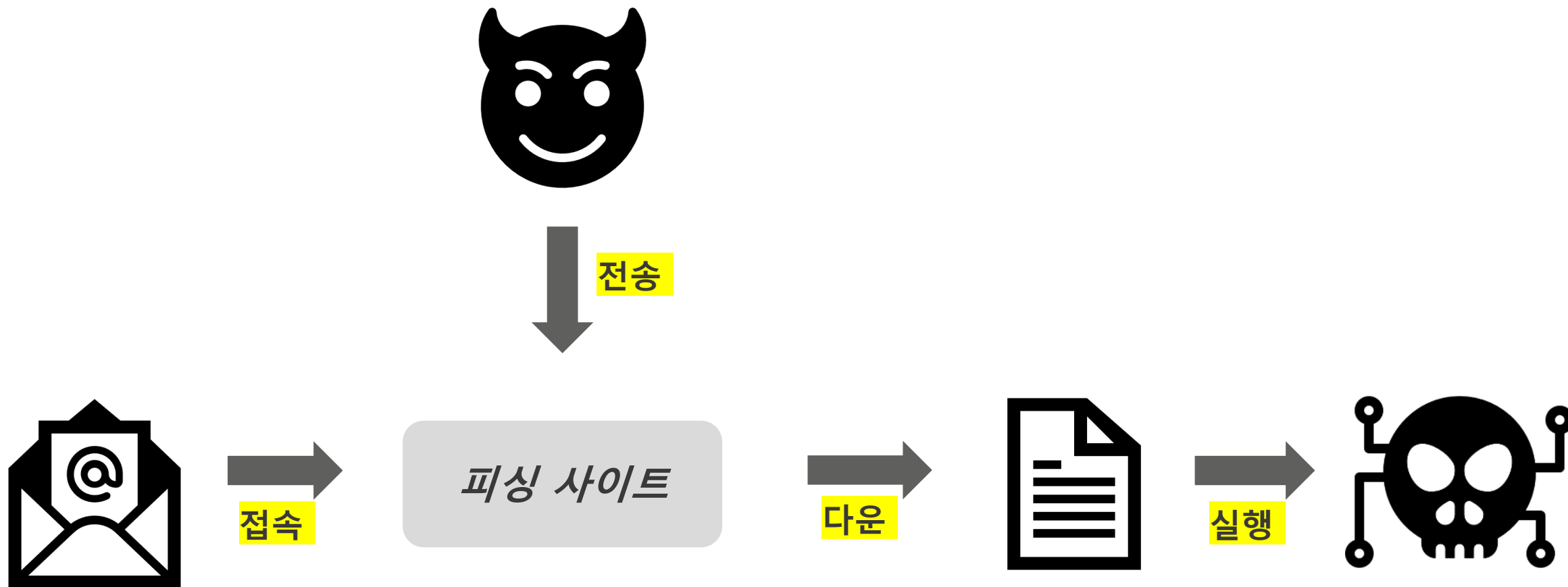
- 1 시나리오
- 2 핵심 기술
- 3 기대효과

Part 1

시나리오

Part 1

시나리오



해킹 대상 : 한국산업단지공단 관계자

해킹 목적 : 한국산업단지공단의 PC를 해킹하여 정보를 탈취하기 위함

해킹 시기 : 연말정산이 이루어지는 연말

Part 2

핵심기술

열린경영
고객마당
주요사업
공단소개
정보공개
기업애로 해결
☰
🔍

공단소개

CEO 인사말

연혁, 비전 및 목표

공단 상징

조직도, 연락처

찾아오시는 길

공단 사보

조직도, 연락처

🏠 > 공단소개 > 조직도, 연락처

담당자명	직위	전화번호	담당업무
윤홍민	팀장	070-8895-7141	운영지원팀 업무총괄
고경선	차장	070-8895-7142	자산, 자회사 관리
김경민	차장	070-8895-7144	계약, 대내외 보고
강문규	대리	070-8895-7143	어린이집, 법인콘도
김종근	대리	070-8895-7145	시설, 에너지, 보안
황가영	주임	070-8895-7147	기관 기록물관리
정진우	주임	070-8895-7146	계약(협상, 수의), 경영평가 계량지표 관리, 동반성장
구유빈	주임	070-8895-7148	사택 및 차량관리

2023 연말정산확인 부탁드립니다 ☞

보낸사람

고경선

22.10.09 13:05 주소추가 | 수신차단

발신자

:한국산업단지공단의
실제 회계 담당자(고경선 차장)의
이름, 연락처를 사칭해
피해자의 신뢰를 얻을 수 있음

Part 2

핵심 기술 – 자극적인 제목



고경선

2023 연말정산확인 부탁드립니다

2023 연말정산확인 부탁드립니다

보낸사람

고경선

22.10.09 13:05 주소추가 | 수신차단

벌써 2022년의 끝을 바라보고 있습니다.

이번 연말정산이 작년과는 변경점이 있어서 저희가 파일로 정리를 해놓았고

밑에 국세청 링크 들어가셔서 2023년도 연말정산 파일 확인해보시면 되겠습니다.

파일은 보안의 문제로 인해 암호화 되어있기 때문에 파일의 설명을 잘 보셔야 합니다.

그럼 즐거운 연말 지내시길 바랍니다. 올 한해도 수고 많으셨습니다.

개인적인 문의사항이나 궁금한 부분은 제 메일로 문의주시길 바랍니다.

(가짜 국세청 링크)

제목

: “연말정산”과 같은
자극적인 단어를 사용

= 피해자가 메일을 열람할
수
있도록 유도함

본문

: 시기에 맞는 연말정산
안내문 + 피싱 사이트로
연결되는 링크

2023 연말정산확인 부탁드립니다 ☐

보낸사람

고경선

22.10.09 13:05 주소추가 | 수신차단

벌써 2022년의 끝을 바라보고 있습니다.

이번 연말정산이 작년과는 변경점이 있어서 저희가 파일로 정리를 해놓았고

밑에 국세청 링크 들어가셔서 2023년도 연말정산 파일 확인해보시면 되겠습니다.

파일은 보안의 문제로 인해 암호화 되어있기 때문에 파일의 설명을 잘 보셔야 합니다.

그럼 즐거운 연말 지내시길 바랍니다. 올 한해도 수고 많으셨습니다.

개인적인 문의사항이나 궁금한 부분은 제 메일로 문의주시길 바랍니다.

(가짜 국세청 링크)

변경된 부분이 있다는 것을
알려 궁금증을 유발함

= 피해자가 링크에 접속할
수
있도록 유도함

국가기관을 사칭해 신뢰감 드는 링크 제공

2023 연말정산확인 부탁드립니다

보낸사람

고경선

22.10.09 13:05 주소추가 | 수신차단

벌써 2022년의 끝을 바라보고 있습니다.

이번 연말정산이 작년과는 변경점이 있어서 저희가 파일로 정리를 해놓았고

밑에 국세청 링크 들어가셔서 2023년도 연말정산 파일 확인해보시면 되겠습니다.

파일은 보안의 문제로 인해 암호화 되어있기 때문에 파일의 설명을 잘 보셔야 합니다.

그럼 즐거운 연말 지내시길 바랍니다. 올 한해도 수고 많으셨습니다.

개인적인 문의사항이나 궁금한 부분은 제 메일로 문의주시길 바랍니다.

(가짜 국세청 링크)

보안의 문제라는 이유로
피싱 사이트의 **암호화를 합리화**

뒤에 이어지는 매크로를
작동시키는 데에 **트리거를 발동**시킬 수 있음

= 피해자가 **암호화를
합리화**하고
파일 매크로에 동의하게 함

Part 2

핵심 기술 – 피싱 사이트

<https://www.homelax.go.kr/>

<https://www.hometax.go.kr/>

실제 국세청 사이트 url과 유사한 피싱 url

My홈택스

로그인 회원가입 인증센터 국세청홈페이지 법령정보 부서사용자 가입하기 화면크기 100%

HomeTax 국세청홈택스 조회/발급 민원증명 신청/제출 신고/납부 상담/제보 세무대리/납세관리 검색 전체메뉴

로그인

국세청 홈택스에 오신 것을 환영합니다.

① 로그인 안되는 경우 [로그인 안내]를 눌러 도움받으세요. 로그인 안내 PC용 보안 프로그램 적용

공동-금융인증서

간편인증
(민간인증서)

아이디 로그인

생체인증
(얼굴지문)

비회원 로그인

회원가입

인증서 등록

홈택스 회원 아이디와 비밀번호가 없는 경우
회원가입을 하셔야합니다.

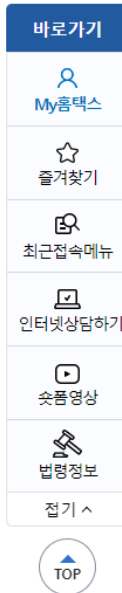
아이디

비밀번호

로그인

☐ 아이디 저장 아이디/비밀번호 찾기

아이디는 영문, 숫자포함 6~20자리까지 가능합니다.
비밀번호는 영문, 숫자포함 9~15자 이내로 입력 가능합니다.



실제 국세청 홈페이지와 유사한 UI

· 개인정보보호를 위하여 홈택스 서비스를 이용하신 후 반드시 [로그아웃]을 하시기 바랍니다.

Part 2

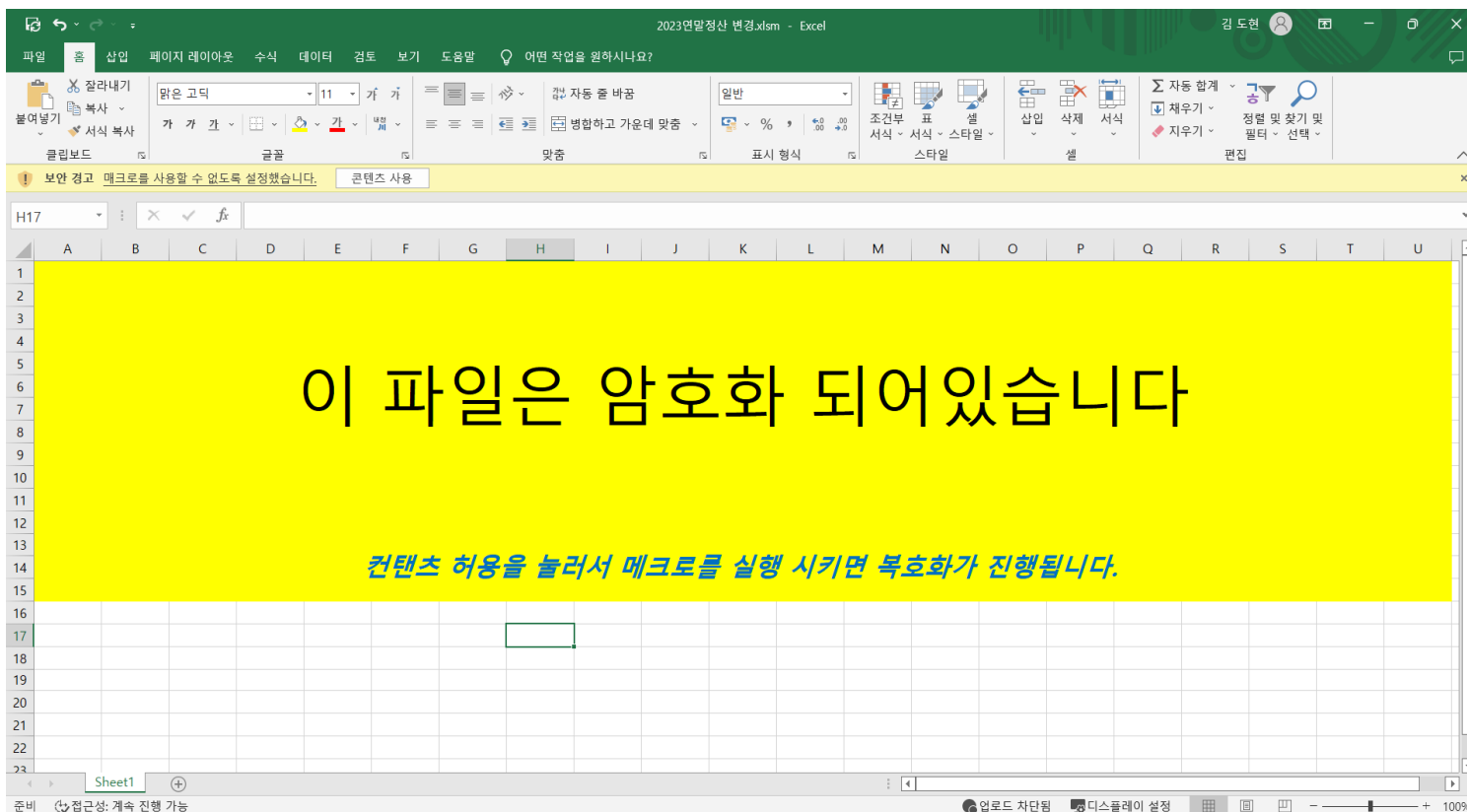
핵심 기술 - 엑셀

백신의 탐지를 어렵게 하기 위해

암호화된 악성코드를 **엑셀 파일**에 담아서

매크로를 활성화시키도록 유도

= 악성코드 실행





Part 3

기대효과

1

로그인 정보를 바탕으로 한 타 사이트 로그인으로 정보 탈취

2

주민번호 등 개인정보 탈취

3

악성코드를 이용한 기밀문서 탈취 또는 암호화

4

개인이나 기업 모두에 피해

