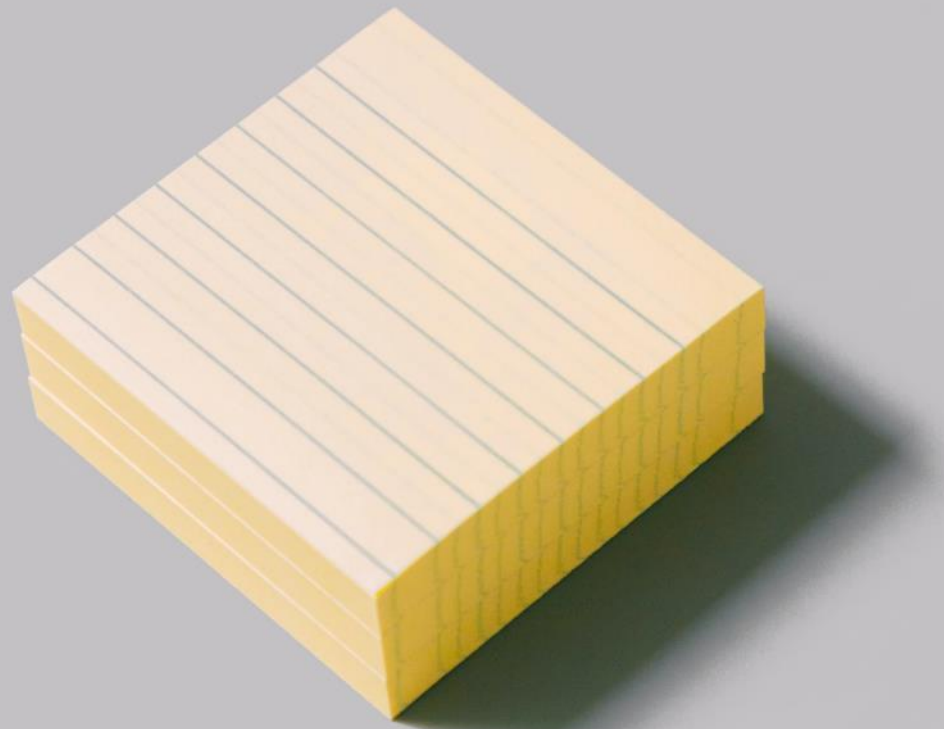


피싱을 이용한 웨일링 공격

Team - 자료만드느라배가고팟습니다

2023.10.14

Part 0
소개

시나리오

확인

피싱 사이트

비밀번호 입력

개인정보
탈취

Part 0

웨일링(Whaling) 이란?

웨일링(Whaling) 공격은 스피어 피싱(Spear Phishing)의 한 종류입니다.

더 넓게는 신뢰를 기반으로 사람의 취약점을 공략해 원하는 정보를 얻는 방식을 사회공학적 해킹(Social Engineering Hacking)이라고도 합니다.

웨일링 공격은 그 중에서도 CEO, CFO 등 기업 내 고위 경영진, 정치인, 연예인 등을 타깃으로 한 공격을 말합니다.

공격 목적은 일반적인 피싱과 같습니다. 대상자의 PC에 악성코드를 심어 기업 및 단체의 중요 정보를 탈취하는 것입니다. 정보를 캐내는 것뿐만 아니라 가짜 송금을 유도해 금전적인 이익을 탈취하기도 합니다.

Part 1
핵심 기술

Part 1

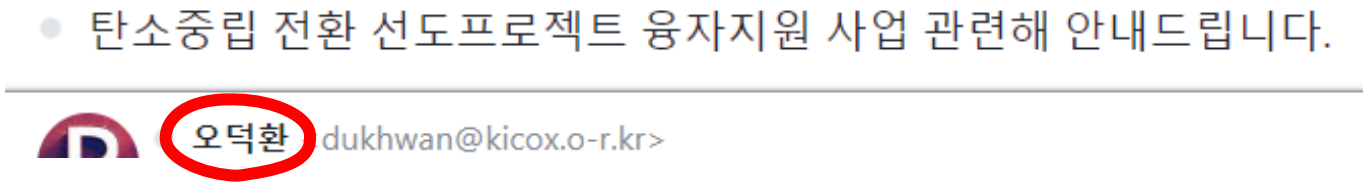
1. 신뢰도 높은 메일

sense

조직도 및 직원검색

공단소개 > 조직 및 연락처 > 조직도 및 직원검색

담당자명	직위	전화번호	담당업무
오덕환	팀장	[redacted]	디지털산단팀 총괄
김장순	차장	[redacted]	디지털산단 업무
이경아	차장	[redacted]	지역특성화
오유나	과장	[redacted]	대개조 총괄
김후남	과장	[redacted]	통합관제센터 구축사업 담당
김현수	과장	[redacted]	경영평가, KPI
지상준	대리	[redacted]	스마트그린산단 홍보, 공정혁신시뮬레이션 센터 사업 관리, 스마트물류플랫폼 사업 관리, 산업단지 대진단 사업 관리



탄소중립 전환 선도프로젝트 융자지원 사업 관련해 안내드립니다.

오덕환 dukhwan@kicox.o-r.kr>

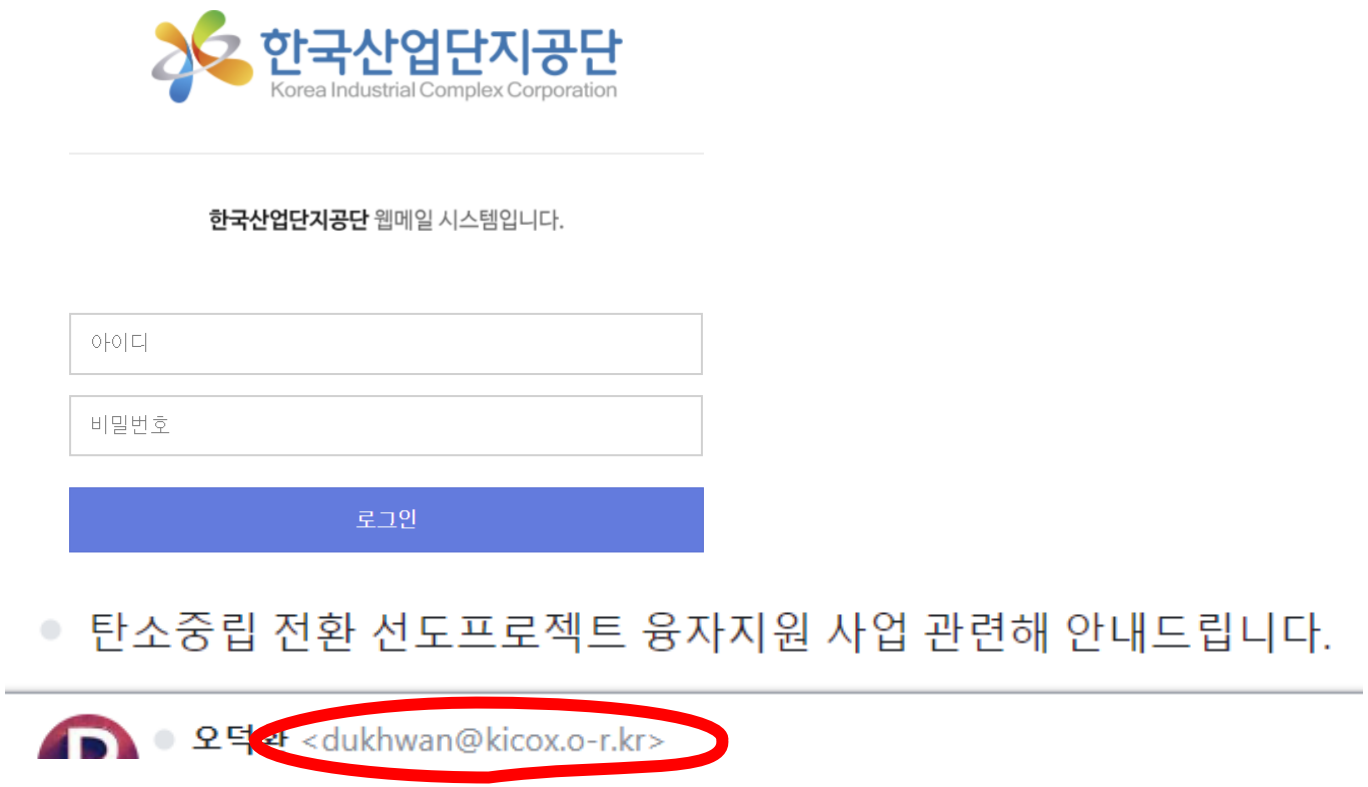
발신자 사칭

실제 한국산업단지공단의
디지털산단팀 총괄 팀장
(오덕환 팀장) 을 사칭하여 메일을 전송,

수신자는 신뢰를 얻을 수 있습니다.

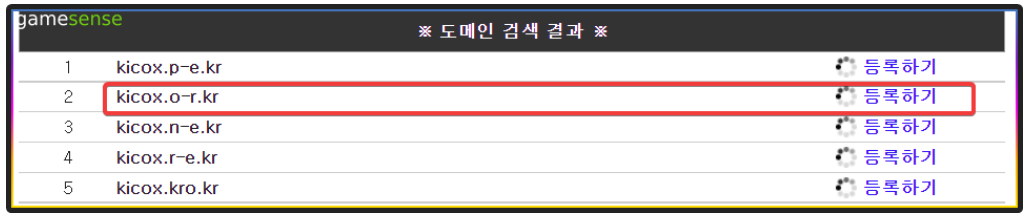
Part 1

2. 비슷한 도메인을 사용해 전송



비슷한 도메인

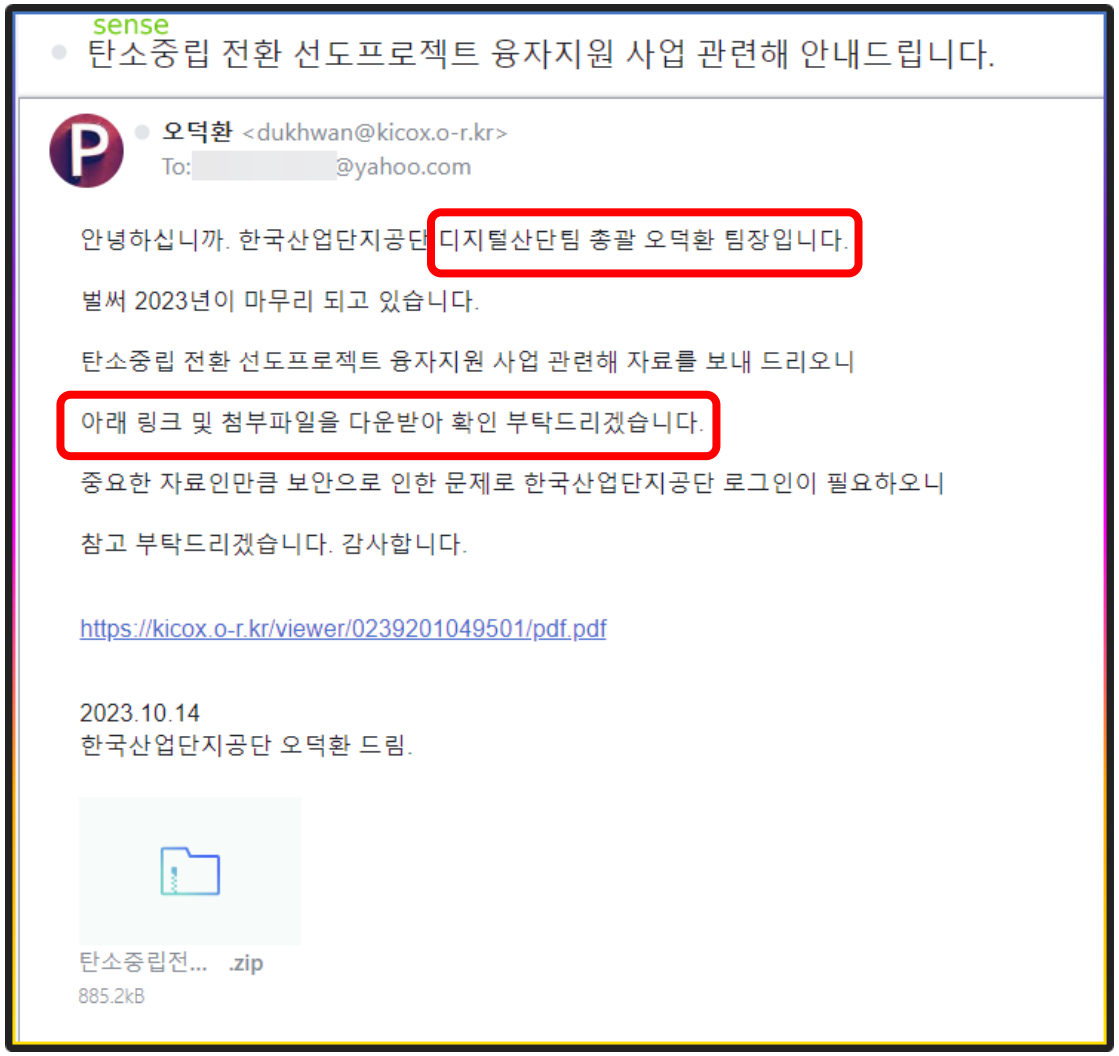
한국산업단지공단의 임직원 메일이 있음을 고려하여, 비슷한 도메인을 사용해 메일을 발송하여, 한국산업단지공단에서 보낸 메일처럼 전송합니다.



한국산업단지공단 : kicox.or.kr
구할 수 있는 도메인 : kicox.o-r.kr

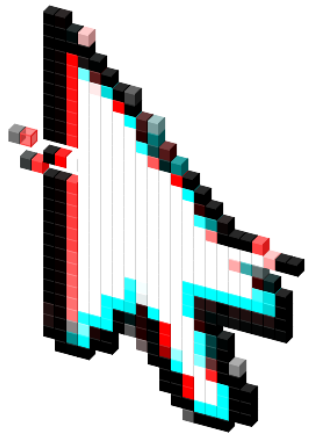
Part 1

3. 수신자의 유도



수신자 메일 클릭 유도

**수신자가 피싱 링크 및 악성코드가 담긴 첨부파일을 클릭하기 앞서,
수신자는 발송한 메일을 클릭해야 합니다.
제목과 내용을 업무 관련된 것으로 선정해 전송하여 수신자는 메일을 클릭할 수 밖에 없도록 유도 합니다.**

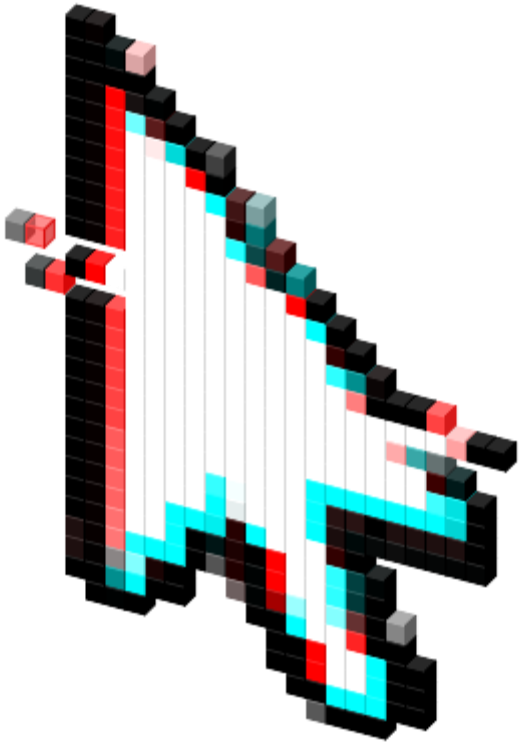


Part 2
기대 효과

Part 2

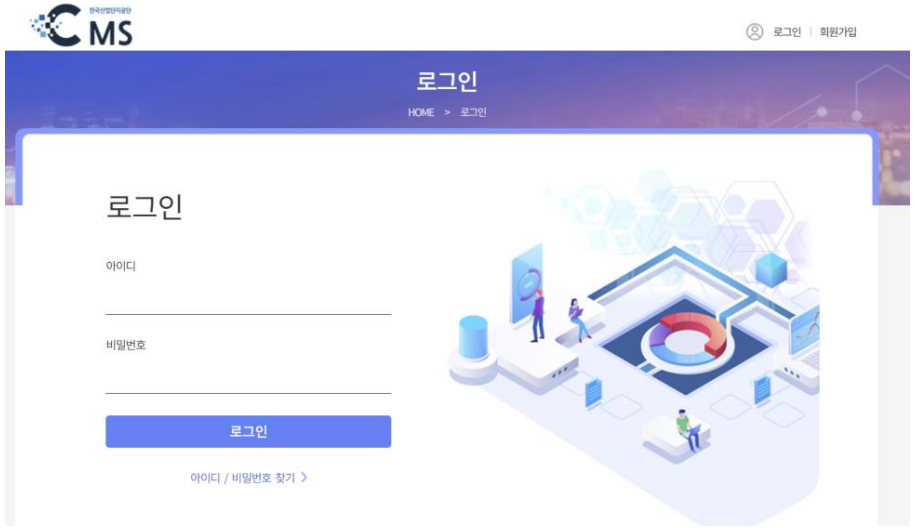
1. 주요 사업

한국산업단지공단에서 아직도 진행중인 주요 사업에 관한 내용이기 때문에, 수신자는 메일을 클릭할 수 밖에 없습니다.

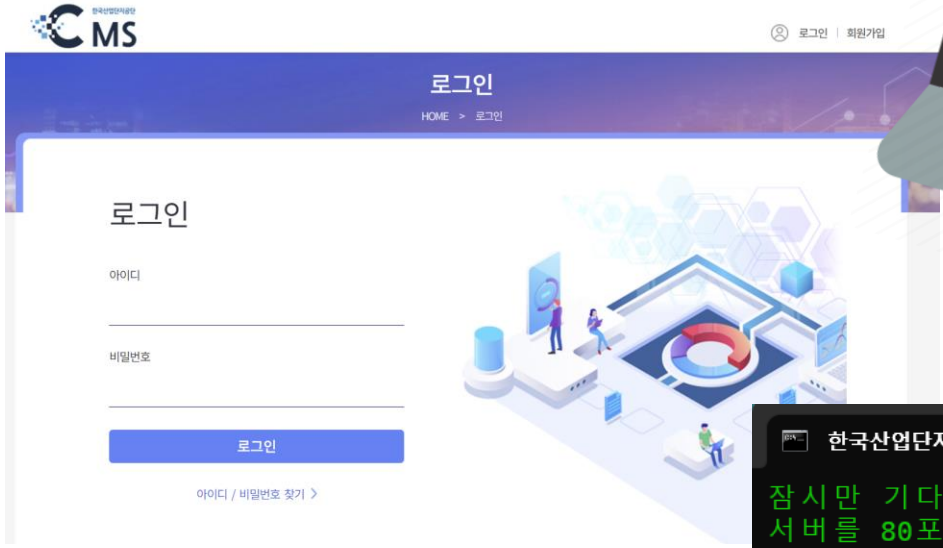


Part 2

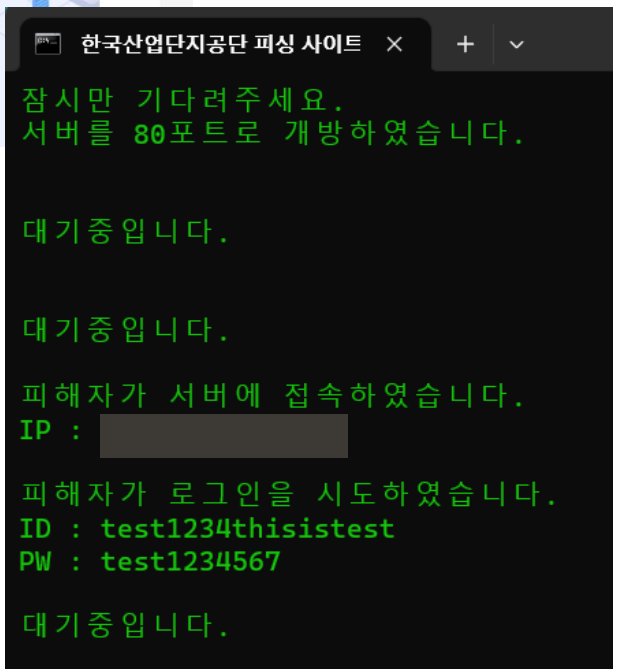
2. 비슷한 UI



한국산업단지공단 사이트



제작된 피싱 사이트



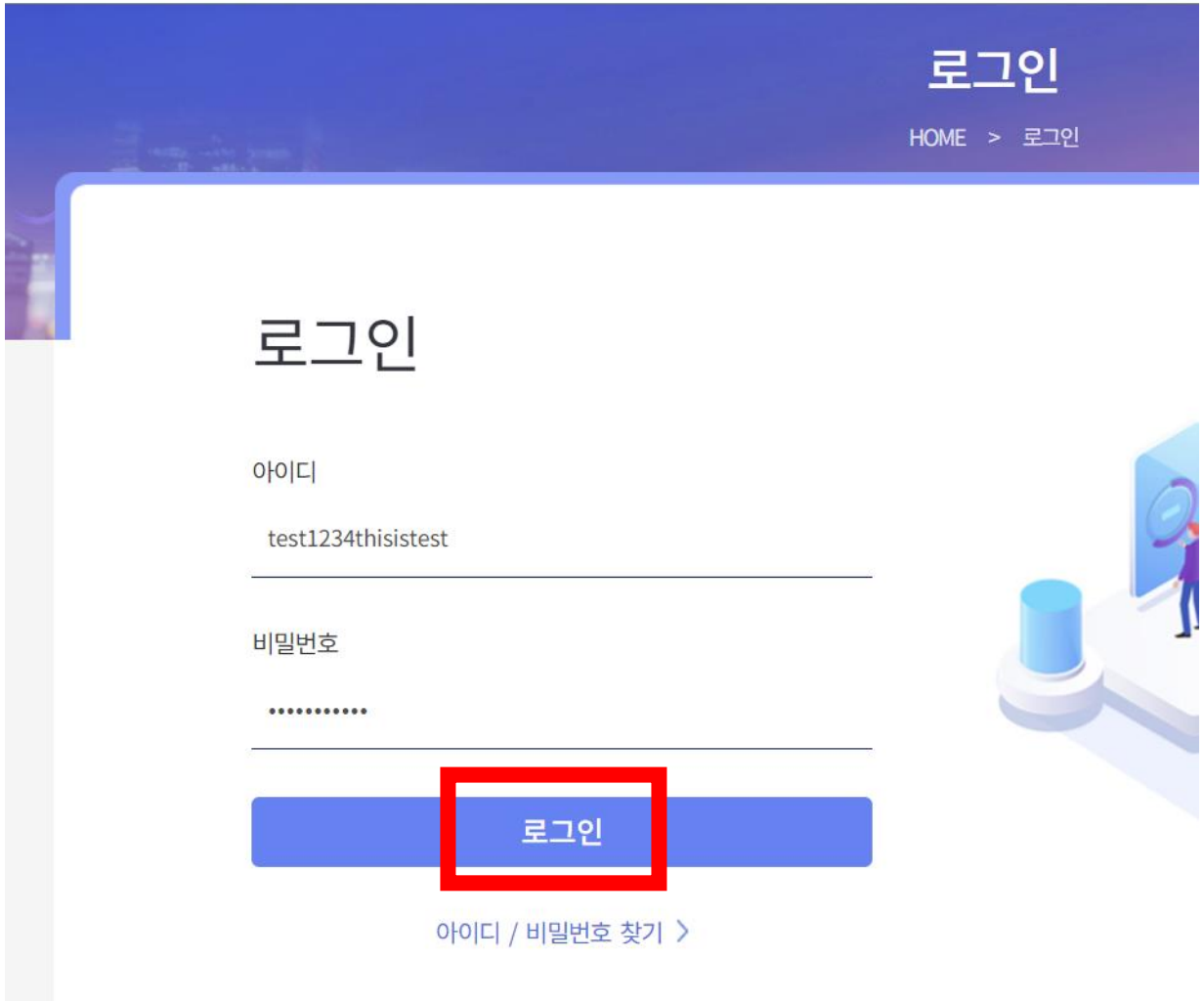
피싱 사이트 로그인 로그

한국산업단지공단의 로그인 폼과 다르면
=> 사람들이 의심하여 로그인하지 않을 것입니다.

[최대한 비슷한 UI를 고려해 피싱 사이트로 유도]

Part 2

3. 기업의 기밀사항 유출



피싱 사이트로 유도해 받은 개인정보로
한국산업단지공단 시스템/웹메일에 로그인

=> 중요한 기밀 문서,
중요 편지함 유출로 이어집니다.

Part 3
피해 발생 및 2차 피해

Part 3

1. 피해 발생

위 공격으로 인해 한국산업단지공단에선,
중요한 기밀정보가 유출되어, 정부의 신뢰를 잃고,
또한 기밀 중 신기술이나 이런 것들이 유출이 되게 된다면,
그 기업의 피해는 막심할 수 있습니다.

Hacked by Dogbo

TOP Secret

최첨단 탄소중립 신기술!!!!
유출함니다!!!!^^
64KY64qU7JW8lOqyjOyd
tOuLpC4

Part 3

2. 2차 피해

한국산업단지공단에서 공격을 받고 나서,
2차 피해를 줄이기 위해 해킹 메일 모의훈련을 실시할 수 있습니다.
이때, 모의훈련 결과라고 속인 PDF 파일에
악성코드를 삽입하여 전송합니다.
팀장급 관리자들은 직원을 통솔하기 때문에 결과를 확인할 수 밖에 없습니다.
의도적으로 PDF 파일을 열었을 때, 손상 된 파일이라는 메시지를 띄우고, 백그라운드에서 악성코드가 실행 되도록 합니다

Thank you.

Team - 자료만드느라배가고팟습니다

2023.10.14