한국산업단지공단

해킹메일 공격 아이디어 경진대회 기술발표

산업공단 낚는 낚시꾼들 (김신영 · 김수빈 · 최형빈)

2021.11.20

목차

A Table of Contents

01
팀 소개

팀 소개 About the team

산업공단 낚는 낚시꾼들 : 대구대 낚시 동호회

Daegu National University Fishing Club
Fishermen fishing at the Korea Industrial Complex

Private data + Fishing = Phishing

한국산업단지공단을 향한 고도의 Email-Phishing을 통해
성공적으로 산업공단에 낚을 해킹아이디어를 발표하며
산업공단을 순식간에 속일 수 있을 만큼의 전문적인
Email-Phishing에 대한 전문성과 애정을 표현하는 팀명

팀원 소개 About the team members

김신영 팀장

(현) 대구대학교 정보보호영재원 고등전문B
정보보호영재원 3년 연속 재학
대구중앙고등학교

김수빈

(현) 대구교육청 진로진학플랫폼 개발위원
팀 담쟁이숲 Relations Manager
2021 삼성주니어창작대회 입상
경북대학교 사범대학 부설고등학교

최형빈

(현) KITRI BoB 10th 보안컨설팅 트랙
(전) 대구대학교 정보보호영재원 고등전문B
2021 가명정보활용대회 우수상
경북대학교 사범대학 부설고등학교

02
공격기법 소개

공격기법 배경 Background of Phishing technique

코로나19 와 관련한 가짜뉴스 유포가 진화하고 언론사나 공공기관을 사칭한 허위 정보에서부터 특정 업체에 대한 명예훼손 또는 업무방해 소지가 있는 정보까지 출처를 알 수없는 정보가 빠르게 생산되고 퍼져나가고 있다.

또한 선거를 앞두고 불법적으로 여론을 조작하기 위해 언론사를 사칭하는 사례가 늘어나고 있음에 따라 정보화 사회에서 사칭에 대한 위험성과 심각성을 느꼈다.

우리 팀 '산업공단을 낚는 낚시꾼들'은 최근 이슈가 되고있는 대장동비리 사건과 같이 사회적으로 각광받고 있는 문제인 공정,비리 관련 이슈로 주제를 잡고 언론사를 사칭하여 피싱 공격을 하기로 계획하였다.

화천대유, 대장동 5개 블록 불법 수의계약…

대장동 논란이 던진 질문, '공공개발' 어떻게 해야 하나

하남 진출 명지병원 '특혜' 의혹…주민들, 비대좇 구성

감사원, 인천공항공사 스카이72 사업자 선정 관련 특혜 의혹 감사

[사진] 실제 최근 공정관련이슈 보도

한국산업단지공단

해킹메일 공격 아이디어 경진대회 기술발표

공격기법 내용 Phishing technique content

메일주소 spiritsbs@gmail.com

메일제목 [해명요청] SBS8 뉴스 인천뿌리산업중심 소부장 선정 과정 불법자금의혹 보도 전 최종 해명 요청 드립니다.

안녕하세요 SBS '끝까지 판다' 탐사보도팀 김관진 기자입니다.

본 취재팀은 한국산업단지공단의 대개조 산업중 '인천 뿌리산업중심 소부장' 선정과정에서 인천광역시청 도시계획국과의 불법 유착 및 불법자금의혹 관련 공익제보를 제보 받고

2개월간 탐사보도를 진행하였고, 탐사보도를 금일 SBS 8시 뉴스에서 단독보도할 예정입니다.

이와 관련해 본지는 한국산업단지공단의 해명과 의견을 묻고자, 유선 상으로 3차례 이상이나 문의드렸으나, 유선상으로도 연락이 닿지 않아 서면으로 한국산업단지공단 비리 관련 보도 최종 해명요청 드립니다.

본지의 SBS 8시 뉴스 최종 원고마감 시간인 19:00 까지 메일을 회신하지 않을 경우 탐사보도팀의 보도는 한국산업단지공단의 해명이나 의견은 일체 포함 되지 않은채로

금일 SBS 8시 뉴스에 보도 될 수 있음을 다시한번 통지해드립니다. *회신시에 담당부서/직책/성함/전화번호 남겨주시면, 본 취재팀에서 연락드리겠습니다.

감사합니다. 좋은하루되세요

SBS 탐사보도팀 '끝까지 판다' 드림

김관진 기자 / spiritsbs@gmail.com

첨부파일 한국산업단지공단 불법 비자금조성 핵심 자료 (외부용).hwp

공격기법 소개 (1) About Phishing technique (1)

메일주소 spiritsbs@gmail.com

메일제목 [해명요청] SBS8 뉴스 인천뿌리산업중심 소부장 ... (중략)

안녕하세요 SBS '끝까지 판다' 탐사보도팀 김관진 기자입니다.

본 취재팀은 한국산업단지공단의 대개조 산업중 '인천 뿌리산업중심 소부장' 선정과정에서 인천광역시청 도시계획국과의 불법 유착 및 불법자금의혹 관련 공익제보를 제보 받고 2개월간 탐사보도를 진행하였고, 탐사보도를 금일 SBS 8시 뉴스에서 단독보도할 예정입니다.

…… (중략)

[사진] SBS 뉴스 탐사보도 전문팀 '끝까지 판다'

실제 SBS 소속 탐사보도 전문보도 기자명과 이메일 주소를 유사하게 사칭

- 탐사보도, 비리, 공정 관련 이슈를 전문적으로 취재하는 실제 기자 프로필 사칭
- 이메일 주소는 실제 기자가 사용하는 spirit@sbs.co.kr 과 유사한 spiritsbs@gmail.com 사용
- 실제 관련 이슈 보도 전문 사회부 기자 프로필을 사칭하여 대상자로부터 메일의 신뢰도 확보

[사진] 실제 김관진 기자의 프로필

공격기법 소개 (2) About Phishing technique (2)

메일제목 [해명요청] SBS8 뉴스 인천뿌리산업중심 소부장 선정 과정 불법자금의혹 보도 전 최종 해명 요청 드립니다.

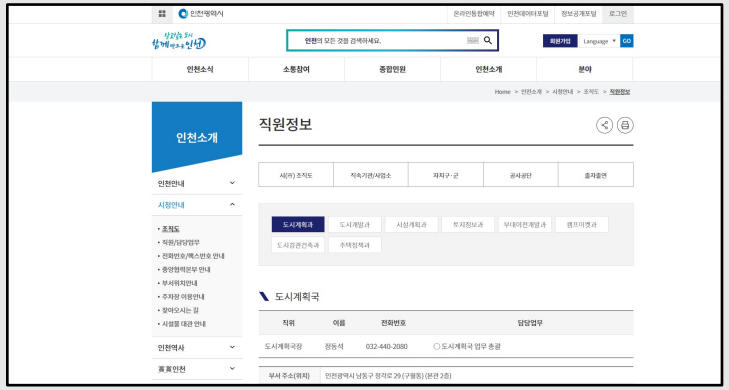
안녕하세요. SBS '끝까지 판다' 탐사보도팀 김관진 기자입니다.

본 취재팀은 한국산업단지공단의 대개조 산업중 '인천 뿌리산업중심 소부장' 선정과정에서 인천광역시청 도시계획국과의

불법 유착 및 불법자금의혹 관련 공익제보를 제보 받고 2개월간 탐사보도를 진행하였고, 탐사보도를

금일 SBS 8시 뉴스에서 단독보도할 예정입니다.

……(중략)



[사진] 해당사업 공동시행기관 인천광역시 도시계획국

실제 한국산업단지공단에서 추진한 구체적인 사업명과 시행기관 언급

- 비교적 관심도가 떨어지는 시기인 사업완료 후 1년 이상 경과된 사업명 언급
- 사업 공동 시행기관의 구체적인 부서명과 '불법유착', '불법자금' 등의 자극적인 단어 사용

공격기법 소개 (3) About Phishing technique (3)

메일제목 [해명요청] SBS8 뉴스 인천뿌리산업중심 소부장 ... (중략)

안녕하세요 SBS '끝까지 판다' 탐사보도팀 김관진 기자입니다. …… (중략)

이와 관련해 본지는 한국산업단지공단의 해명과 의견을 묻고자, 유선 상으로 3차례 이상이나 문의 드렸으나, 유선상으로도 연락이 닿지 않아 서면으로 한국산업단지공단 비리 관련 보도 최종 해명 요청 드립니다. 본지의 SBS 8시 뉴스 최종 원고마감 시간인 19:00 까지 메일을 회신하지 않을 경우 탐사보도팀의 보도는 한국산업단지공단의 해명이나 의견은 일체 포함 되지 않은 채로 금일 SBS 8시 뉴스에 보도 될 수 있음을 다시한번 통지 해드립니다.

*회신시에 담당부서/직책/성함/전화번호 남겨주시면, 본 취재팀에서 연락드리겠습니다.

감사합니다. 좋은하루되세요

SBS 탐사보도팀 '끝까지 판다' 드림

김관진 기자 / spiritsbs@gmail.com

회신 기한 시간 및 보도예정 등의 대상자에게 강한 압박을 주는 내용 사용

- 최대 회신가능 기한 및 메일 회신에 대한 협박 및 압박성 내용사용
- '최종해명요청', '일체 포함되지 않는다' 등 자극적인 단어 사용
- 대상자에게 심리적 압박 및 심리적 혼란을 유발하는 강한단어 활용

공격기법 소개 (4) About Phishing technique (4)

메일제목 [해명요청]SBS8뉴스 인천뿌리산업중심 소부장 ...(중략)

안녕하세요 SBS '끝까지 판다' 탐사보도팀 김관진 기자입니다. ……(중략)

이와 관련해 본지는 한국산업단지공단의 해명과 의견을 묻고자, 유선 상으로 3차례 이상 이나 문의 드렸으나, 유선상으로도 연락이 닿지 않아 서면으로 한국산업단지공단 비리 관련 보도 최종 해명 요청 드립니다. 본지의 SBS 8시 뉴스 최종 원고 마감 시간인 19:00 까지 메일을 회신하지 않을 경우 탐사보도팀의 보도는 한국산업단지공단의 해명이나 의견은 일체 포함 되지 않은 채로 금일 SBS 8시 뉴스에 보도 될 수 있음을 다시 한번 통지 해드립니다.

*회신시에 담당부서/직책/성함/전화번호 남겨주시면, 본 취재팀에서 연락드리겠습니다.

감사합니다. 좋은하루되세요

SBS 탐사보도팀 '끝까지 판다' 드림

김관진 기자 / spiritsbs@gmail.com

메일 회신 유도 및 대상자 개인정보 탈취 및 수집을 위한 요청사항 사용

- 대상자가 회신한 개인정보를 통해 2차 공격, 다단계 공격에 활용
- 대상자 메일 회신유도를 통해 신뢰기반 사회공학적 해킹 활용
- 메일 회신시에만 본 문제를 해결 할 수 있다는 심리적 압박 유도

공격기법 소개 (5) About Phishing technique (5)

메일제목 [해명요청] SBS8 뉴스 인천뿌리산업중심 소부장 ... (중략)

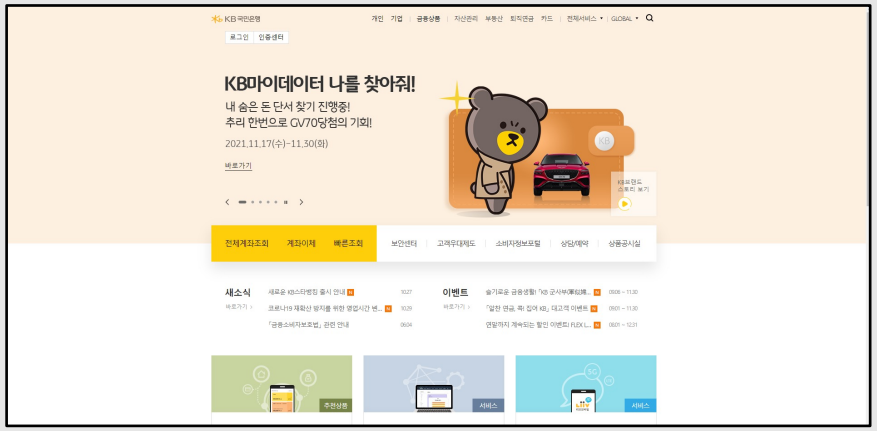
안녕하세요 SBS '끝까지 판다' 탐사보도팀 김관진 기자입니다. …… (중략)

감사합니다. 좋은하루되세요

SBS 탐사보도팀 '끝까지 판다' 드림

김관진 기자 / spiritsbs@gmail.com

첨부파일 한국산업단지공단 불법 비자금조성 핵심 자료 (외부용).hwp



[사진] DNS캐시오염을 통한파밍 사이트

본 보도와 관련된 핵심 자료를 사칭한 불법 악성파일 첨부파일 첨부

- '외부용' 키워드를 포함한 파일명으로 사용해 보도를 준비중인 내부 파일이 있는 것을 암묵적으로 암시
- 확장자명을 hwp로 감추고 있지만, 실제 확장자는 exe 형태의 악성스크립트 실행파일
- 악성코드 내 '백도어' 기능 부터 DNS 변조(오염)를 통한 '파밍' 등 추가적인 APT 공격 등 다양한 2차 공격의 시작점으로 활용 가능

한국산업단지공단

해킹메일 공격 아이디어 경진대회 기술발표

Similar Phishing technique

유사 공격사례

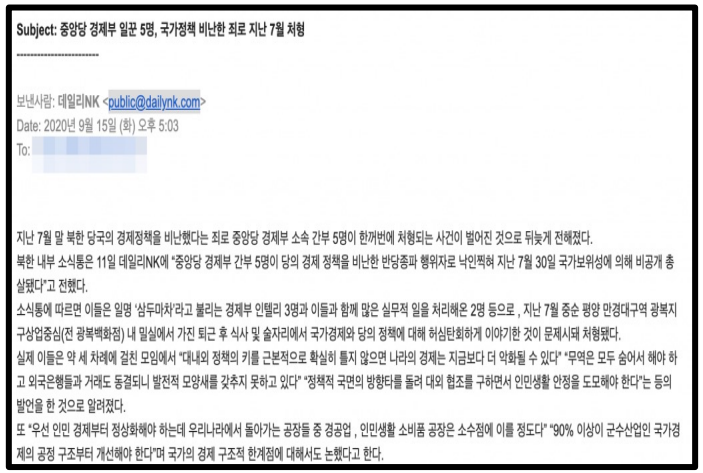
데일리NK 기자까지 사칭…
대북 단체장에 피싱 메일 발송돼

이광백 국민통일방송·데일리NK 대표와 김승철 북한개혁방송 대표에게 '국회 국방위보고서 본문'이라는 제목인 메일이 발송되었다.

분석 결과, 메일의 첨부파일은 실제 첨부된 파일이 아니고 해당 부분을 클릭하면 네이버 보안 인증을 위장한 새로운 창이 나타난다.

DAILK NK 문동희 기자

이번엔 데일리NK 사칭
피싱 메일 포착… 해커 소행?

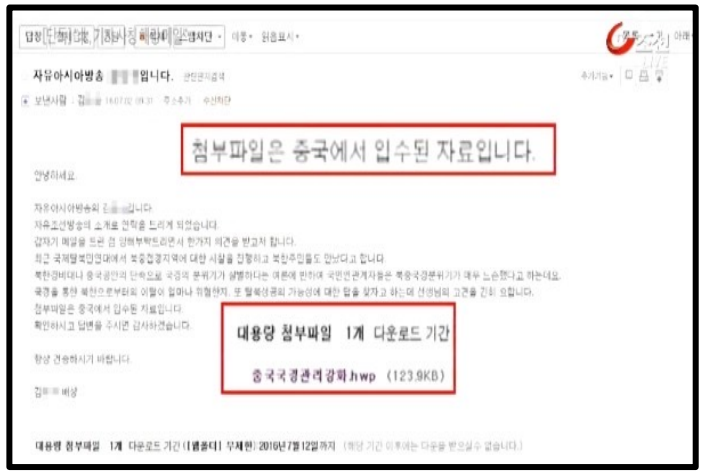


북한인권 NGO 대표에게 본사 기사를 활용하여 '중앙당 경제부 일꾼 5명, 국가정책 비난한 죄로 지난 7월 처형'이라는 제목인 메일이 발송되었다. 수신자를 속이기 위해 본지 기사 활용

분석 결과, 메일에서 악성 코드가 발견되지는 않았으나, 비콘이 발견되었다.

DAILK NK 문동희 기자

RFA기자 사칭 '해킹메일' 확산…
소행 추정



대북 방송매체 직원들은 '자유아시아방송(RFA)'의 김 모 기자이름으로 탈북의 위험성 및 성공 가능성에 대한 수신자의 의견을 구하는 내용 발송

중국국경관리강화'라는 이름의 MS 워드 파일 속에 악성코드가 있었으며, 열어 본 즉시 감염되었다.

NewDaily 노민호 기자

03
기대효과

기대효과 Expectation effectiveness

발생 가능 위험행위	파급력	발생 가능여부
대상자 이메일 열람	하	O
대상자 첨부파일 다운로드	중	O
대상자 정보 입력하게 하여 탈취	상	O
대상자 메일 회신 및 지속적인 신뢰구축	상	O

[표] 해킹메일을 통한 발생가능한 위험행위

신뢰관계를 기반으로 조직을 흔드는 사회공학적 해킹의 기반으로 활용 가능성!

가짜 전화번호, 가짜 명함 등의 다양한 기법으로 기자를 지속적으로 사칭하여 다양한 조직 내부 자료를 탈취하거나 요구하며 조직에 혼란을 발생시키고 APT 공격과 같은 지능형 공격에 시작점으로 활용될 가능성이 있다.

Q&A

감사합니다

산업공단 낚는 낚시꾼들 (김신영 · 김수빈 · 최형빈)
2021.11.20