2023-1 2023년 상반기

사이버 보안 소식

경기교육사이버안전센터(GECSC)

경기도교육정보기록원

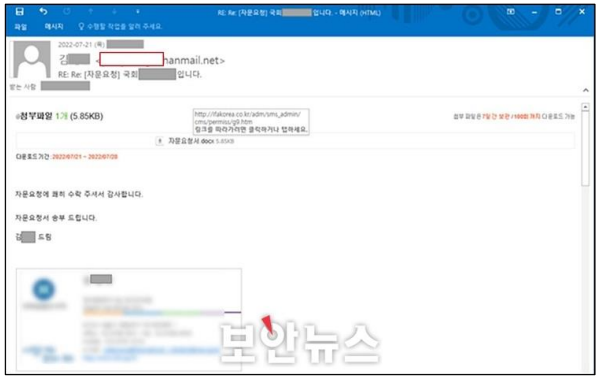
INDEX

별첨1) 경기교육사이버안전센터(GECSC) 사이버침해사고 대응

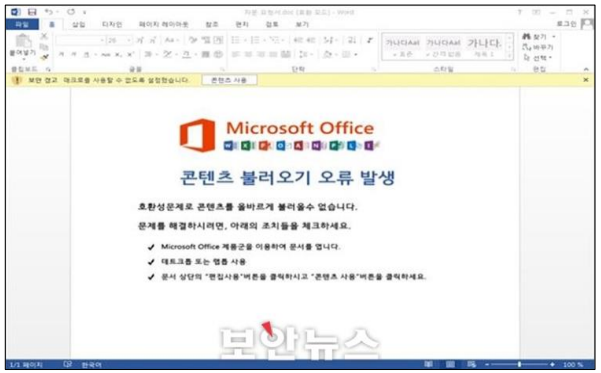
별첨2) 개인정보 유출사고 위험진단 / 최고의 개인정보취급자

해킹메일 사고 사례

□ "자문요청서" 파일첨부형 해킹메일 및 피해 사례

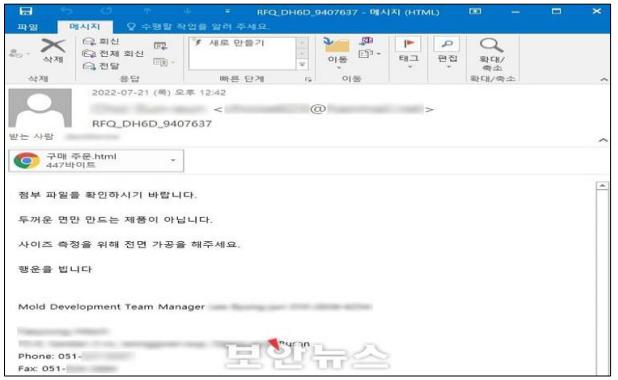


"자문요청서" 등 업무와 관련이 높은 문서 파일을 첨부하는 방식의 해킹메일을 발송



첨부된 문서 파일 실행 시 "콘텐츠 사용 알람" 발생, 해당 알람을 실행하면 악성코드가 다운로드됨 (랜섬웨어, 가상화폐채굴 등)

□ "구매주문"으로 위장한 해킹메일 및 피해 사례



"구매주문 수정" 등 업체 직원을 사칭하는 방식의 첨부 파일 삽입형 해킹메일을 발송

첨부된 파일 실행 시 미리 만들어진 위장페이지(피싱사이트)로 연결되어 포털 및 SNS 계정 정보 등 탈취 유도

- 출처: 과학기술정보통신부, 범부처 사이버보안 사고사례 홍보

https://www.boho.or.kr/kr/bbs/view.do?searchCnd=1&bbsId=B0000127&searchWrd=%EB%B2%94%EB%B6%80%EC%B2%98&menuNo=205021&pageIndex=1&categoryCode=&nttId=67085

해킹메일 예방 방법

해킹메일이란?

Q. 해킹(피싱) 메일이란 무엇인가요? *(#해킹메일, #피싱메일)*

✓ 개인정보(Private data)와 낚시(Fishing)의 합성어로

✓ 메일을 통해 이용자의 PC를 악성코드로 감염시키거나 임의의 URL로 접속을 유도하여 주요 정보를 탈취하는 해킹 기법입니다.

Q. 어떻게 악성코드 감염 등 피해가 발생하게 되나요? *(#감염경로)*

✓ 메일의 본문에 포함된 신뢰할 수 없는 URL 링크를 클릭하거나 악성행위가 포함된 첨부파일을 실행할 경우 감염되게 됩니다.

Q. 해킹메일을 통해 어떠한 피해가 발생하게 되나요? *(#해킹메일 피해)*

✓ URL 링크 또는 첨부된 파일을 통해 악성코드에 감염되거나 웹페이지로 정보 입력을 통해 정보가 외부로 유출되게 됩니다.

Q. 해킹 메일이 주로 사용되는 내용, 유형이 있나요? *(#해킹메일 유형)*

✓ 개인의 경우 쇼핑·택배안내·연말연시 행사·이벤트 등 일상생활과 밀접한 정보로 위장하여 발송되고 있습니다.

✓ 기업의 경우 사업제안서·견적서 등 업무와 관련되거나, 협력업체 직원 등을 사칭하여 발송되고 있습니다.

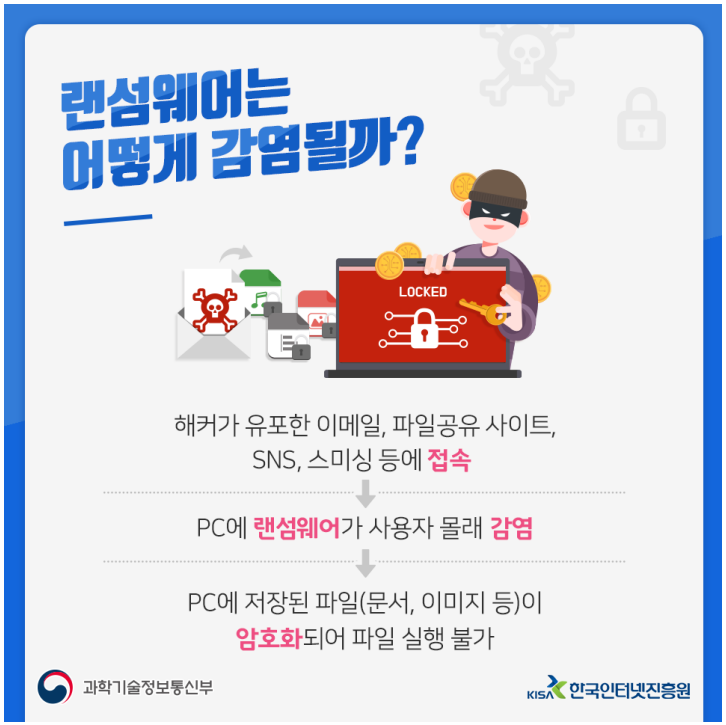
- 출처: 과학기술정보통신부, 범부처 사이버보안 사고사례 홍보
https://www.boho.or.kr/kr/bbs/view.do?searchCnd=1&bbsId=B0000127&searchWrd=%EB%B2%94%EB%B6%80%EC%B2%98&menuNo=205021&pageIndex=1&categoryCode=&nttId=67085

해킹메일 수신 시 유의 사항

- 출처: KISA 인터넷보호나라&KrCERT > 사이버위협 > 자세히 알아보기
https://www.boho.or.kr/kr/bbs/view.do?bbsId=B0000030&nttId=70087&menuNo=205027

랜섬웨어 감염 경로 및 증상

랜섬웨어 감염 경로



- ▶ 이메일, 파일 공유 사이트, SNS 등에 접속
- ▶ 악성코드 감염 이후 랜섬웨어 추가 감염
- ▶ PC내 저장된 파일이 암호화됨(문서, 이미지등)

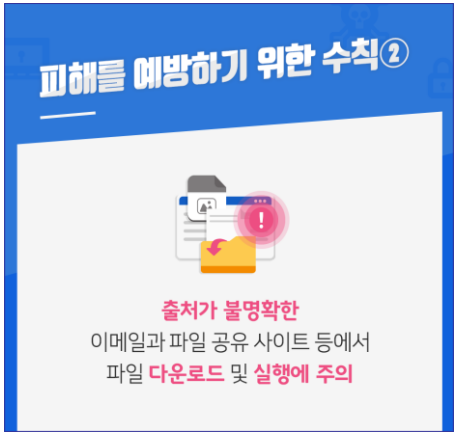
랜섬웨어 감염 증상

- ▶ 감염 파일 실행 불가 (파일 암호화)
- ▶ 화면 잠금, 키보드/마우스 동작 불가
- ▶ 시스템파일 손상, PC 재부팅 불가

- 출처: 한국인터넷진흥원 블로그 https://blog.naver.com/kisa118/221218861926

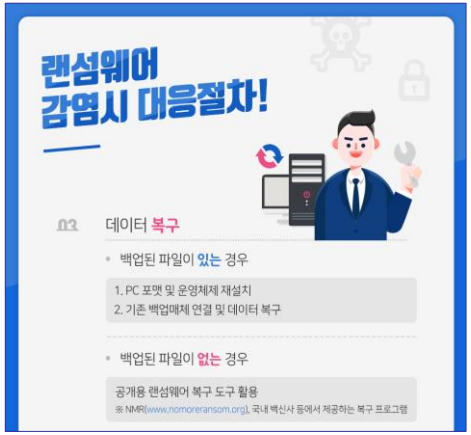
랜섬웨어 피해 예방 및 대응 절차

랜섬웨어 피해 예방 수칙



- ▶ 최신 버전 업데이트
- ▶ 출처가 불명확한 파일 다운로드 및 실행 주의
- ▶ 중요자료 정기적 백업

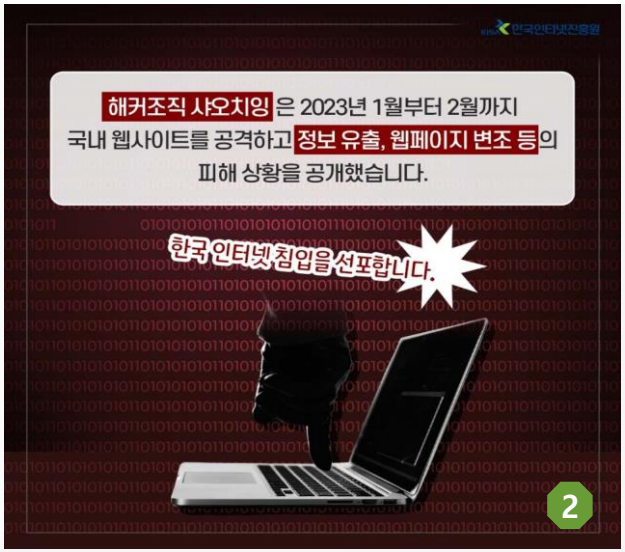
랜섬웨어 감염시 대응 절차

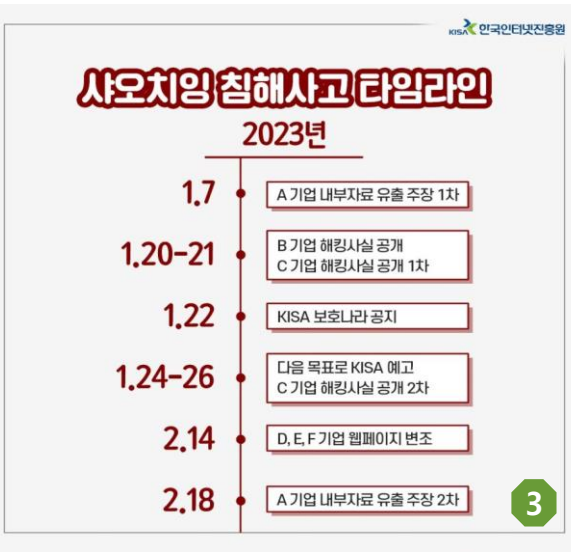


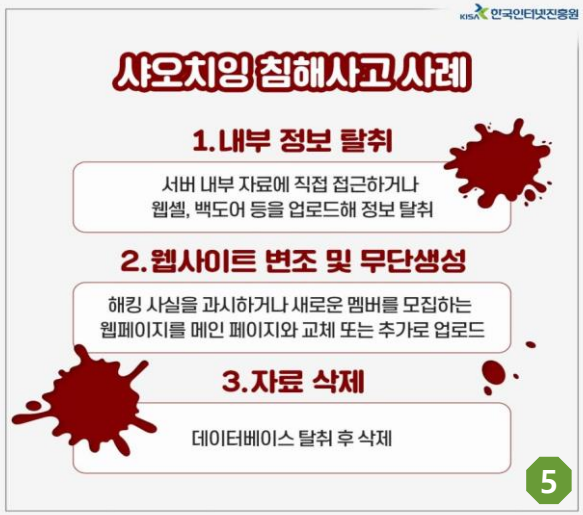
- ▶ 증상 확인
- ▶ 관련기관 신고
- ▶ 데이터 복구

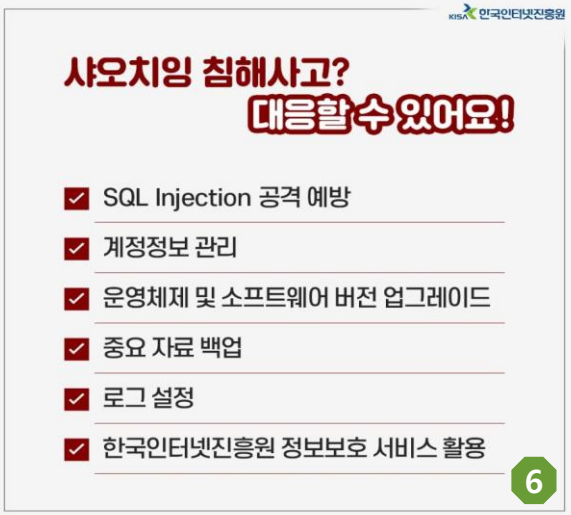
- 출처: 한국인터넷진흥원 블로그 https://blog.naver.com/kisa118/221218861926

샤오치잉 관련 침해사고와 대응 방안





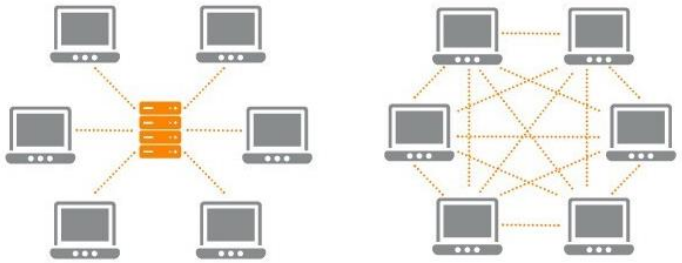




- 출처: 한국인터넷진흥원 블로그 https://blog.naver.com/kisa118/223085396557

P2P!! 사용 금지 해야된다!

P2P(Peer To Peer)에 대한 이해



(서버 기반 프로토콜과 P2P프로토콜 차이)

(다양한 종류의 토렌트 프로그램)

▲ 출처: https://focuskr.tistory.com/426

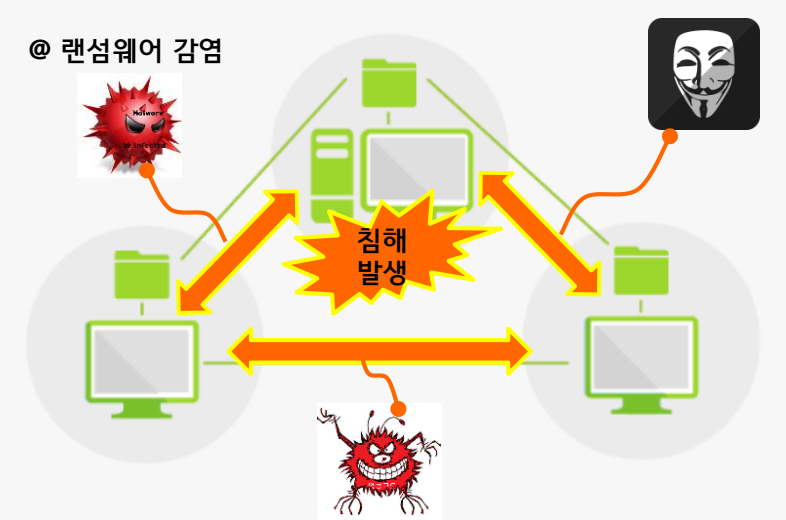
▶ P2P(Peer To Peer)는 ?

- 사용자 연결 구조로 서로 간 데이터 공유
- 기존 서버 환경 구조보다 빠른 데이터 전송
- 서로 간 데이터 공유 전달로 인한 연결 유지성 탁월
- 공유 파일의 조각 별 다운로드로 매우 빠른 다운로드 속도

사용 시 발생되는 문제점

- 서로 간 연결구조로 인한 악성코드 감염 증가
- 불완전한 파일 다운로드 시 랜섬웨어 / 해킹 위협에 노출
- 불법 파일 다운로드로 인한 저작권 침해
- 지속적인 연결 유지로 인한 내부 네트워크 부하 발생

@ 해킹, 정보유출



@ 악성코드 감염

2023년 상반기 보안 이슈 동향

2023년 1월 보안 이슈

- [보안뉴스] 넷서포트 RAT 악성코드, 포켓몬 게임으로 위장
- [보안뉴스] 구글 홈 스마트스피커, 도청 가능 취약점 발견
- [보안뉴스] 중국의 해킹 단체, 동아시아 단체들 공격
- [보안뉴스] 중국발 해킹 '디페이스 공격', 홈페이지가 바뀜

2023년 2월 보안 이슈

- [보안뉴스] 수강신청 페이지 해킹 시도, 컴퓨터공학과 학생들
- [보안뉴스] 中해커조직 추가공격예고 "다음 달 28일부터 韓공격"
- [보안뉴스] URL 단축 서비스인 지오링크를 피싱에 악용
- [보안뉴스] 작년 전국학력평가 응시생 성적 유출, 해킹 여부 수사

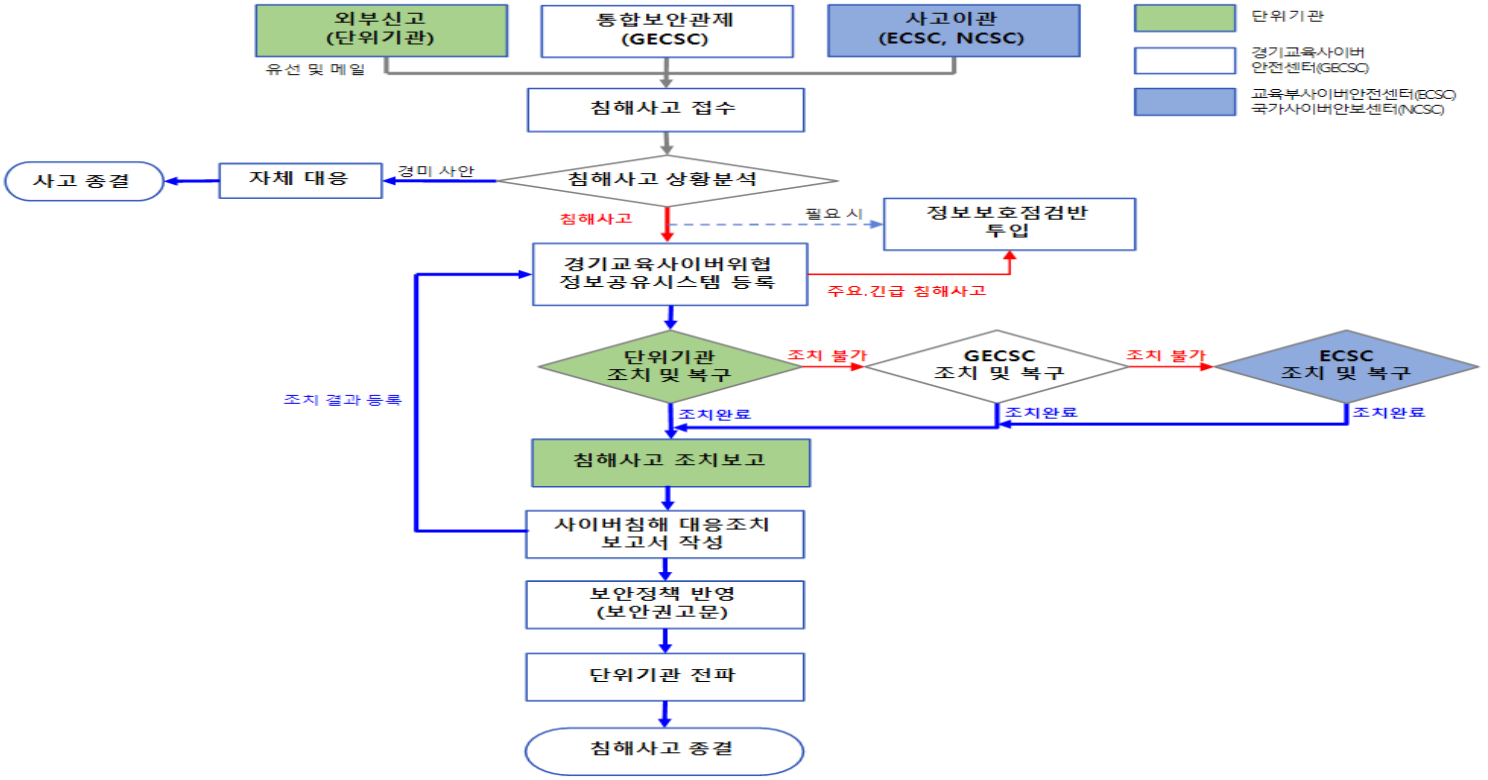
2023년 3월 보안 이슈

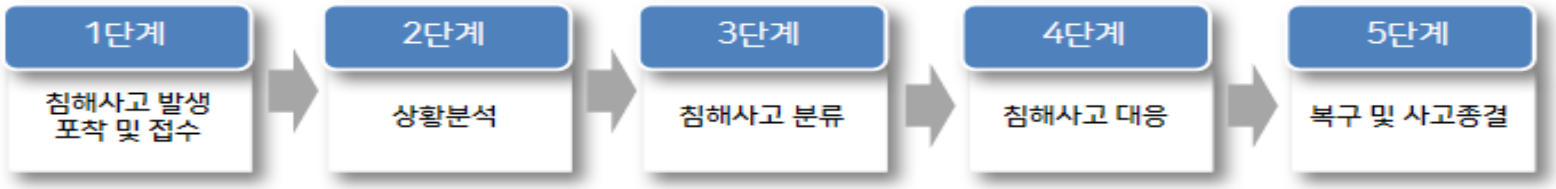
- [보안뉴스] 미국 연방보안청, 랜섬웨어 공격에 당해
- [보안뉴스] 금융정보 탈취 악성코드 이모텟, 이메일로 유포
- [보안뉴스] MS 스마트스크린 기능, 제로데이 통해 랜섬웨어 퍼져
- [보안뉴스] 김수키 해킹그룹, 사례비 지급 위장한 악성코드 퍼뜨려

2023년 4월 보안 이슈

- [보안뉴스] 트리고나 랜섬웨어, 관리 미흡 MS-SQL서버 통해 유포
- [보안뉴스] 보안인증프로그램 취약점 악용 해킹사건, 북한 소행
- [보안뉴스] 미국 CISA, 크롬과 맥OS서 발견된 취약점을 KEV에 추가
- [보안뉴스] 레드아이즈 공격그룹, 록랫 악성코드 링크 파일 통해 유포

[별첨1] 경기교육사이버안전센터(GECSC) 사이버침해사고 대응





◆ 출처: 경기도교육청 정보보호 업무 추진 계획 및 사이버분야 위기대응 실무 매뉴얼

[별첨2] 개인정보 유출사고 위험진단 / 최고의 개인정보취급자

◆ 출처: 교육부 개인정보보호 홍보용 자료

https://privacy.moe.go.kr/cop/pds/selectEduDataList.do?bbsId=BBSMSTR_000000000005