랜섬웨어 대응 가이드

2019. 8.

서강대학교
SOGANG UNIVERSITY

INDEX

01. 교내 랜섬웨어 피해사례

02. 랜섬웨어 감염증상

03. 랜섬웨어 감염경로

04. 랜섬웨어 감염 시 대응방안

05. 랜섬웨어 사전예방 및 대응절차

1. 교내 랜섬웨어 피해사례

▶ 최근 들어 교내 랜섬웨어 피해사례가 증가하고 있음

1) 매월 각 행정부서 및 연구실 PC 등에서 평균 4군데 감염 사례 발생(연간 50회의 피해사례 발생)

2) 이메일에 첨부된 파일실행 및 URL 클릭을 통한 감염사례가 가장 많이 발생

 # 사례 1.

본교 메일 관리자를 사칭 후
불법 URL 첨부하여 클릭 유도

제목	귀하의 이메일 계정 확인... 피하기 위해 폐쇄
보낸 날짜	2019/03/28 목요일 오전 11:11:11
보낸 사람	Sogang University
받는 사람	
참조	
첨부	

서강대학교
SOGANG UNIVERSITY

친애 하는

송강 대학교의 모든 직원 및 학생에게 활성 계좌를 확인하고 있음을 통보하는 것입니다.

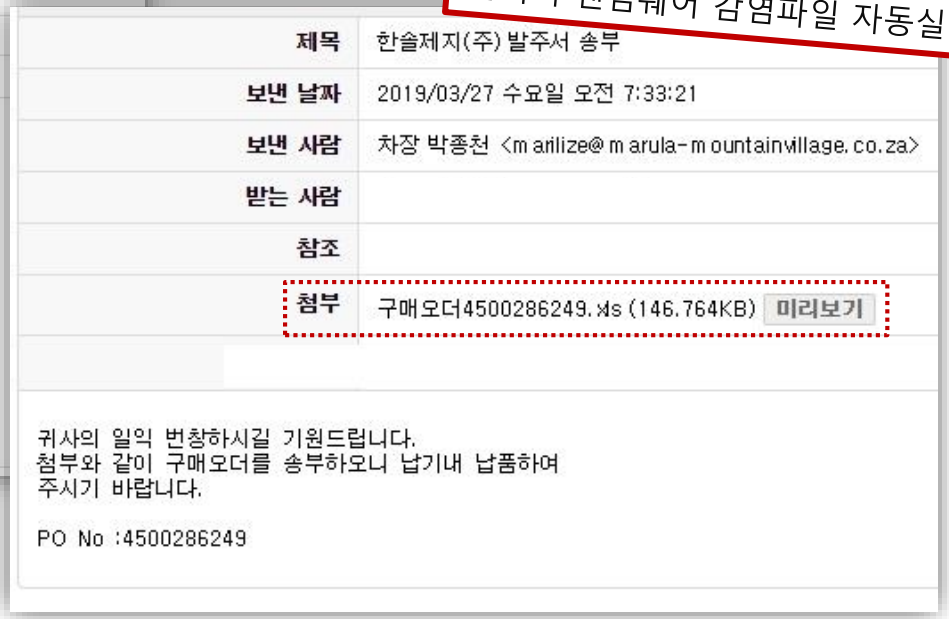
아래의 확인 링크를 클릭 하 여 계정을 계속 사용 중인지 확인 하십시오:

이메일 계정 확인

진심으 로,
메일 관리자.

 # 사례 2.

메일 내 불법 첨부파일을 송부하여
클릭시 랜섬웨어 감염파일 자동실행



제목	한솔제지(주) 발주서 송부
보낸 날짜	2019/03/27 수요일 오전 7:33:21
보낸 사람	차장 박종천 <marilize@marula-mountainvillage.co.za>
받는 사람	
참조	
첨부	구매오더4500286249.xls (146.764KB) 미리보기

귀사의 일익 번창하시길 기원드립니다.
첨부와 같이 구매오더를 송부하오니 납기내 납품하여
주시기 바랍니다.

PO No :4500286249

2. 랜섬웨어 감염증상

윈도우 탐색기 내
파일확장자 변형

이름	수정한 날짜	유형	
텍스트문서.txt.CRAB	2018-04-11 오후...	CRAB 파일	1KB
CRAB-DECRYPT	2018-04-11 오후...	텍스트 문서	5KB
사진파일.jpg.CRAB	2018-04-11 오후...	CRAB 파일	12KB
그림파일.png.CRAB	2018-04-11 오후...	CRAB 파일	15KB
한글문서.hwp.CRAB	2018-04-11 오후...	CRAB 파일	119KB
엑셀문서.xlsx.CRAB	2018-04-11 오후...	CRAB 파일	171KB
PDF문서.pdf.CRAB	2018-04-11 오후...	CRAB 파일	665KB
mp4파일.mp4.CRAB	2018-04-11 오후...	CRAB 파일	1,091KB
psd파일.psd.CRAB	2018-04-11 오후...	CRAB 파일	1,338KB
PPT문서.pptx.CRAB	2018-04-11 오후...	CRAB 파일	2,888KB
워드문서.docx.CRAB	2018-04-11 오후...	CRAB 파일	4,563KB
압축파일.zip.CRAB	2018-04-11 오후...		

복호화 비용 요구
(약 200만원)

3. 랜섬웨어 감염경로

▶ 랜섬웨어 감염경로

1 이메일
랜섬웨어를 유포하는 파일이 첨부되거나 다운로드 할수 있는 URL 링크 포함

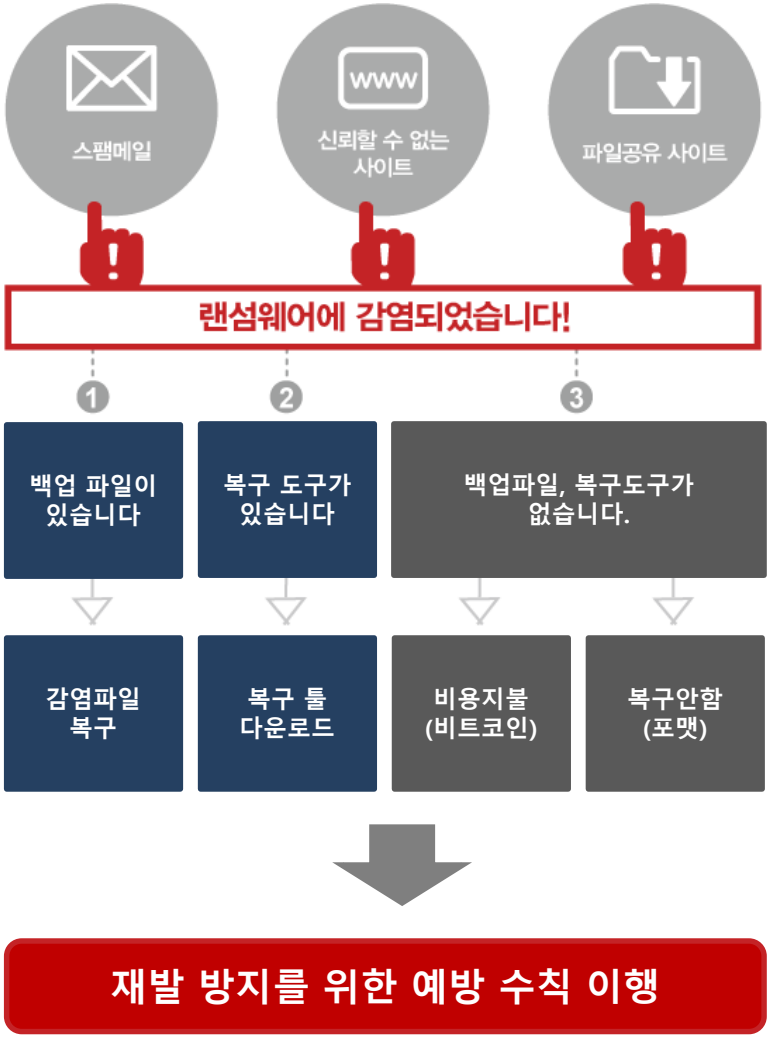
2 취약점 악용
보안이 취약한 웹사이트, 커뮤니티 등에 접속 시 PC 내 운영체제나 응용프로그램 취약점 이용

3 파일공유사이트
랜섬웨어를 포함한 위장파일(영화, 사진 등)이 존재하며, 이러한 파일 다운로드를 통해 감염

4 네트워크 전파
유/무선 네트워크 설정 미흡으로 인해 랜섬웨어 확산 및 감염

4. 랜섬웨어 감염 시 대응방안

▶ 랜섬웨어 복구절차



5. 랜섬웨어 사전예방 및 대응절차

▶ 랜섬웨어 피해예방수칙

1 모든 소프트웨어는 최신 버전으로 업데이트 하여 사용

- **보안업데이트가 제공되는 최신 버전의 운영체제 사용 및 매달 발표되는 보안 업데이트 적용**
  ※ 윈도우 XP, 비스타 등 보안 지원이 중단된 운영체제는 최신 버전으로 교체

- 사용하지 않는 불필요한 소프트웨어는 즉시 삭제

2 백신 소프트웨어를 설치하고, 최신 버전으로 업데이트

- **최신 업데이트를 유지하고 실시간 감시 기능 활성화 등 백신 소프트웨어가 정상적으로 동작하도록 설정**

- **주기적으로 PC 악성코드 검사 수행**

3 출처가 불명확한 이메일과 웹사이트 주소(URL) 실행 금지

- **수상한 이메일 열람과 첨부파일 실행, URL 클릭 절대 금지**

- 이메일에 첨부되어 있는 스크립트(JS, JAVA 등)나 실행파일(EXE, SCR, VBS 등) 실행 금지

5. 랜섬웨어 사전예방 및 대응절차

▶ 랜섬웨어 피해예방수칙

4 파일 공유 사이트 등에서 파일 다운로드 및 실행에 주의

- **영화, 음원 등 무료제공 사이트는 악성코드 및 랜섬웨어의 주요 유포지**

5 개인 PC 내 중요 자료는 정기적으로 백업 실시

- **업무 및 기밀문서, 각종 이미지 등 중요파일은 주기적으로 백업**
- 특히 중요파일은 PC 외에 외부 저장장치나 웹하드 등을 이용한 2차 백업 실시

5. 랜섬웨어 사전예방 및 대응절차

▶ 랜섬웨어 대응절차

1 증상확인

1) 파일 사용불가 : 평소 문제없이 열렸던 문서, 사진, 그림, 음악, 동영상 파일들 중 일부 혹은 전체가 읽을 수 없게 되거나 열리지 않는 현상이 발생

2) 파일 확장자 변경 : 파일의 이름과 확장자가 바 뀌거나 파일 확장자 뒤에 특정 확장자가 추가 된 것을 볼 수 있음

3) 부팅 불가능 : 사용하던 운영체제로 부팅이 되지 않고, 랜섬웨어 감염 사 실 및 금전요구 화면을 볼 수 있음

4) 바탕화면 변경 및 감염 알림 창 : 사용자의 파일이 암호화되었음을 알리고 이를 해제하기 위 한 비용과 지불할 방법을 보여주는 안내창을 볼 수 있음

2 긴급조치

1) 부서 문서함 및 외부 저장장치 연결 해제 : 랜섬웨어는 공유폴더, PC에 연결되어 있는 이동 식 저장장치(USB)나 외장하드 등에 저장되어 있는 파일에도 접근해서 암호화할 수 있으므로 즉시 연결 해제하기

- **네트워크 차단 :** 네트워크를 통해 랜섬웨어가 확산 될 가능성이 있으므로, 감염 사실 확인 시 네트워크 차단

5. 랜섬웨어 사전예방 및 대응절차

▶ 랜섬웨어 대응절차

3 신고하기

1) 화면 캡쳐하기 : 감염 알림창과 암호화 된 파일이 생성된 화면 캡쳐 및 저장

2) 신고하기 : 정보통신원 시스템운영팀(내선 8738)에 해당 사항을 신고하고 남겨놓은 증거물 (화면 캡쳐본)을 제출

4 데이터 복구하기

1) 랜섬웨어에 의해 암호화되지 않은 PC 또는 이동식 저장장치(USB)에 데이터 백업하기

2) PC 포맷 및 운영체제 재설치, SW 최신 보안 업데이트 적용

3) 기존 백업매체 연결 및 데이터 복구