컴퓨터 바이러스에 안전한

진료실 환경 만들기

(주)이지스헬스케어 / 김형록 개발팀장

강사소개

- ㈜이지스헬스케어 - 김형록
- 이지스 전자차트 개발팀장

eGHIS 이지스 의원용 전자차트 Extended Generation Health Information System ?

1991년	길병원 전산실 Dr's Order System 개발 및 유지보수
2000년	가천의대 길병원 전산실에서 ㈜엠씨씨로 사외분사 한국통신 EDI 서비스 사업 협정
2001년	기업 부설 기술 연구소 설립 (한국산업기술진흥협회)
2014년	차세대 OCS & EMR 솔루션 출시 의원용 전자차트 이지스(eGHIS) 솔루션 출시
2016년	㈜엠씨씨 에서 ㈜이지스헬스케어 분사

바이러스 & 랜섬웨어

"백신"과 "방화벽"만으로

컴퓨터 바이러스로 부터 안전한가?

바이러스 & 랜섬웨어

- 백신, 방화벽 만으로는 **"안심할 수 없다."**
- 공격패턴이 분석되어야
  백신 및 방화벽의 방어기술을 개발할 수 있다.
- 현재 안티 바이러스 솔루션은 모두 과거의 바이러스(패턴이 밝혀진 악성코드)를 탐지하기 위한 것이며 미래의 악성코드에 대응하기 어렵다.

바이러스의 종류

“知彼知己
百戰百勝”

1.컴퓨터 바이러스 (Computer Virus)

- 파일에 감염되어 해당 파일 또는 시스템을 파괴를 목적으로 하는 악성 프로그램
- 국가기관, 기업, 개인의 시스템을 공격하기 위함

2.웜 (Warm)

- 자체적으로 실행되어 시스템을 파괴하고 컴퓨터 처리 능력을 저하시키는 악성 프로그램
- 독자적 번식이 가능한 경우가 많으며 전파속도가 빠름

3.트로이목마 (Trojan horse)

- 개인정보의 삭제와 유출을 위한 악성프로그램
- 키보드 자판정보, 화면 스크린샷 등의 후킹을 통해 카드번호, 비밀번호 등의 “개인정보를 외부로 유출”하는데에 목적이 있음

4.스파이웨어 (Spyware)

- 정상 프로그램으로 위장하여 개인정보를 탈취하거나 원치 않는 광고를 유포하는 악성프로그램
- 무료프로그램 혹은, 불법경로로 다운로드한 프로그램
  (Windows,MS-Office 등)

5.랜섬웨어

- 몸값 (ransom) 과 소프트웨어(software)의 합성어
- 시스템을 잠그거나 데이터를 암호화한 후 일종의 몸값을 요구하는 악성 소프트웨어
- 랜섬웨어의 종류
  - 크립토락커
  - 워너크라이
  - 록키
  - 카카오톡랜섬웨어 등 다양화
- 비트코인의 등장으로 공격이 극심화
  (비트코인의 익명성)

5-1.랜섬웨어 특징

- 랜섬웨어에 감염되면 해당 컴퓨터의 모든 드라이브와 공유폴더의 지정파일 혹은 모든 파일의 확장자를 변경하고, 암호화 함

<워너크라이 랜섬웨어 감염사진>

의료 정보와
랜섬웨어

의료정보와 랜섬웨어

- **의료기관의 전산의존도가 점점 높아짐**
  - 개인정보, 진료정보, 검사결과, PACS 등

- **저장된 자료들의 가치가 매우 높음**
  가치가 높을 수록 복호화 비용을 지불할 가능성이 높음

- **전세계 의료산업에 대한 사이버 공격이 2016년 대비 64% 증가**

- **안티 바이러스 장비를 갖추지 못해 방어에 취약한**
  1차 기관(의원)의 경우 타겟이 되면 더욱 위험

랜섬웨어(바이러스) 침입경로

- **사례 1 - 택배송장 사칭메일**

- 오토크립터의 변종

- 정교하게 한글로 작성
  한국인이 개입되었을 가능성이 높음

- 주문자 정보가 해킹된 상황이었다면
  피해는 더욱 심각했을 것

랜섬웨어(바이러스) 침입경로

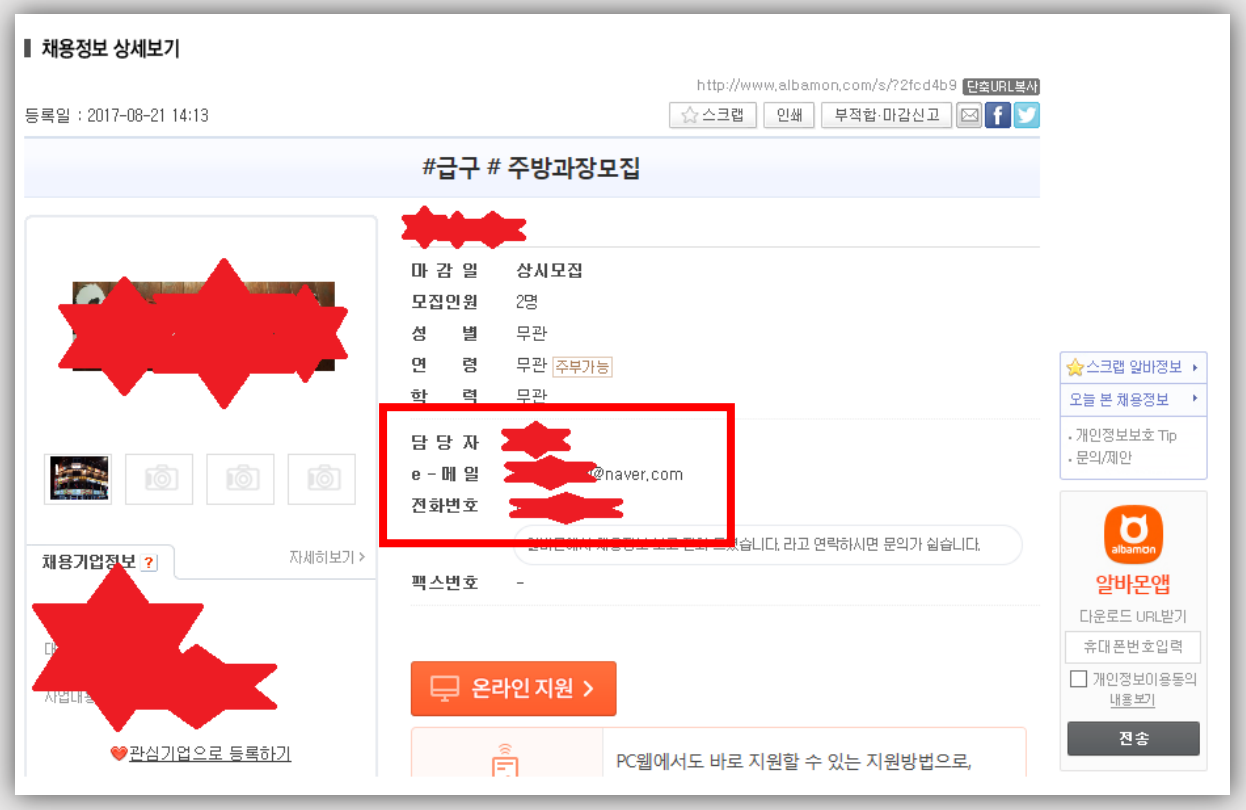
- 사례 2 – 알x몬 이력서 사칭메일

- 구직사이트의 구직글을 보고 노출되어 있는 이메일을 통해 사칭 메일 전송

- 첨부된 이력서를 통해 랜섬웨어 감염

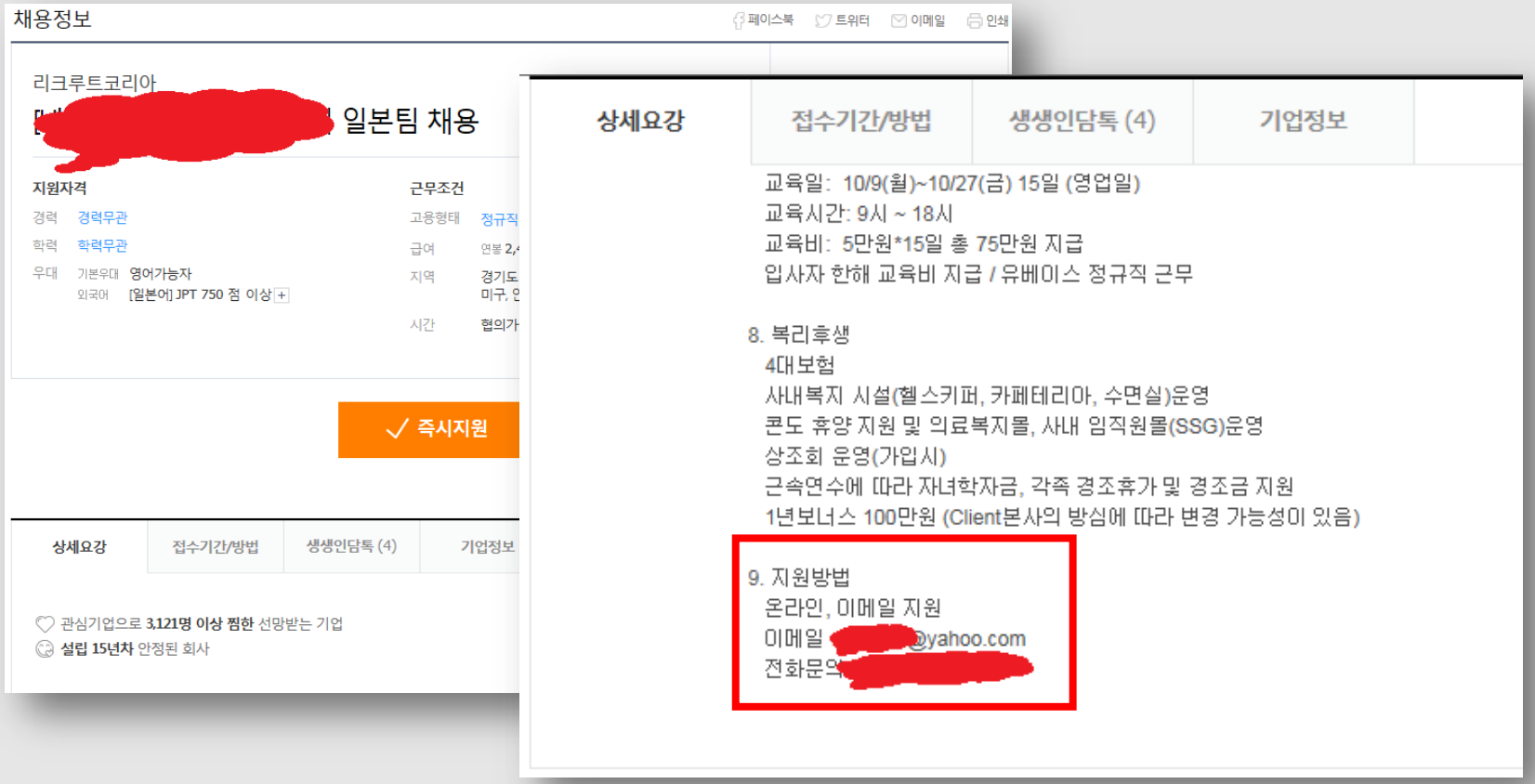
랜섬웨어(바이러스) 침입경로

- 사례 2 (상세)– 알x몬 검색 현황



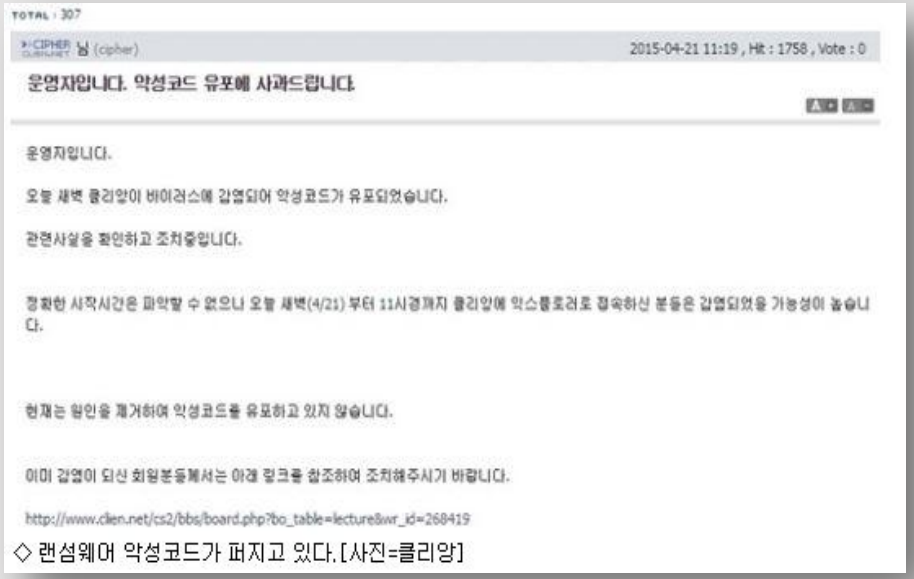
랜섬웨어(바이러스) 침입경로

- 사례 2 (상세)– 잡*리아 검색 현황



랜섬웨어(바이러스) 침입경로

- **사례 3 – 유명 게시판을 통한 유포**


TOTAL : 307

CIPHER 님 (cipher) 2015-04-21 11:19 , Hit : 1758 , Vote : 0

운영자입니다. 악성코드 유포에 사과드립니다.

운영자입니다.

오늘 새벽 클리앙이 바이러스에 감염되어 악성코드가 유포되었습니다.

관련사실을 확인하고 조치중입니다.

정확한 시작시간은 파악할 수 없으나 오늘 새벽(4/21) 부터 11시경까지 클리앙에 익스플로러로 접속하신 분들은 감염되었을 가능성이 높습니다.

현재는 원인을 제거하여 악성코드를 유포하고 있지 않습니다.

이미 감염이 되신 회원분들께서는 아래 링크를 참조하여 조치해주시기 바랍니다.

http://www.clien.net/cs2/bbs/board.php?bo_table=lecture&wr_id=268419

◇ 랜섬웨어 악성코드가 퍼지고 있다.[사진=클리앙]

- 클리앙 사이트의 광고에서 유포 (2015년 4월 21일 오전1시~11시)

- 광고를 클릭하면 악성프로그램 실행

- 클립토락커 바이러스 감염

- 회사원들이 자주 애용하는 커뮤니티 사이트의 감염으로 기업의 피해도 발생

- 감염 PC 당 약 40만원 지불요구 (현재 비트코인 가격 약 500만원)

랜섬웨어(바이러스) 침입경로

- **사례 4 – 온라인광고를 통한 유포 2**

<mp3 파일 변환 사이트 내 삽입된 위장 광고>

- 유투브 동영상 변환 사이트에 게시된 광고를 통한 감염사례

- 온라인광고 업체가 별도 존재하며 해당업체의 광고를 배너로 도입한 여러 사이트가 감염경로가 될 수 있음 (멀티바이징 수법)

- 광고가 주 수익원인 사이트에서는 많은 방법으로 광고의 클릭을 유도함

랜섬웨어(바이러스) 침입경로

랜섬웨어 감염에 이용되는 경로 TOP 5
1. 출처가 불분명한 이메일 첨부 파일
2. 변조된 웹사이트(배너광고 포함) 접속 시, 사용자 PC의SW 취약점 이용
3. '방송 다시보기' 해외 스트리밍 사이트
4. 토렌트 등 P2P 프로그램 통한 불법 자료 다운로드
5. 애드웨어 업데이트 서버 변조

(자료제공 : 이스트소프트)

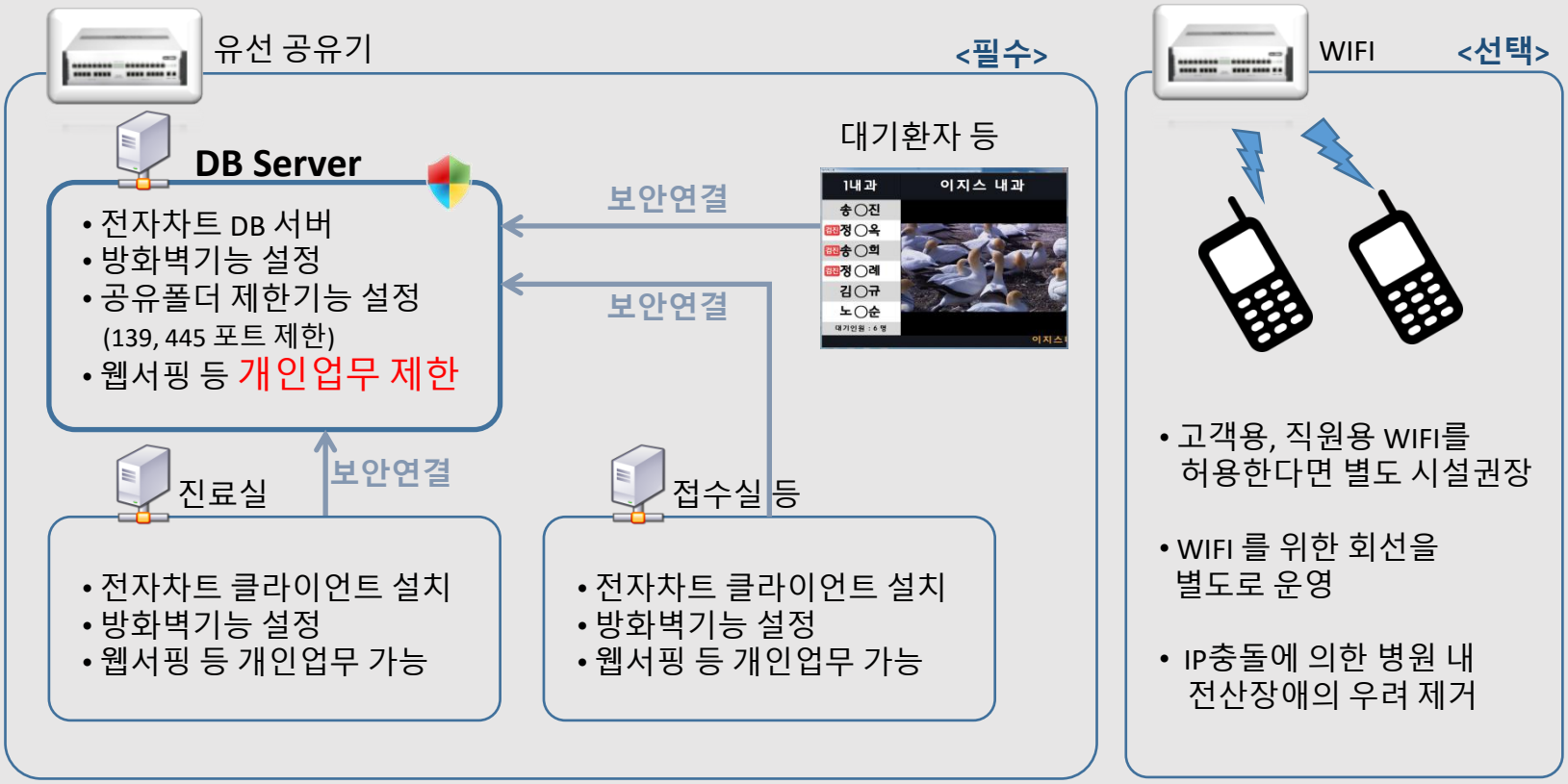
우리가 할 수 있는 대비책

랜섬웨어 대비책 – 1단계 (Windows)

1. 정품 OS(Windows) 사용
2. 단종된 OS 사용 자제
3. 윈도우 업데이트
4. 백신 프로그램 사용
5. 백신 최신 엔진 업데이트
6. 윈도우 방화벽 해제 금지
7. (가능하다면) 웹서핑용 네트워크 및 PC를 별도 설치

랜섬웨어 대비책 – 2단계 (네트워크)

7. 서버컴퓨터, 진료실컴퓨터 분리 운영



- 1차기관 환경에서 모든 컴퓨터에 공유폴더를 제한할 경우 프린터 공유의 장애가 발생할 수 있음
- 방화벽 설정 및 공유폴더 제한방법은 자료실(29p)에 윈도우 버전 별로 게시

랜섬웨어 대비책 – 3단계 (사용자)

8. 웹서핑 : IE 보다는 크롬, 파이어폭스 등
ActiveX사용 불가능한 웹브라우저 사용.
안전이 보장되지 않은 사이트 및 이메일 첨부파일 접근금지.

9. 토렌트 등 P2P 사용금지
불법소프트웨어 및 출처가 불분명한 프로그램, 웹하드를 통해
동영상, 음악 등 컨텐츠 다운로드 금지

랜섬웨어 대비책 – 4단계 (백업)

10. 전자차트, PACS 등 진료정보 **"백업 필수"**

- 1차. 서버 컴퓨터의 백업 (감염시 백업까지 위험)

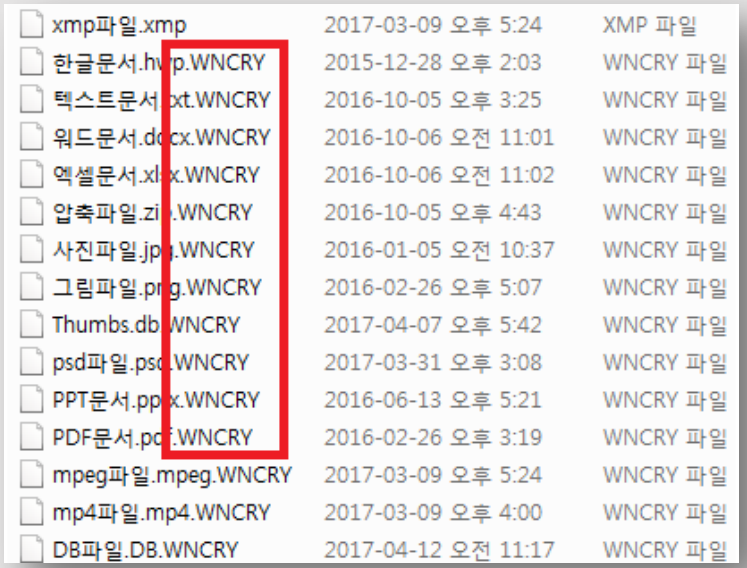
- 2차. 서버 외 클라이언트 컴퓨터에서 백업 **"필수"**
  (진료컴퓨터,접수컴퓨터 등)

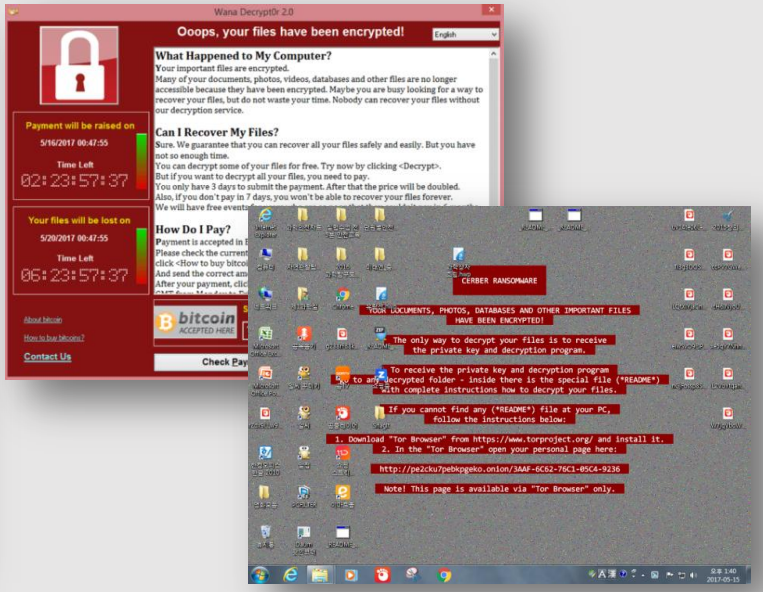
- 3차. 담당자는 백업 후 파일을 외장하드 등 물리적 공간에 복사 후 컴퓨터에서 분리보관

랜섬웨어에 감염 되었다면?

랜섬웨어 증상

- 컴퓨터의 부팅속도 및 구동속도가 저하됨
- 컴퓨터의 파일명이 일괄적으로 변경됨
- 실행할 수 없는 파일이 생김
- 바탕화면 또는 폴더마다 금전을 요구하는 페이지가 작성됨





랜섬웨어 대응법(1)

1. 감염된 컴퓨터의 네트워크를 신속히 분리
   (랜선분리, 확산속도를 늦추기 위해 컴퓨터를 종료하는 것도 좋음)

2. 감염된 컴퓨터가 서버라면, 서버 외 다른 컴퓨터에서 백업한 DB자료를 외장하드에 복사 후 외장하드 분리
   (전자차트 백업, PACS 백업 등, 평소의 백업 습관이 중요)

3. 서버 외 다른 컴퓨터의 백업이 없는 경우, 컴퓨터 내 모든 파일이 감염되기까지의 시간이 상당히 소요되므로 백업 데이터가 감염되지 않았을 가능성을 고려하여 서버 컴퓨터의 백업 및 자료를 외장하드에 복사 후 외장하드 분리

4. 자료가 확보되었다면, 감염된 컴퓨터를 포멧하고, 윈도우 재설치

5. 각 프로그램 담당자에게 의뢰하여, 확보된 백업파일로 서버 재설치

랜섬웨어 대응법(2)

1. 초기 대응에 실패한 경우, (백업이 확보 되지 않은 경우)
2. 원본 DATA가 회손되지 않도록 컴퓨터의 전원을 제거
3. 하드디스크를 분리하여 복구업체에 문의 (명*보기술 등 유명업체 권장)
4. 많이 알려진 랜섬웨어의 경우에는 금전지불 없이 복구되는 경우도 있음
5. 신종 랜섬웨어의 경우 금액을 지불하고 복구를 시도할 수 있음
6. 금액 지불 후 복구를 해 주지 않는 경우 발생할 수 있음
7. 복구율 또한 100%가 아닐 수 있음

관련자료

- **http://www.eghis.co.kr**

  PPT 및 관련 자료는 이지스 홈페이지주소 자료실에서 다운로드 받으실 수 있습니다.

  - "컴퓨터 바이러스에 안전한 진료실 환경만들기" PPT
  - 윈도우 버전 별 방화벽 및 공유포트 제한 가이드
  - 랜섬웨어 복구여부 판단 프로그램, 복구 프로그램
  - 안전한 네트워크 설계 가이드
  - 개인정보 자율점검 가이드
  - 기타 자료

**바이러스 및 악성코드가 나날이
지능화 되고 있습니다.**

미리미리 대비해야 소중한
진료정보를 안전하게
지킬 수 있습니다.

감사합니다