분석가와 관리자가 바라보는 랜섬웨어

Dalgomtaeng

dalgomtaeng@gmail.com

@dalgomtaeng

Who Am I ?

- 아직은 20대
- 분석가에서 관리자로, 이제는 설계자
- 관심사 : DFIR, 대규모 인프라 보안, 클라우드, 오픈소스, 육아(?)

목차

랜섬웨어

- **랜섬웨어란?**
  - **Ransom(몸값) + Ware(제품)**
  - **파일을 인질로 잡아 몸값을 요구하는 소프트웨어**

- 왜 핫한가?
  - 수요를 계속해서 창출
    - ✓ 공격자 입장에서는 전세계 인터넷 기기가 모두 고객
  - 쉽게 돈을 벌 수 있음
    - ✓ 가상화폐를 이용하고 구조가 단순

랜섬웨어 침해사례

랜섬웨어 침해사례

- **Case 1**
  - 지인 A의 PC의 일부 파일이 암호화
  - 확장자만 바뀐 파일도 존재
  - 암호화에 사용했던 키가 PC에 존재
    - ✓ 리버싱으로 해결!

랜섬웨어 침해사례

- **Case 2**
  - 지인 B의 회사 다수의 PC의 일부 파일이 암호화
  - 암호화 된 PC에서 랜섬웨어 및 유입 경로를 찾을 수 없었음
  - VSC(Volume Shadow Copy)를 이용하여 복구

- **Case 2**
  - 암호화 된 PC는 공유폴더를 사용 중이었으며, 암호화 된 파일 모두 공유폴더 안에 존재
    - ✓ 최초 감염된 PC에서 공유폴더를 암호화 함으로서 피해를 확산
  - 최초 감염자는 누구?
    - ✓ 같은 사무실의 C부장으로 컴퓨터가 느려지고 금전 요구화면에 위기 의식을 느끼고 포맷

랜섬웨어 침해사례

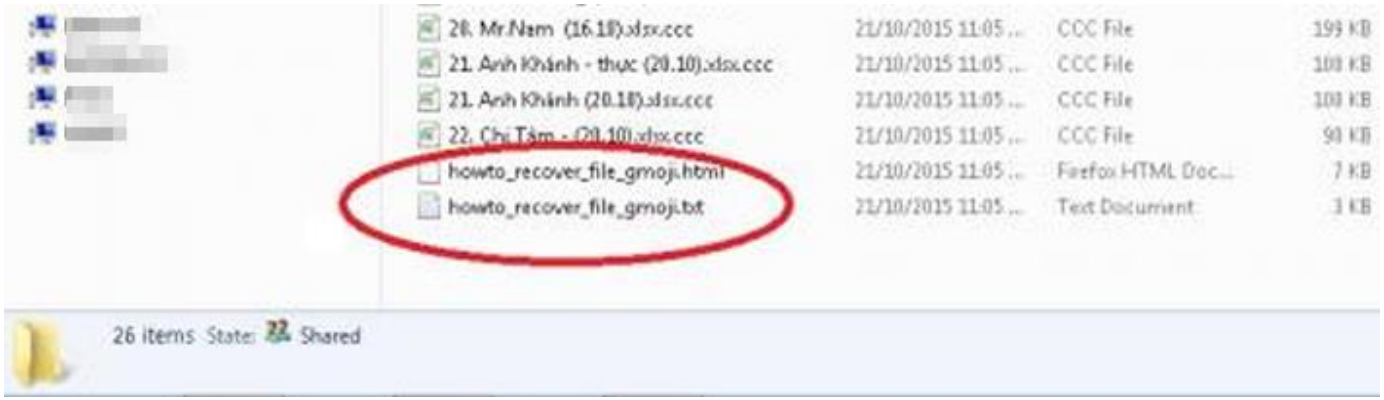
- **Case 3**
  - 지인 D의 회사 다수의 PC의 일부 파일이 암호화
  - 암호화 된 PC 모두에서 랜섬웨어 및 유입 경로를 찾을 수 있었음
    - ✓ 사내 ERP서버 해킹으로 인한 악성링크 삽입
  - 파일 복구 불가
    - ✓ 암호화에 사용된 키를 PC에 남기지 않음
    - ✓ 랜섬웨어가 VSC를 모두 삭제함



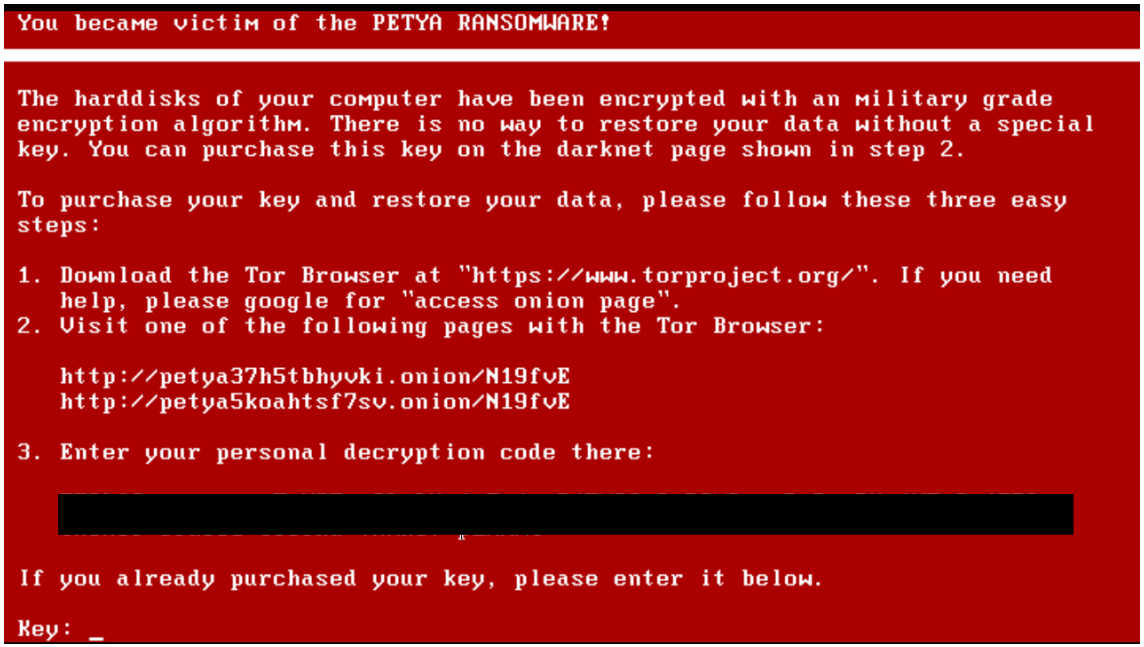
생각해 볼 것들

생각해 볼 것들

- 대응은 어찌하나?
  - 대규모 감염 시 최초 감염 PC선별 필요
    - ✓ 암호화로 생긴 파일의 시간이 제일 빠른 PC
    - ✓ 공유 폴더 외에서 암호화된 파일이 발견된 PC
    - ✓ 공유 폴더 내의 랜섬웨어 안내문을 생성한 사용자의 PC



- 대응은 어찌하나?
  - 랜섬웨어의 분석이 필요한가?
    - ✓ C&C 통신 확인으로 추가 감염자 확인 가능
    - ✓ 쉽게 복구 가능한 경우가 있음



생각해 볼 것들

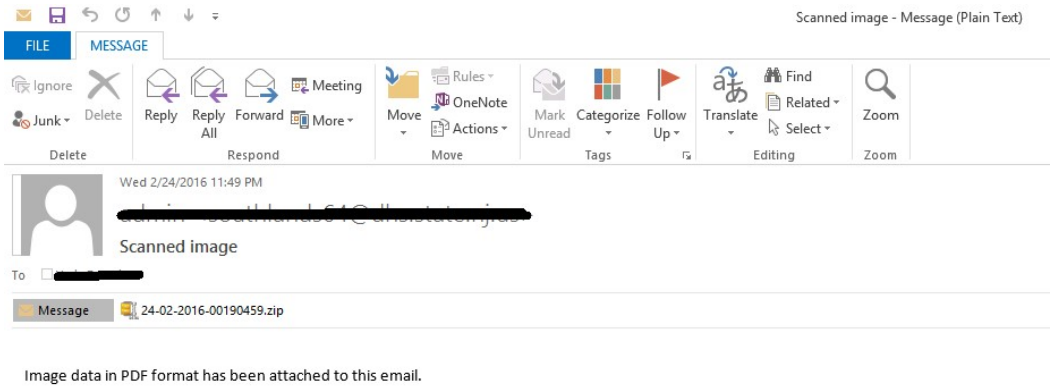
- 점점 복구가 어려워 진다
  - 암호화 키 자체 삭제
  - VSC 및 윈도우 백업 본 삭제
  - 암호화된 파일을 원본 파일에 덮어쓰기

생각해 볼 것들

- 돈을 주고 복구하면 될까?
  - 일종의 사업이라 신뢰가 중요
    - ✓ 몸값 지불시, 대부분이 복구됨
  - 신뢰할 사업자(?) 만 존재하는가?
    - ✓ 랜섬웨어는 제작이 쉬운편이라, 점점 다양해짐
    - ✓ 복구의 의무는 없음

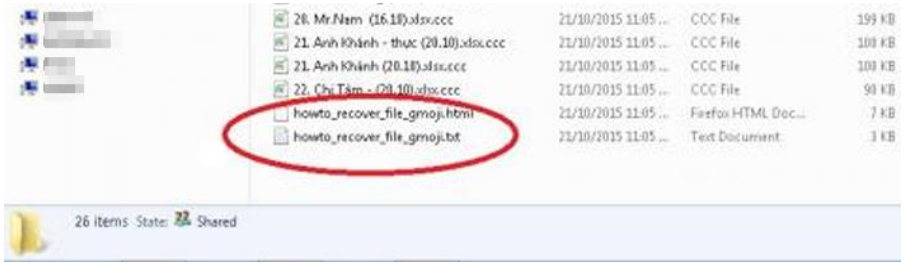
생각해 볼 것들

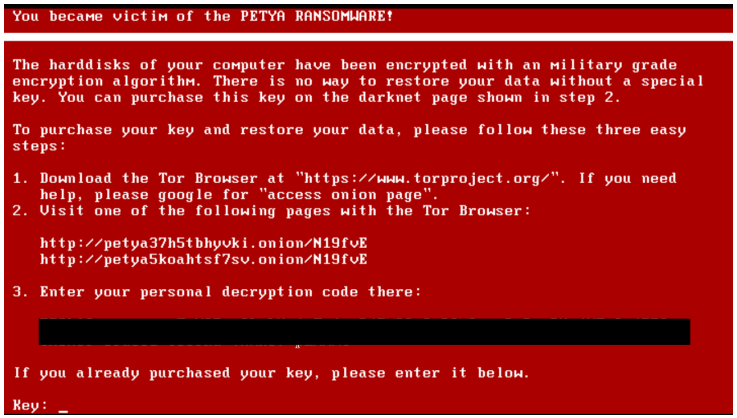
- 유입 경로의 다양화 및 AV우회
  - 스팸 메일
    - ✓ 비밀번호가 첨부된 파일 또는 문서가 아닌 파일로 AV우회
  - 악성 링크 삽입
    - ✓ 불특정 다수의 사람이 접근하는 사이트
    - ✓ 회사 내부 서버에 삽입



생각해 볼 것들

- 랜섬웨어가 무섭다
  - 다양한 암호화 알림 방식





생각해 볼 것들

- 랜섬웨어가 무섭다
  - 업무 관련 파일 암호화로 인해 은폐하려는 경우 발생
    - ✓ 교육과 홍보를 통한 인식개선
    - ✓ 네크워크 포렌식을 통한 분석

생각해 볼 것들

- 랜섬웨어 예방
  - 꾸준한 보안 업데이트
  - 수상한 첨부파일 열지 않기
  - 업무와 비업무의 분리

Question and Answer