중소기업 대상 신규 랜섬웨어(Midnight/Endpoint) 공격 주의 권고

□ 개요

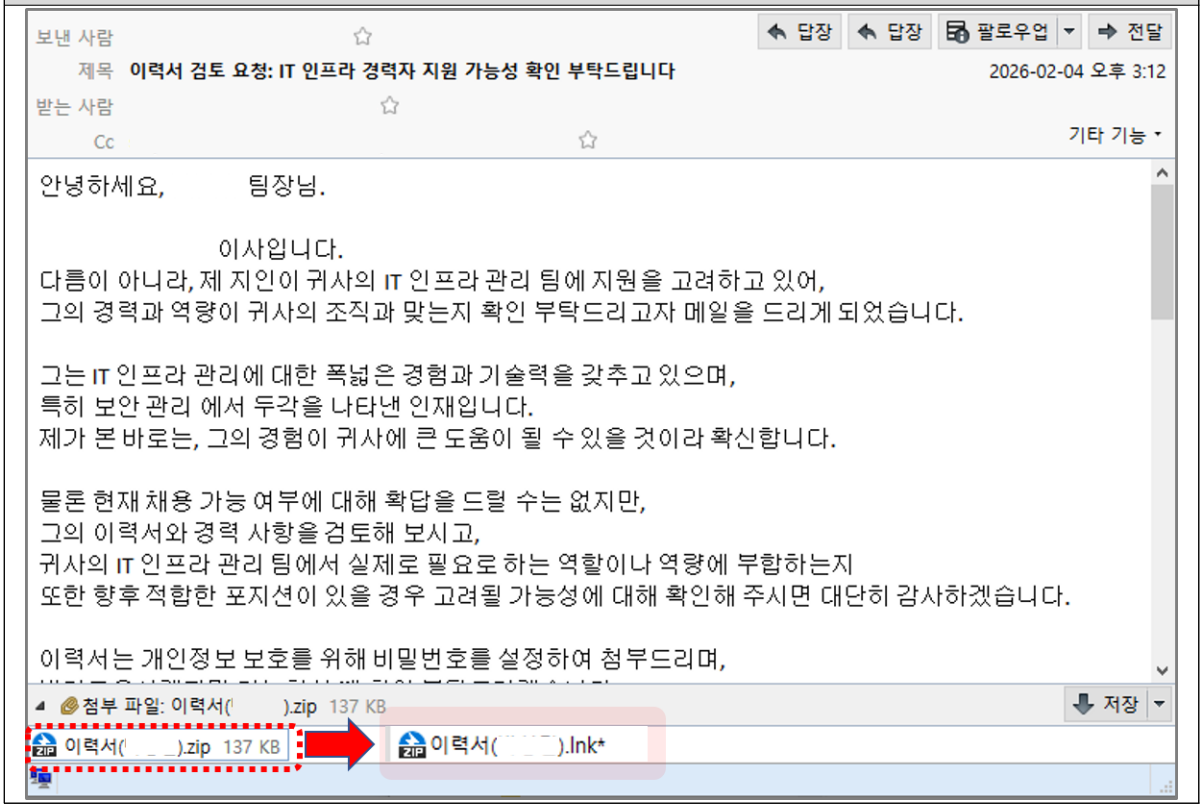
○ 최근 악성 이메일을 통한 Midnight(Endpoint) 랜섬웨어 피해가 급증하고 있으며, 피해가 발생하지 않도록 철저한 보안 점검 및 대비 필요

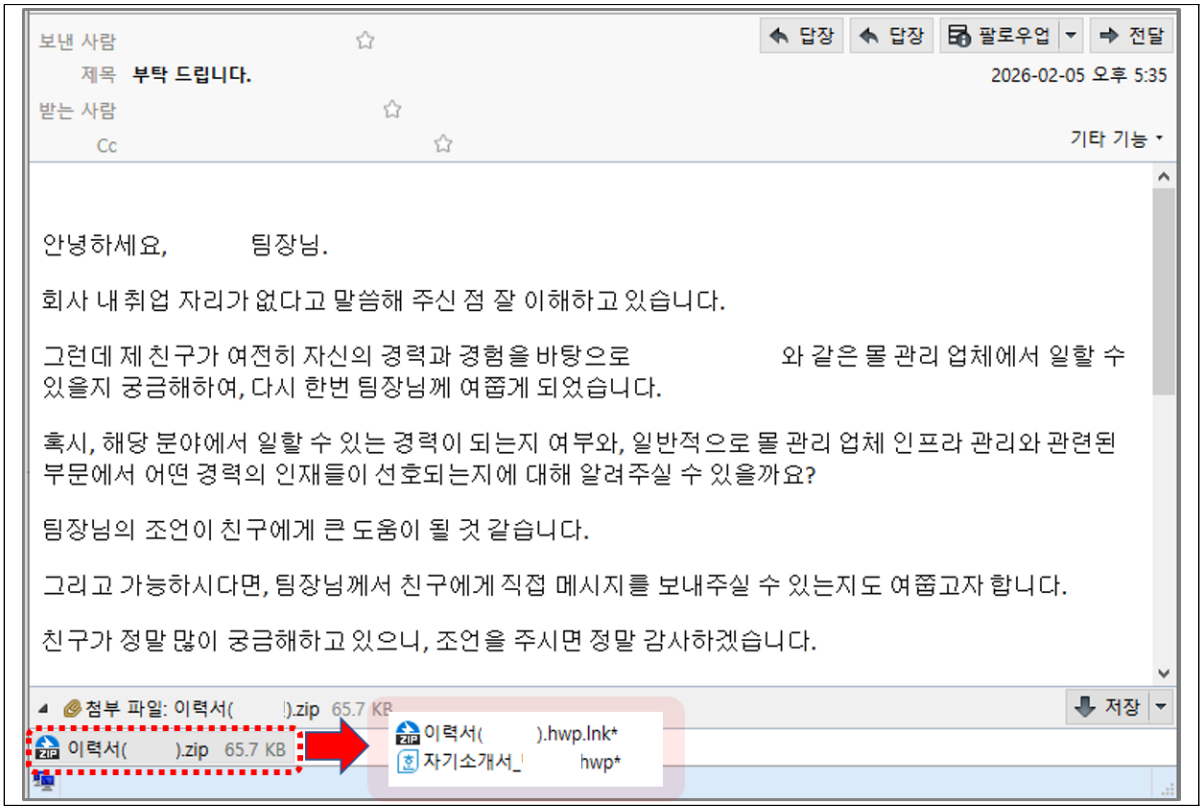
□ 주요 내용 - 랜섬웨어 침해사고 주요 사례

○ 악성 이메일을 통한 랜섬웨어 감염 및 주요 자료 유출

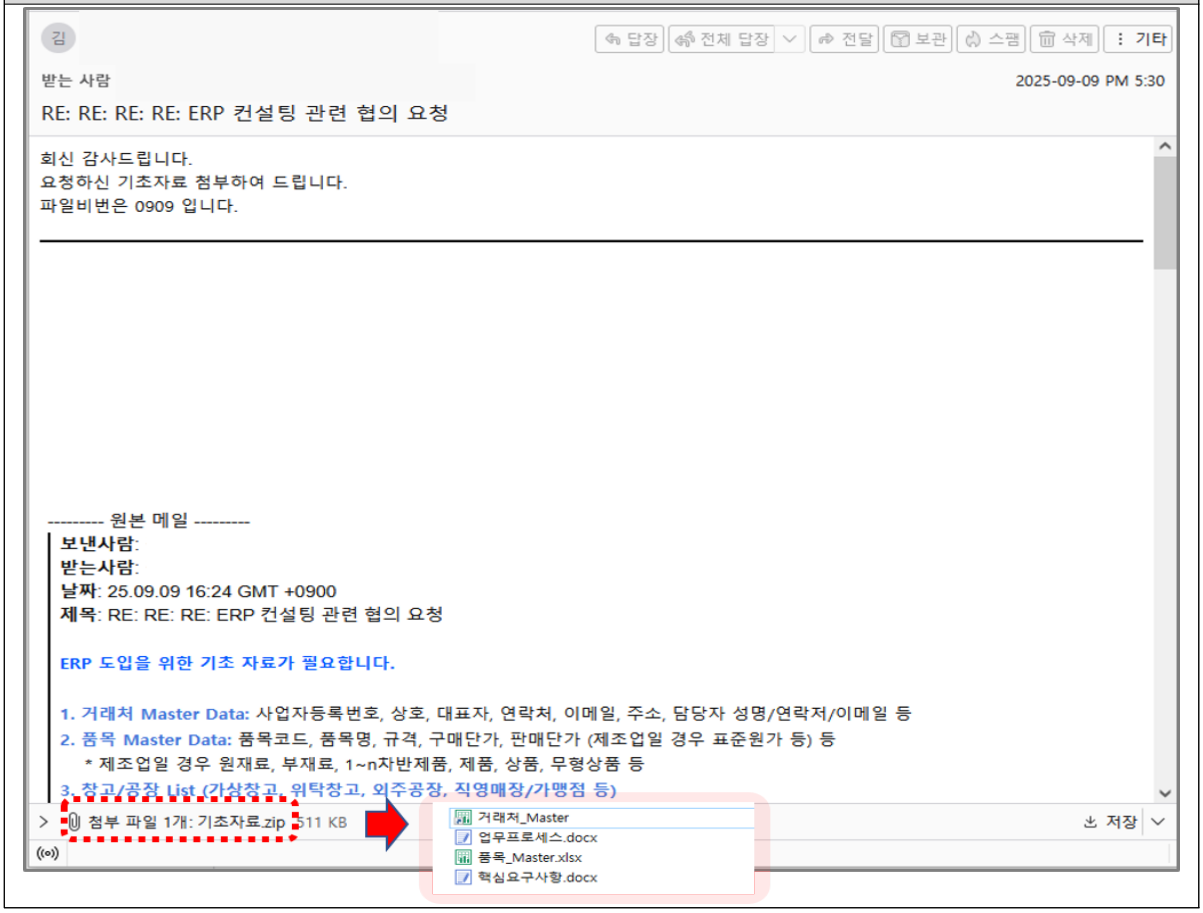
- [사례1] 공문, 이력서, 견적서 등으로 위장한 악성메일의 첨부파일(랜섬웨어) 실행

(1) 입사 지원 문의 – 이력서 위장 첨부파일



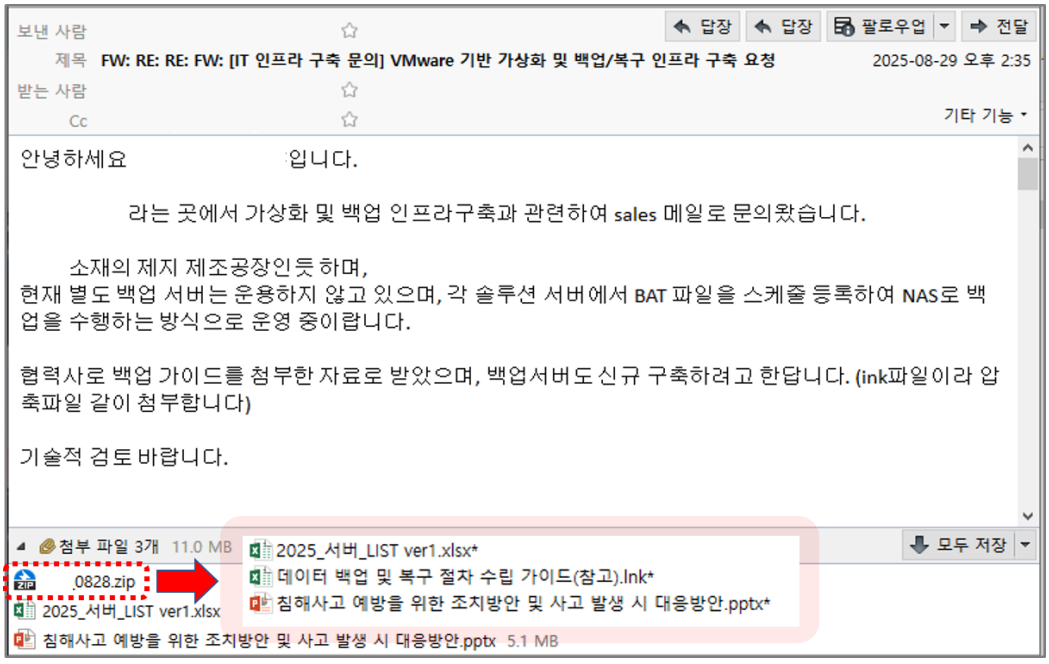


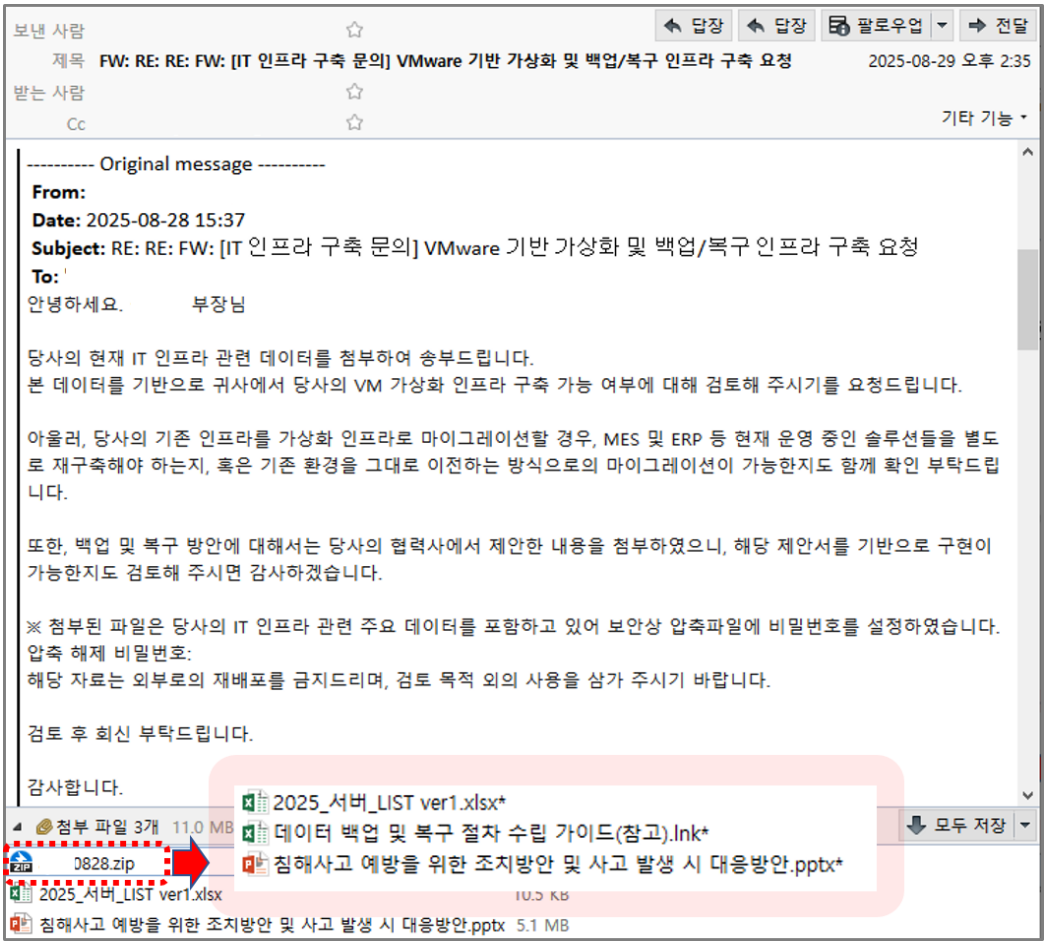
(2) 컨설팅 문의 – 견적서 위장 첨부파일



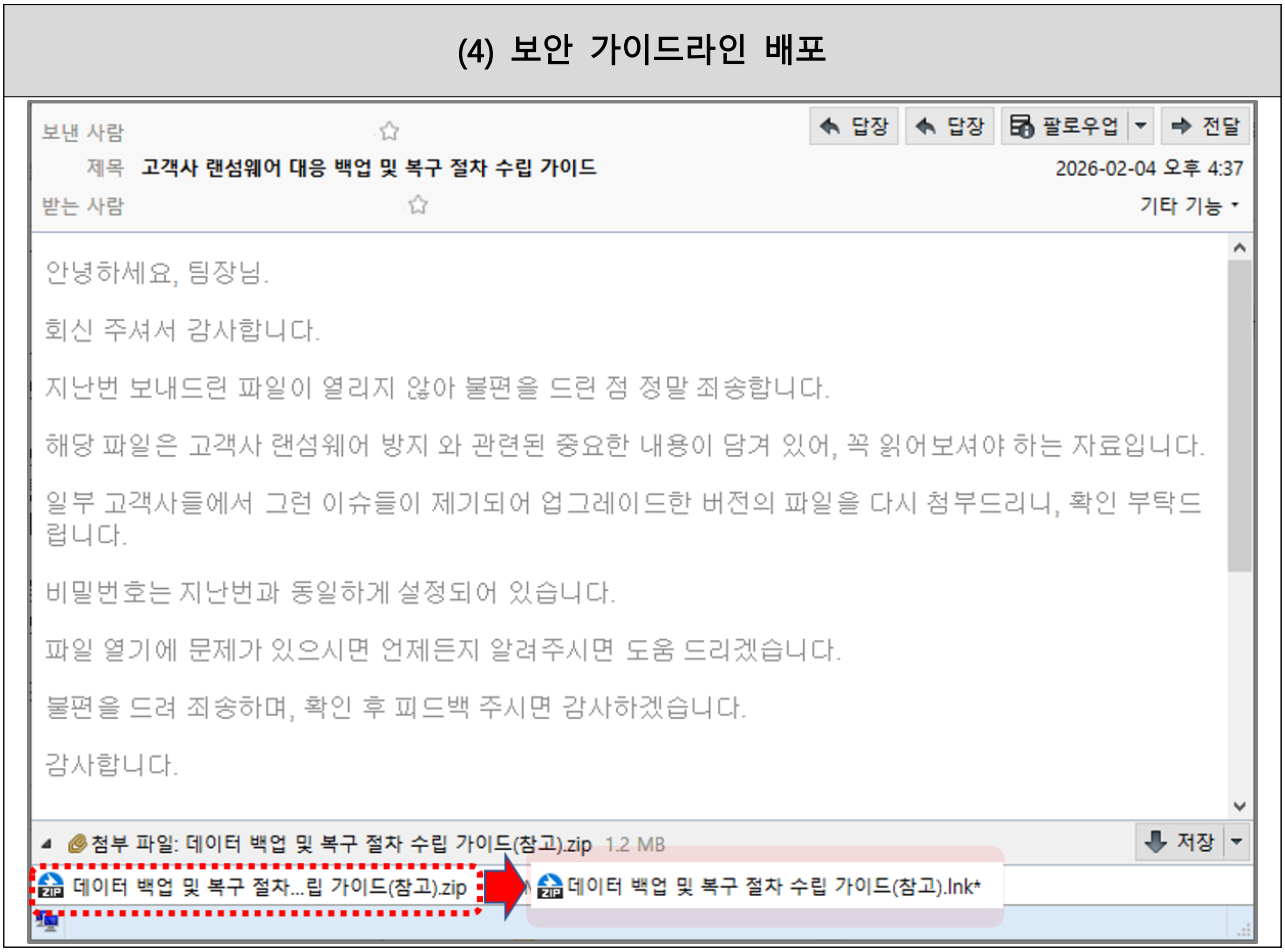
- [사례2] IT 서비스 제공업체를 사칭해 인프라 구성안, 서비스 설치 안내 등으로 위장한 악성메일을 통해 권한 탈취 및 서버 침입 후 랜섬웨어 설치

(3) 인프라 구축 요청





(4) 보안 가이드라인 배포



□ 대응 방안

○ 이메일 사용자 보안 강화

- 사용자는 송신자를 정확히 확인하고 모르는 이메일 및 첨부파일은 열람 금지
  * 가상화 기반의 격리된 네트워크 환경에서 이메일 첨부파일 내용 확인
- 이메일 수신 시 출처가 불분명한 사이트 주소는 클릭을 자제
- 첨부파일의 확장자를 확인하고 문서 아이콘으로 위장한 실행파일(.exe 등)은 클릭 자제
  * 윈도우 사용자의 경우, 파일 탐색기 > 보기 > '파일 확장명' 체크 상태
  * 파일 탐색기 > 보기 > 옵션 > 폴더 및 검색 옵션 변경 > 보기 > '알려진 파일 형식의 파일 확장명 숨기기' 체크 해제 상태
- 이메일 보안 솔루션 사용으로 유해성 유무 확인 및 악성 이메일 차단

○ 이메일 시스템 관리자 보안점검

- 비인가 계정 등록 여부 및 비정상 로그인 시도 점검
- 기존 평문으로 수발신한 메일 내용 內시스템 계정정보 점검·변경
- 시스템 계정정보 등 민감한 정보 평문 발송 금지
- 이메일 보안 솔루션 사용으로 유해성 유무 확인 및 악성 이메일 차단

○ 외부 접속 관리 강화

- 기업 자산 중 외부에 오픈된 시스템(DB 서비스, NAS, 공유기 등) 현황을 파악하고, 불필요한 시스템*은 연결 차단

  * 특히 테스트 서버, 유휴 서버 등 방치되어 있는 시스템 점검 및 중요 시스템 접속자의 경우 개인 단말에 임의로 원격 제어 프로그램을 설치 사용 여부 확인

- 불필요한 네트워크 서비스 중지 및 기본 서비스 포트(22, 1433, 3389 등) 사용 지양
- 외부 접속 허용이 필요한 경우 접속 IP 및 단말기기 제한, 다중 인증 설정, 내부이동 차단을 위한 서버별 접근제어 설정·확인, 비정상 접속여부에 대한 주기적인 로그* 확인

* 해외 및 야간·주말 접속 IP, 평소와 다른 일반적이지 않은 네트워크 통신량 등

※ 유지보수를 위한 외부업체의 접속연결은 필요시에만 허용, 상시 연결 허용 지양

○ 계정 관리 강화

- 최초 설치 시 기본 관리자 패스워드는 반드시 변경 후 사용
- 사용하지 않는 기본 관리자 계정 비활성화 및 권한 제외
- 알파벳 대문자와 소문자, 특수문자, 숫자를 조합한 복잡한 패스워드 사용
- 정기적으로 비밀번호 변경
- 계정 비밀번호 인증 이외의 추가적인 2차 인증수단 적용
- 시스템 원격 접속 계정정보 평문 저장 금지

○ **백업 관리 강화**

- 중요 자료는 네트워크와 분리된 별도의 저장소*에 정기적인 백업 권고

* 많은 피해기업이 백업을 수행하였으나, 동일 저장소에 보관함으로써 암호화되어 복구에 어려움을 겪음

※ 외부 클라우드 등에 중요 자료를 보관하고 소유기반의 이중인증 적용 등

- 클라우드 자체에 대한 랜섬웨어 감염을 대비하여 클라우드에 보관된 자료에 대해서도 정기적인 백업 수행

○ **기타 참고 사항**

- 자동 업데이트를 활성화하여 운영체제, 소프트웨어 최신 보안패치 적용
- 바이러스 백신 설치 및 최신의 업데이트 상태를 유지
- 랜섬웨어 감염에 대비한 복구 계획수립 및 모의훈련 수행

□ 침해사고 신고

○ ‘KISA 인터넷보호나라&KrCERT’ 홈페이지(www.boho.or.kr)
→ 침해사고 신고

□ 작성 : 디지털위협대응본부 국민피해대응단 랜섬웨어대응팀

○ 본 문서는 경찰청과 공동으로 작성되었습니다.