**문항1.일반 악성코드와 랜섬웨어의 차이점에 대해 설명하시오. (40점)**

|  |  |  |
| --- | --- | --- |
| 구분 | **일반 악성코드** | **랜섬웨어** |
| 유포 | 웹사이트, 이메일, 네트워크 취약점 등 **유포방식 동일** |
| 감염 | SW 취약점 또는 피해자의 실행으로 **악성코드 감염 동일** |
| 동작 | 정보 및 파일 유출, DDoS 공격 등 | 문서, 사진, MBR 등 데이터 **암호화** |
| 대응 | 악성코드 유포지 및 명령조정지(C&C)서버 주소 차단\* C&C: 해커가 악성코드에 감염된 PC에 원격으로 접속하기 위한 서버, PC로 악성코드 감염 시 C&C에 연결되어 해커의 명령을 수행 | 악성코드 유포지 및 명령조정지(C&C)서버 주소 차단\*복호화 키가 저장된 서버(도메인/IP)와의 통신경로는 미차단 |
| 치료 | 백신 등을 통해 악성코드 치료 | 백신 등을 통해 악성코드 치료**-> 암호화된 파일은 복구 어려움** |
| 피해 | 개인, 금융 정보 유출 및 이를 이용한 2차 공격으로 피해 발생 | 암호화된 파일에 대한 복호화를 빌미로 **가상통화(비트코인 등)로 금전을 요구** |

**문항2. 랜섬웨어 감염을 최소화하는 6가지 예방법에 대한 설명을 서술하시오(60점)**

1) 플래시 플레이어(Flash Player)/어도비 리더(Adobe Reader)/자바(Java) 등을 항상 최신 버전으로 유지하는 것

2) 인터넷 익스플로러(Internet Explorer)보다는 크롬(Chrome) 사용을 권장합니다

3) 발신자가 불분명한 이메일 열람 및 첨부파일 실행을 자제합니다. 최근 악성코드에 감염된 사용자의 메일 계정을 사용해 악성코드를 첨부한 후 메일을 발송하는 경우가 있습니다. 모르는 메일은 삭제하고 특히 첨부 링크는 실행하지 않아야 합니다.

4) 3-2-1 백업 규칙을 실천합니다. 클라우드와 같은 네트워크 연결형 백업만 유지할 경우, 랜섬웨어 감염 시 해당 드라이브까지 암호화해 버리는 최악의 상황까지 갈 수 있습니다. 이를 대비해 ‘3-2-1 백업’ 규칙을 적용해 적어도 3개 이상 복사본, 2개 이상 다른 형식으로, 1개의 오프라인 복사본을 저장하는 등 번거롭지만 자체적 노력을 기울여야 할 것입니다.

5) PC 및 네트워크 ‘공유 폴더’를 철저히 관리합니다. 사내에서 개인 PC가 랜섬웨어가 감염되면, 공유 폴더를 통해 전사로 퍼질 위험이 있습니다. 사내 공유 폴더 운영 시에는 해당 공유 폴더는 ‘숨김 공유 설정’을 하거나 권한 정보를 획득한 사용자만 접근할 수 있도록 설정하는 것이 안전합니다.

6), 백신 설치 OK, 중복 설치는 NO. 안전함에 너무 치중한 나머지 여러 개의 백신 프로그램을 설치하는 경우가 있는데, 백신 간 충돌로 악성코드를 탐지하지 못하는 결과를 초래할 수 있습니다. 따라서 한 개의 정품 백신 설치 후 제대로 관리하는 것이 중요합니다.