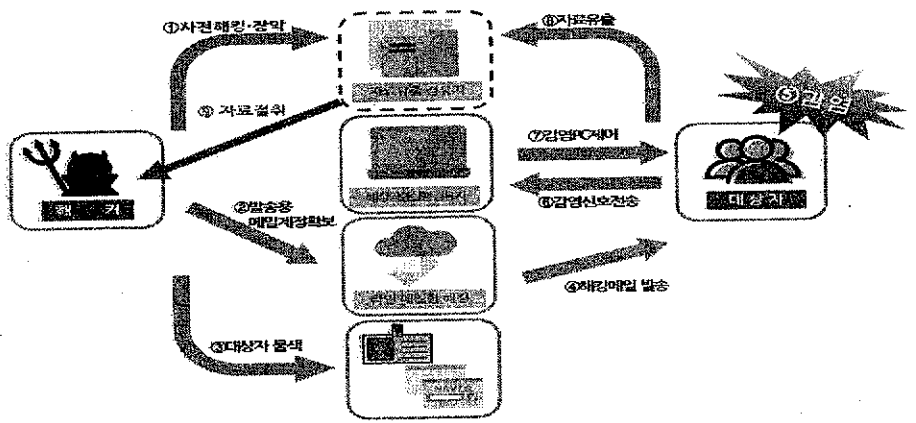
해킹 메일 대응방법

1 공격수법

❑ 공격과정



① 경유저 사전 해킹 장악
- 공격자는 자신의 위치를 숨기기 위해 다수의 경유지를 구축 확보

② 발송용 메일계정 확보
- 해킹메일 발송명의를 위장하기 위해 익명 가입여 용이한 해외 상용메일(gmail, hotmail, yahoo 등)에 가입하거나 보안이 취약한 불특정 다수 개인 메일함을 해킹해 메일 계정 확보

③ 대상자 물색
- 해킹메일 유포 대상자 선정을 위해 인터넷 검색, 명함, 각종 동기회 홈페이지 등을 통해 주요인사의 이메일 주소를 수집

④ 해킹메일 발송
- 대상자의 직업관련 내용, 지인의 안부인사, 사회적 이슈 등 수신자의 관심을 끌만한 소재로 메일 본문을 작성
- 해킹프로그램을 은닉한 문서파일을 첨부하여 대상자에게 발송

⑤ 수신PC 감염
- 대상자가 해킹메일을 열람하거나 첨부파일 클릭시 PC가 해킹프로그램에 감염
- 해킹프로그램에 기록되어 있는 해킹명령 실경유지로 감염신호를 자동 전송
- 공격자가 감염PC 현황을 파악, 이를 제어 가능

⑥ 정보절취
- 공격자는 감염PC를 제어하며 PC저장자료 및 USB메모리 연결시 저장자료를 자료유출 경유지로 전송
- 공격자는 이 경유지에 접속해 유출된 자료를 가져가기도 하며, 감염PC를 이용하여 내부 전산망을 추가 해킹

본 문서의 불법유출 시, 관계법과 규정에 의해 처벌됩니다.

❑ 공격유형

○ 첨부파일형
- 첨부파일형은 MS오피스, 한글, PDF 등 문서편집기의 임의코드 실행가능 보안취약점을 이용해 문서에 해킹프로그램을 은닉하여 발송한 후 수신자가 문서파일을 열람 시 PC가 악성코드에 감염되도록 하는 공격 방법

○ 자동감염형
- 악성코드가 은닉된 문서파일 등을 첨부하지 않고 메일사이트 및 웹 관련 스크립트 등의 취약점을 이용하여 메일을 열람만 하여도 지정된 사이트에 접속, 악성코드를 다운로드 받아 감염되도록 하는 공격 방법

○ 피싱형
- 메일 열람 시 공격자가 구축한 피싱 사이트로 자동 연결되도록 하여 메일계정 · 금융정보 등을 입력하게 하며 이를 절취하는 방법

2 식별방법

❑ 첨부 파일 열람을 유도하는 내용으로 본문이 작성되어 있으며, 여책한 표현이 많으므로 메일 열람 시 주의해야 함.

❑ 메일 열람 시 로그아웃 된 것처럼 보이면서 ID/PW 등 계정 입력을 유도하므로 보낸 이를 확인한 후, 모르는 사람일 경우 즉시 메일 삭제

❑ 첨부파일 확장자로 한글·MS오피스·PDF 문서 및 압축파일을 활용하므로 다운로드 및 백신 검사 후 열람해야 함.

※ 주요 해킹악용 첨부파일 확장자 : hwp, doc, pdf, xls, ppt, mdb, zip, rar, htm

3 대응방법

❑ 출처가 불분명한 메일은 열람하지 말고 바로 삭제

❑ 메일에 파일이 첨부되어 있는 경우 첨부파일을 PC에 다운로드 하고 백신으로 검사 후 파일 열람.

❑ 해킹메일을 열람한 경우 정보화기획처로 즉시 신고(5746/lake@smrt.co.kr). 끝.