이승용 - bongbongco.github.com

인터파크 개인정보 유출사고 정리

1. 목적

최근 발생한 인터파크의 개인정보 유출 사고 과정을 살펴봄으로써 APT 공격 위협에 대해서 알아보고자 함.

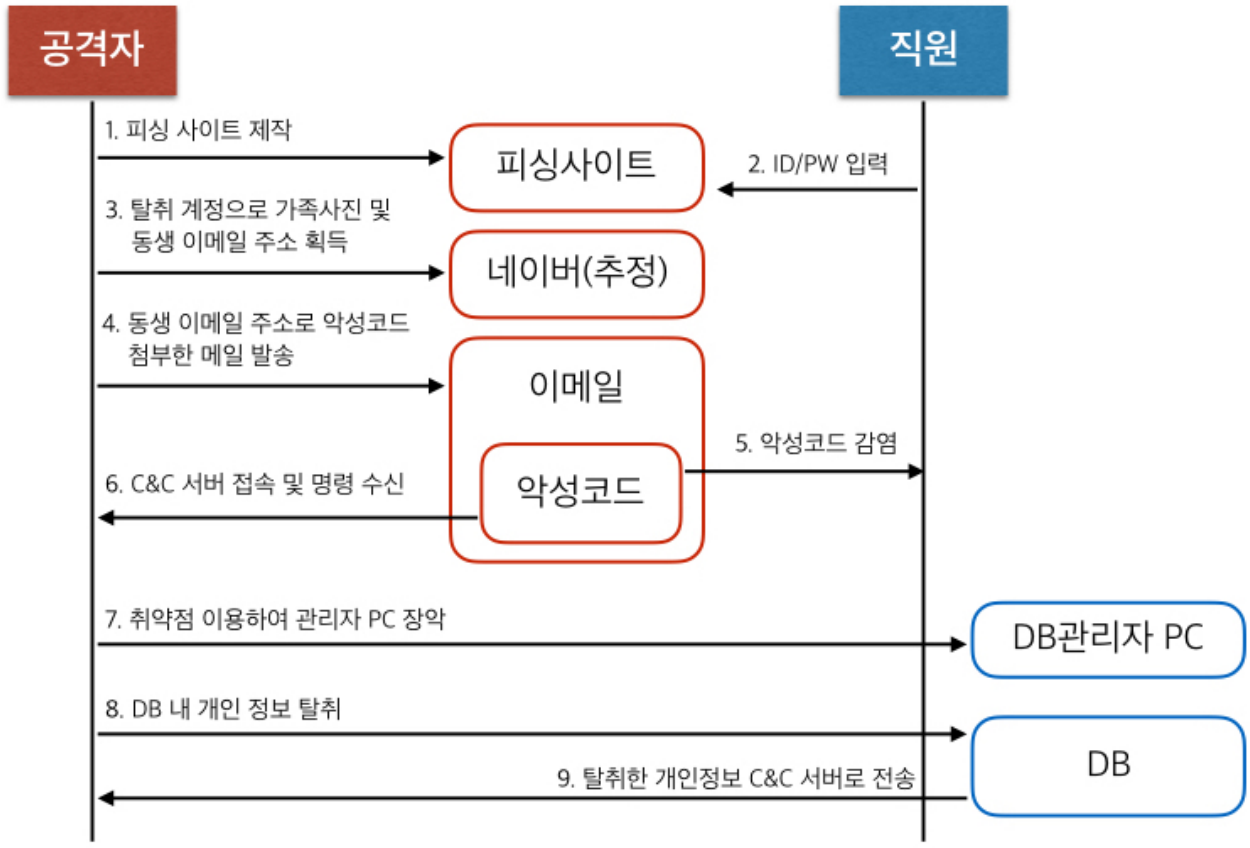
2. 개요

기업들의 크고 작은 침해사고는 끊임없이 발생하고 있습니다. 보안을 위한 많은 노력에도 불구하고 그 피해의 규모는 좀처럼 줄어들지 않고 있습니다. 최근 인터파크에서 고객의 개인정보가 천만건 이상 유출되는 사건이 발생하였습니다. 개인정보 유출 뿐만아니라, 탈취한 개인정보를 이용해서 금품을 요구한 사실이 확인되어 놀라움을 느낍니다. 인터넷에 공개된 여러 자료들을 보고 인터파크 개인정보 유출 사고의 발생과정을 정리하여 APT 공격 위협에 벗어나는 방법을 알아보겠습니다.

3. 설명

3.1. APT 공격으로 인한 개인정보 유출 사고 발생 과정

3.1.1. 개인정보 탈취 순서도



3.1.2. 개인정보 탈취 상세 과정

1. 공격자: 포털 피싱 사이트 개설
2. 직원: 포털 피싱 사이트에 ID/PW 입력
3. 공격자: 탈취한 계정을 이용하여 클라우드 드라이브 및 이메일 접속
4. 공격자: 가족 사진 및 동생 이메일 주소 획득
5. 공격자: 이메일 발송 서버 접속
6. 공격자: 동생 이메일 주소를 이용하여 악성코드가 첨부된 이메일 발송
7. 직원: 화면보호기를 통한 최초 악성코드 감염
8. 직원 PC에 설치된 악성코드: C&C 서버 접속 및 명령 수신
9. 공격자: 원격 데스크톱을 이용하여 내부 파일 서버 장악
10. 공격자: IPC$ 취약점 공격 및 RAT 악성코드 감염을 통해 내부 관리자 PC 장악
11. 공격자: DB 서버 접속
12. 공격자: 개인정보 탈취
13. 공격자: 수원 PC방에서 탈취한 개인정보 C&C 서버로 전송

3.1.2. 악성코드 유포 이메일

이메일 발송 시 실제 동생의 이메일 주소를 활용했을 뿐아니라 동생의 말투를 따라하여 메일 내용을 작성 하였으며 개인 신상정보를 파악한 후 이를 활용한 메일을 발송하였습니다. 악성코드 실행 시 화면에 출력되는 사진은 실제 가족사진으로 의심하기 어려웠을 것이라는 것을 알 수 있습니다.

3.1.3. 악성코드 목록

공격에 사용된 악성코드는 총 5가지로 확인되고 있습니다.

No	파일 이름	설명
1	우리 가족.scr	드랍퍼
2	msoia.exe	ielowutil.exe 생성 및 실행
3	ielowutil.exe	C&C 통신 및 명령 수신
4	iehmmapi.dll	C&C 명령에 의해 다운로드 되는 악성코드
5	rdpclip.exe	원격 제어

3.1.4. 악성코드 상세 정보

(1) ielowutil.exe

1. C&C 서버 통신(220.132.191.110-대만, 190.185.124.125-온두라스, 202.137.244.198-뉴질랜드)
2. 감염 PC 정보 수집 및 전송
3. 특정 파일 정보 수집 및 전송
4. 동작 중인 프로세스 정보 수집 및 전송
5. iehmmapi.dll 파일 다운로드

(2) rdpclip.exe

1. 최초 감염 후 2차 감염을 위한 원격제어 악성코드
2. C&C 서버(220.132.191.110:443-대만, 190.185.124.125:443-온두라스, 202.137.244.198:443-뉴질랜드)

(3) iehmmapi.dll

1. ielowutil.exe, rdpclip.exe와 유사한 코드 구성으로 되어 있으며, rdpclip.exe와 기능 동일
2. C&C 서버 통신(220.132.191.110-대만, 190.185.124.125-온두라스, 202.137.244.198-뉴질랜드)

4. 결론

공격 초기에 내부 직원에게 악성코드를 내려받게 하기 위해서 동생의 말투를 참고하여 본문을 작성하고 동생의 실제 이메일 주소를 활용하여 발송을 했다는 것을 보고 의심하기 힘들겠다는 생각을 했습니다. 악성코드 또한 실제 가족 사진을 사용했다는 점에서 파일 실행 후 정상적인 파일로 보이기 위해 섬세하게 만들어졌다는 것을 알 수 있습니다. APT 공격은 정확한 표적을 대상으로 지속적으로 수행하는 공격으로 오랜 기간동안 정보를 수집하고 공격한다는 점에서 SQL Injection 이나 단순한 악성코드를 이용한 공격과 차이를 보입니다. 특히 표적에게 사회공학적 기법을 이용하여 접근하기 때문에 공격임을 알기 어렵고 대응이 쉽지 않습니다. 공격을 감지해야하는 부분은 네트워크 트래픽과 악성코드로 보입니다만, APT 공격에 사용되는 악성코드가 백신에 감지될리 없으므로 트래픽관리와 보안 교육이 가장 적절한 대응 방법이라고 생각했습니다. 회사 PC 에서는 외부로 접속 가능한 네트워크를 화이트리스트 정책으로 관리하고 파악되지 않은 네트워크 트래픽 발생 시 해당 트래픽 발생 원인을 규정하는 것이 좋을 것 같습니다. 만약 이와 같은 정책의 적용이 어렵다면 최소한 사내에서 외부 메일의 접속을 제한하고 파일 클라우드 서비스의 접속은 제한하며 사내 메일의 업무 목적 이외 외부 공개를 금하도록 보안 교육을 실시한다면 상당부분 위험이 감소할 것으로 예상됩니다. (하지만 궁극적으로 사고 발생원인은 망분리를 하지 않은 것이며 망분리를 실시해야함을 전제로 합니다.)