침해사고

1 침해사고 유형

1.1 웹을 통한 감염

1.1.1 악성 ActiveX 설치 유도

- 동영상 플레이어, 보안 프로그램 등으로 위장하여 설치 유도

1.1.2 웹 애플리케이션 취약점

- 웹 키보드 보안 모듈, 공인인증서 모듈 등의 취약점 이용

1.1.3 악성 파일 다운로드 실행

- 동영상, 토렌트 파일의 확장자 변조 (.avi.exe, .torrent.exe)
- 애플리케이션(동영상 플레이어, 한글, 오피스 등) 취약점 활용

1.2 웹하드를 통한 감염

1.2.1 웹하드 다운로드 관리자 감염

- 7.7 DDoS, 3.4 DDoS, 6.25 사이버테러의 원인
- 웹하드 서버를 공격하여 "다운로드 관리자" 프로그램 감염

1.2.2 웹하드 불법저작물/음란물에 포함된 악성코드에 감염

- 관심도가 높은 파일에 악성코드를 포함시켜 업로드
  - 무료 추가 다운로드.exe
  - 무료 다운로드 방법.html
- 자체 압축 풀림(self-extracting archive, SFX)으로 배포
  - SFX로 배포하는 정상 파일인지, 악성코드인지 인지하기 어려움
- 애플리케이션 취약점 활용
  - 동영상 플레이어의 취약점을 악용하는 파일 배포

1.3 이메일을 통한 감염

1.3.1 무작위 스팸 vs. 사회적 관심사(올림픽,사고 등) 이용 vs. 특정 조직 대상(스피어피싱)

1.3.2 악성사이트 접속 유도

- 정상 이메일처럼 사용자를 다른 사이트로 접속 유도
- 금융 정보, 휴대폰 요금, 동창회/교우회 등 조직 사칭 등

1.3.3 악성 첨부파일 실행 유도

- 무작위 스팸, 사회적 관심사(올림픽, 테러 등) 이용, 특정 조직을 대상
- 한글, 워드, 엑셀 등의 문서 애플리케이션 취약점을 이용
- 어도비 플래시/리더 취약점 이용

1.4 외장저장장치를 통한 감염

1.4.1 감염된 외장저장장치(USB) -> 연결 시 자동 실행

- 국가 기간망(스턱스넷, 듀크, 플레임)과 같이 폐쇄망을 타겟
- 농협 전산망 마비와 같이 내부 시스템 감염을 위해 사용

1.4.2 MS 보안 업데이트

- MS 보안 업데이트 자동 실행 기능을 비활성화 방법
- http://support.microsoft.com/kb/967715/ko

1.5 업데이트/관리 서버를 통한 감염

1.5.1 업데이트 서버

- 대형 개인정보 유출사고와 기밀 유출 사고의 원인
- 주로 애플리케이션 개발사에서 운용 최근 자체적으로 내부 업데이트 서버를 유지
- 기업 내부로 침투할 수 있는 가장 효과적인 방법
- 업데이트 서버의 설정을 조작하여 특정 기업만 침투하기도 함

- 대상 기업의 보안성 >> 업데이트 서버의 보안성

1.5.2 관리 서버

- 3.20 사이버테러의 확산 원인
- 기업 내부에 침투한 후 감염을 확장시키기 위한 용도로 사용
- 초기 설치 이후 제대로 관리되지 않음

2 악성코드

대부분의 침해사고는 악성코드에서 시작하여 악성코드로 끝남
특정 목적을 이룰 때까지 지속적으로 사용됨

2.1 악성코드 동향

2.1.1 부팅방해

- MBR, VBR 영역 손상

2.1.2 데이터 영역 삭제

- 데이터 영역의 일정 영역을 특정 문자열 혹은 랜덤 데이터로 덮어쓰기

2.1.3 파일 삭제

- 확장자 기반의 주요 사용자 데이터 파일을 특정 문자열 혹은 랜덤 데이터로 덮어쓰기

2.1.4 MBR, VBR 손상

- 100퍼센트 복원가능

2.1.5 특정 영역 혹은 파일 덮어쓰기

- 덮어쓴 파일은 복원 불가

2.2 악성코드 유형

2.2.1 다운로드/드로퍼

- 추가적인 악성코드 설치

2.2.2 백도어

- 원격 접속 기능 필요

2.2.3 스틸러/스파이웨어

- 정보를 빼내감

2.2.4 보안 소프트웨어 위장

- 감염된 것처럼 위장해 결제 유도

2.2.5 시스템 자원 사용

- 감염 시스템 자원을 다른 공격에 사용 (DDoS, email relay, VPN 등)

2.2.6 접근 차단

- 특정 자원을 접근하지 못하도록 막은 후 결제 유도 (랜섬웨어, 암호화 등)

2.2.7 데이터 파괴

- 시스템 중요 데이터를 파괴 (MBR 파괴, 특정 문서 삭제 등)

2.3 대응방안

2.3.1 주요 포렌식 데이터 복원

- 파일시스템 메타데이터, 레지스트리, 프리패치, 바로가기 파일, 로그 파일 등

2.3.2 주요 데이터 로깅 강화

- 분석에 필요한 포렌식 데이터를 수시로 중앙 로깅

2.3.3 신속한 대응 절차 마련

- 대응 절차 마련과 모의 훈련을 통한 숙달 필요

3 침해사고 대응

3.1 현장대응 : 클라이언트

3.1.1 라이브 데이터 수집

- 활성 데이터 : 프로세스 정보, 네트워크 정보, 로그온 정보

- 비활성 중요데이터 : 파일시스템 메타데이터, 레지스트리, 이벤트로그
- 물리메모리, 패킷

3.1.2 시스템 종료

- 본체 뒤 케이블 분리 혹은 전원 공급기 차단

3.1.3 원인 분석

- (해당부서) 분석팀에게 저장매체만 전달
- (인프라팀) 표준 환경 재설치(고스트 등 이용)
- (분석팀) 저장매체 압축 이미징 -> 정밀분석

3.2 현장대응 : 서버

3.2.1 라이브 데이터 수집

- 활성데이터 : 프로세스 정보, 네트워크 정보, 로그온 정보
- 비활성중요데이터 : 파일시스템 메타데이터, 레지스트리, 이벤트로그 등
- 물리메모리, 패킷

3.2.2 시스템 종료 vs 라이브 대응

- 시스템 종료에 따른 영향 평가 후 종료가 가능하다면 정상 종료 절차

3.2.3 원인분석

- (분석팀) 라이브 혹은 로컬/원격 이미징
- (인프라팀) 백업 시스템을 이용해 재설치
- (분석팀) 이미지 정밀 분석

3.3 침해지표 관리

3.3.1 IOC

- 침해 혹은 감염을 확인할 수 있는 포렌식 아티팩트

3.3.2 정통적인 침해 지표

- IP 주소, 악성코드의 해시 및 체크섬, C2 URL

3.3.3 향상된 침해 지표

- 악성코드 실행으로 생성되는 시스템 상의 모든 흔적

3.3.4 침해 지표의 활용

- 특정 조직 내의 추가적인 침해시스템 탐지
- 유사한 유형의 침해 흔적을 다른 조직에 적용할 때
- 침해사고 외에 안티포렌식 탐지 등으로 확장 적용 가능

4 침해사고 절차

4.1 사전준비

- 신규 취약점 흔적 연구
- 침해사고 가상 케이스 분석
- 침해지표 관리
- 모의해킹 로그 분석
- 수집 및 분석 도구 테스트
- 조사 및 분석 방법론 정비
- 사본 및 아카이빙 저장용 저장장치 준비

4.2 사고 식별

4.2.1 의심

- IT 보안 장비/솔루션 모니터링 -> 의심 이벤트/트래픽
- 관리자 점검 -> 비정상로그, 권한설정변경, 시스템 자원 불법 사용
- 장비/솔루션 오작동
- 사용자 인지

4.2.2 확인

- IT 보안 장비/솔루션 모니터링 -> 악성 이벤트/트래픽
- 비정상 서비스 -> 웹페이지 변조, 게임머니 상승, 저장장치 파괴, 랜섬웨어 등
- 관리자 점검 -> 웹셸 탐지, 악성로그 확인등
- 공격자 노출 -> 유출 정보 노출, 협박, 조롱

4.2.3 인터뷰

- 대상 시스템 사용자와의 면담
- 이벤트 발생 전후, 최근행위 조사

4.2.4 조사 및 분석 범위 결정

- 시스템 전체 구성도 확인
- 증거가치가 있는 대상 시스템 및 장치 식별

4.3 증거수집

4.3.1 활성(라이브) 데이터 수집

- 시스템 스크립트(윈도우 배치 스크립트, 리눅스/유닉스 : 셸 스크립트)
- 수집 순서는 휘발성 정도에 따라 혹은 중요도에 따라
- 물리메모리 덤프, 네트워크 패킷
- 네트워크 연결, 프로세스 정보, 로그인 사용자, 서비스 목록, 클립보드
- 시스템 정보, 네트워크 인터페이스 정보, 작업목록, 자동실행정보, 감사 정책 정보

4.3.2 비활성 중요 데이터 수집

- MBR, 파일시스템 메타데이터($MFT), 레지스트리 파일, 프리패치, 웹 브라우저 흔적, 로그 등

4.4 조사분석

4.4.1 저장장치 이미징

- 전문 포렌식 이미지 장비 사용
- 라이브 CD, 쓰기 방지 장치, 네트워크 케이블

4.4.2 사전 분석

- 저장장치 이미징 과정과 병행하여 부석 진행
- 수집한 활성, 비활성 데이터로 침해 흔적/타임라인 분석
- 사전분석을 통해 침해 경로, 시점, 정밀 분석 대상 선별

4.4.3 악성 분석

- 이미징 완료 후 사전분석 결과를 토대로 초기 분석 수행
- 침해지표확인(IOC) 확인, 해시 분석, 다양한 AV 탐지, 악성 URL 분석

4.4.4 정밀 분석

- 통합 타임라인 분석, 악성코드 분석, 파일시스템 분석, 로그 분석
- 가상환경 분석, 파일 포맷 분석

4.5 보고 및 발표

- 보고 대상에 맞춘 수준별 보고서 및 발표 준비

4.5.1 보고서 작성

- 일일 보고서
- 최종 보고서

4.6 증거 보존

- 상황에 따라 수집한 증거를 압축 보관
- 케이스 식별부터 보고에 이르는 전 과정의 문서 포함