한국인터넷진흥원 침해사고 분석 절차 안내서

챕터 4. 주요 해킹 사고별 분석 사례

BoB7기 취약점분석 정성조

# 악성코드 은닉 사이트 분석 사례

악성코드 은닉은 일반화됐지만 체계적인 사고 분석과 대응 절차를 걸치지 않으면 악성코드에 피해를 입을 수 있다.

* 웹쉘 등 확인 -> 로그 확인 -> 근본적 원인 제거

# 사고 처리 절차(BASIC)

* 악성코드 삽입사실 인지, 삭제
* 웹 로그/이벤트 로그 분석
* 로그 분석 후 악성코드 재삭제
* 주변 시스템 분석
* 취약점 제거/보안 강화
* 서비스 재개/모니터링

# 악성코드 삽입사실 인지, 삭제

* 웹 페이지에 ifream 또는 object 코드 삽입
* 악성코드 인코딩
* 오류 페이지에 악성코드 삽입
* 자바 스크립트 코드 삽입
* 바이너리 형태의 객체 삽입
* 데이터베이스내 자료 값 변조

# 웹 로그/이벤트 로그 분석

* IIS 웹 로그 분석 ( 중국 툴을 사용하는 경우 수천라인의 로그가 형성됨 )
* 이벤트 로그 분석 ( 시작 -> 프로그램 -> 관리도구 -> 이벤트 뷰어 )

# 백도어/악성 프로그램 제거

* \WINNT\system32, \Windows\system32, 휴지통 확인
* 데이터베이스 테이블 확인

# 주변 시스템 분석

웹 서버가 해킹 당한 경우 그 주변 DB 등도 함께 2차적 해킹이 당했을 수 있으므로 분석해야 한다.

# 취약점 제거/보안강화

제거했다고 해도 다시 해킹을 당할 수 있으므로 보안을 강화해야 한다.

사용자가 입력할 수 있는 모든 부분에 대한 검사가 필요하다.

* URL 인자, 쿼리 문자열, HTTP 헤더, 쿠키, HTML 폼 인자 등
* 검사가 힘들 경우 공개 웹방화벽 사용(WebKnight, ModSecurity)

# 서비스 재개/모니터링

# 악성 BoT C&C 분석 사례

# 사전 준비사항

* 네트워크 패킷 분석 도구(sniffer, etherpeek, ethereal)
* 포트, 프로세스 확인 도구(fport, tcpview)
* 기타 분석도구(Rootkit Hook Analyzer, RootkitRevealer)

악성 봇 C&C 서버가 사용하는 IRC 서버 자체적으로는 악성 프로그램이 아니므로 프로그램이 잡아내지 못한다.

# 악성 봇 C&C 서버로 많이 사용되는 프로그램

IRC – 인터넷 간 대화 목적이지만 파일 전송, 원격 명령 제어 가능

# 분석과정

* 악용 여부 확인
* 공격 호스트와 로그 분석
* 봇 감염 시스템 로그 분석
* 원상 복구

# 악성 봇C&C서버 판별

* 해당 C&C 서버로 접속하여 실제로 운영되고 있는 서버인지 확인한다.
* 네트워크 패킷 캡쳐 후 해당 포트 확인
* 항상 통신하고 있지 않을 수 있기 때문에 100% 확인 불가
* fport, tcpview 등을 이용하여 열린 포트 확인
* 공격 로그 분석(기본 로그파일 및 IRC 설정파일 등)
* 24시간 모니터링
* 트래픽 분석을 통한 봇 감염시스템 분석
* 시스템 원상 복구(네트워크X 모드로 변경해서)

# ARP Spoofing

# 개요

여러대에서 일어난 ARP spoofing을 분석해보니 감염된 서버가 좀비 PC로 변해 다시 ARP spoofing을 하는 구조였다.

ex) down.exe 악성코드를 공격 스크립트에 의해 사용자 계정 Temp 하위 디렉터리에 autoexebc.bat로 복사 및 실행한다. -> 좀비 컴퓨터

# down.exe (autoexecbc.bat) 악성코드 분석

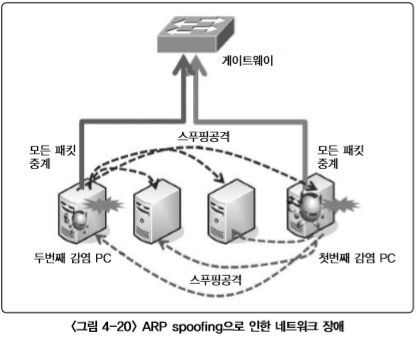
* googleons.exe 다운로드 및 실행 (ARP Spoofing)
* 시스템 시간 변경
* 방화벽 중지, 백신 종료

# googleons.exe 악성코드 분석

* 브로드캐스팅으로 ARP Spoofing을 한다.
* HTTP 패킷에 iframe으로 악성코드를 삽입한다. -> 전염
* USB 디바이스가 확인되면 에 악성 파일을 삽입하여 자동으로 실행시킨다.
* USB 작동도 똑같다.
* 재시작 레지스트에 등록

# ARP Spoofing 공격으로 인한 네트워크 장애

* 좀비 PC가 많아질수록 정상적인 네트워크 서비스 불가



# 결론/대책

* 스위칭 장비에서 Static MAC 모니터링
* arpwatch 등 ARP cache 모니터링, 변경사항 감지