[초청강연]

학 술 발 표 3

최근 해킹범죄 수사 사례

- 경찰청 사이버테러대응센터팀장 정석화 -

최근 해킹범죄 수사사례

2008. 7. 3

정석화
(sf77@police.go.kr)

NETAN 경찰청 사이버테러대응센터

Contents

Ⅰ. 최근 해킹범죄 동향

가. 유형과 목적

	해킹 목적	해킹(감염) 경로	해킹 세부 수법
PC해킹	국가기밀수집	- 메일 - 기관의 민원게시판	- 공무원사칭 메일 발송시 악성코드 첨부 - 민원 게시글에 악성코드 파일첨부
	금융정보수집	- 메일 - 포털사이트 카페	- 인터넷 카페에 악성코드 첨부하여 게시 - 게시 후 게시글 삭제(악성코드는 잔존)
	개인정보수집	- 취약한 웹서버 - 포털 카페 및 미니홈피	- 홈페이지 소스에 <iframe> 태그 삽입 - 미니홈피/블로그에 악성코드 게시
서버해킹	회원 DB 획득 (+ 협박)	- 웹해킹 - 역접속	- OWASP 취약점 공격, 웹셸 설치 - NC, PEEP, REVACC, TRAN, SSH
	DDOS공격 (+ 협박)	- Botnet 매매 - C&C서버 제어	- SYN Flooding - UDP Flooding - IP Spoofing

Ⅰ. 최근 해킹범죄 동향

나. 일반적 특징

① 금전적 목적

- 호기심과 실력과시용 해킹은 전무, 경제적 목적 뚜렷
- 사회적 분위기에 편승한 해킹이 일시적으로 발생

② 일반범죄와 결합

- 기존 범죄 조직이 해커를 조직원으로 고용
- 해킹 후 협박하는 범죄가 일반화

③ 제3국 또는 외국인 고용 해킹

- 중국, 태국, 필리핀 등에 출국 후 원정해킹
- 현지인 고용 또는 국내에서 외국인 고용

④ 내부자에 의한 정보유출

- 웹에이전시 회사직원이 업무상 DB 복제
- 업체 계약 만료시 또는 퇴사시 사취

I. 최근 해킹범죄 동향

다. 기술적 특징

① 악성코드와 역접속

- 보안시스템을 우회하기 위한 수법
- PC 해킹과 웹서버 해킹에 일반적으로 사용되며 탐지가 어려움

② 암호통신과 VPN 악용

- 보안 관리자 또는 사용자가 해킹을 인식하지 못하도록 암호화
- 상용 VPN 서비스에 가입, IP를 은닉

③ DNS 추적회피수법

- 악성코드 제작시 통신할 시스템을 IP가 아닌 도메인주소로 지정
- DNS 서버를 직접 운용하거나 무료 도메인 서비스를 이용

④ ARP 스푸핑 & 봇넷

- 1차 해킹 후 ARP 스푸핑 수행, 계정정보를 가로채 2차 해킹
- DDOS 공격을 위해 봇넷을 매매

II. 최근 해킹범죄 수사사례

가. 2008 상반기 주요 해킹 TOP10

① A은행 인터넷뱅킹 해킹사건 ('08.1)

② B전자상거래 회사 회원정보 해킹사건 ('08.1)

③ 100만대 PC 악성코드 감염사건 ('08.2) – 7명 검거

④ C기관 PC 악성코드 감염사건 ('08.2)

⑤ D증권사 홈페이지 DDOS 공격사건 ('08.3)

⑥ E통신사 개인정보 유출사건 ('08.4) – 1명 검거

⑦ 미니홈피 방문자 추적 해킹사건 ('08.4) – 11명 검거

⑧ F계 제2금융기관 해킹사건 ('08.5) – 2명 검거

⑨ G식업체 DB 유출사건 ('08.5) – 1명 검거

⑩ H업 홈페이지 해킹사건 ('08.6) – 1명 검거

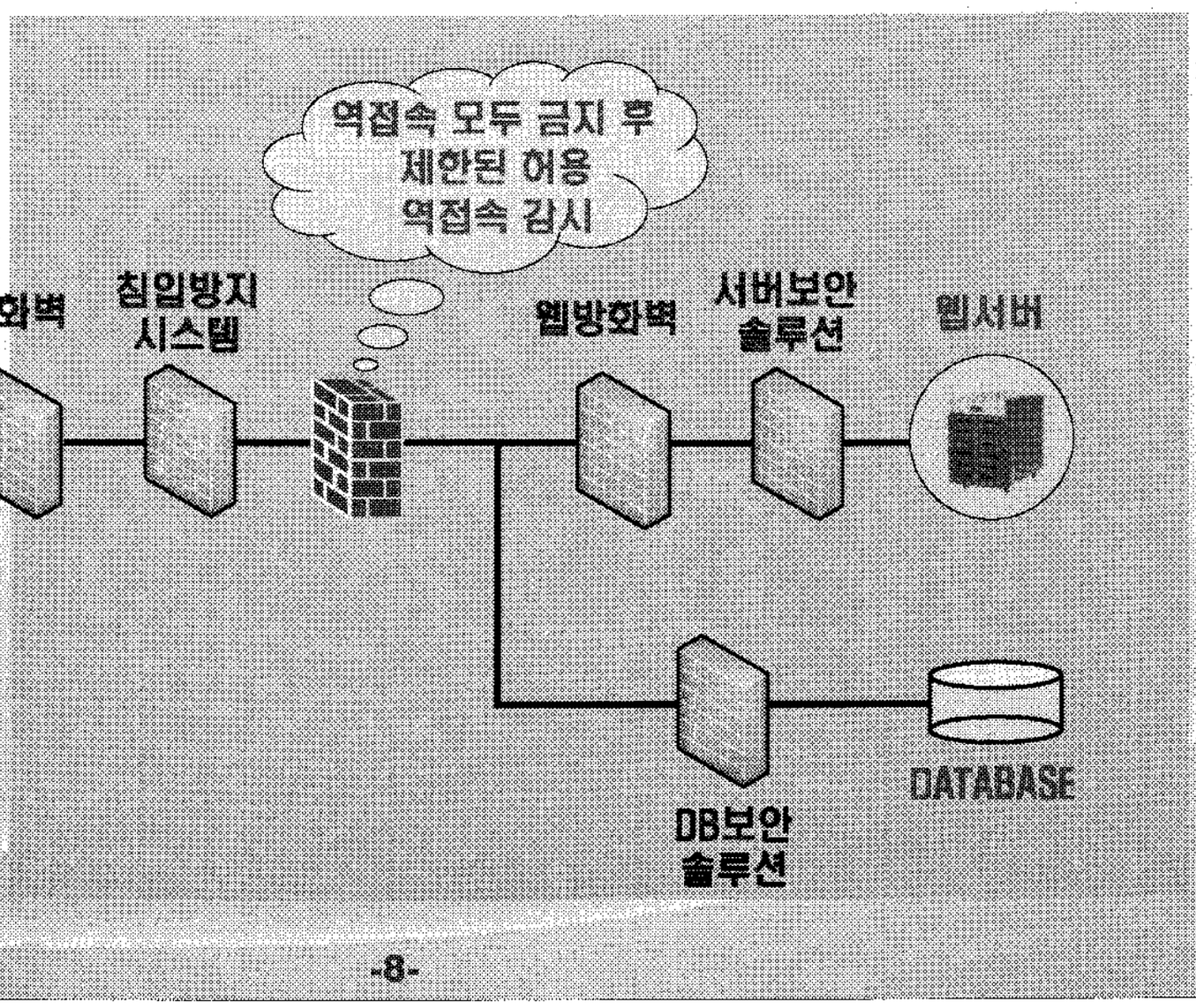
III. 웹서버 및 PC 보안

가. 역접속 해킹의 단계

구 분		1단계	2단계	3단계
공격 행위		PC 또는 웹서버에 웹셸과 악성코드 설치	악성코드 실행 (역접속)	원격 접속, DB등 내부 해킹
동작하는 보안시스템	서버 네트워크	방화벽 웹방화벽 침입탐지시스템 침입방지시스템 서버보안솔루션	?	DB방화벽
	PC 네트워크	인터넷 공유기 백신프로그램 키보드 보안프로그램 PC방화벽 프로그램	?	없음

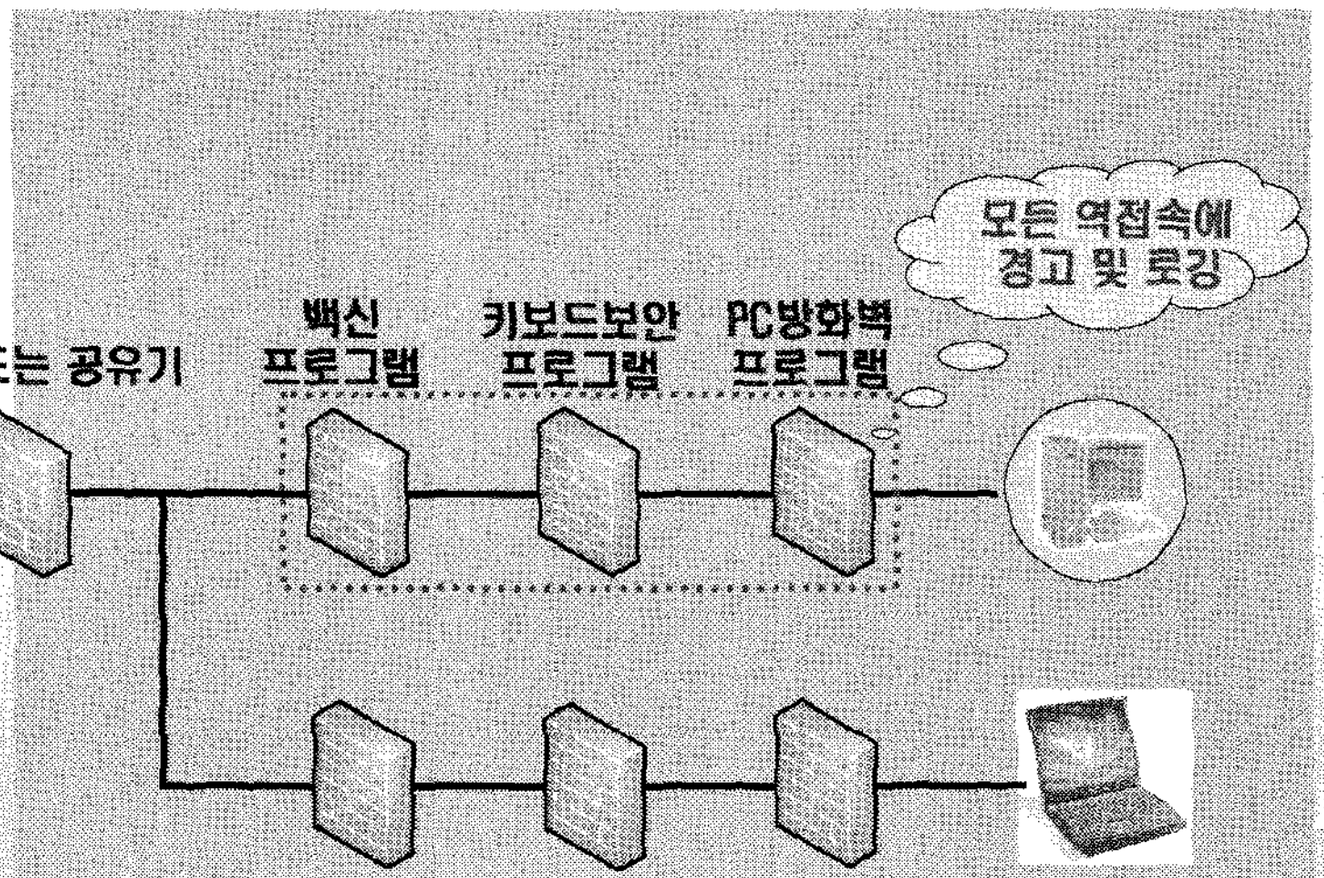
III. 웹서버 및 PC 보안

나. 웹서버 보안



III. 웹서버 및 PC 보안

다. PC 보안



IV. Q & A

감사합니다