농협 전산망 장애사건 수사결과

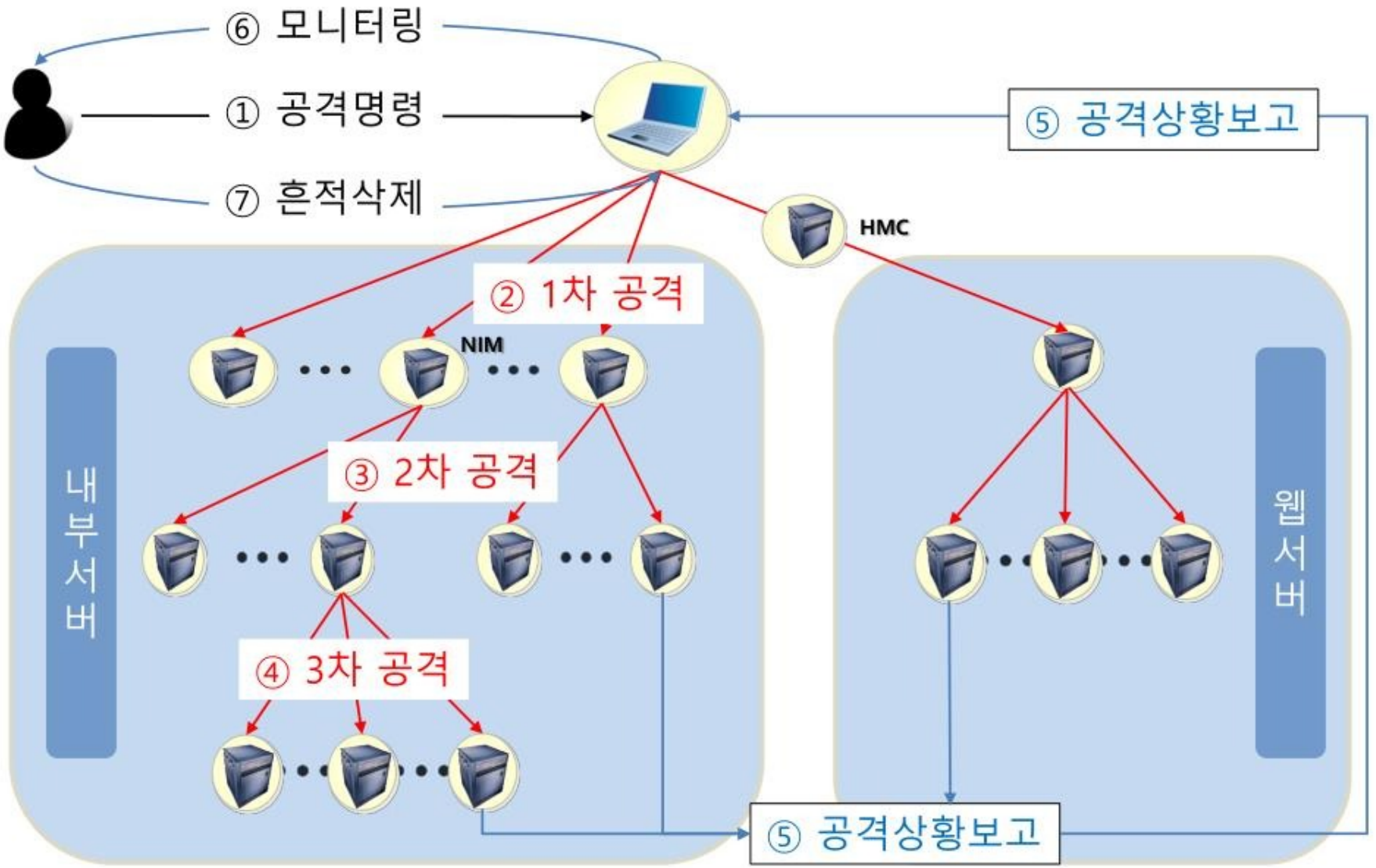
치밀하게 준비된 사이버 테러

2011. 5. 3.

서울중앙지방검찰청 첨단범죄수사제2부

검찰
PROSECUTORS' OFFICE

공격 시나리오


⑥ 모니터링
① 공격명령
⑦ 흔적삭제
⑤ 공격상황보고
HMC
② 1차 공격
NIM
③ 2차 공격
④ 3차 공격
내부서버
웹서버
⑤ 공격상황보고

검찰
PROSECUTION SERVICE

<그림 1> 악성코드 종류

감시용	공격용	범행은폐용
백도어 프로그램	파괴대상 서버목록 프로그램	관련 악성코드 삭제 프로그램
키로깅 프로그램	서버유형별 삭제명령 프로그램	복구 불가능화 프로그램
화면캡쳐 프로그램	삭제실행 프로그램	
도청 프로그램	공격명령 모니터링 프로그램	
공격명령 서버목록 프로그램		

총 81개

<그림 2> 사건 전개 과정

공 격		피 해 대 응
웹사이트로부터 악성코드 감염	2010.9.4. 22:48:04	
키로깅프로그램 설치	2010.10.22. 09:47:28	
백도어프로그램 설치	2011.3.11. 17:47:00	
파일삭제관련 프로그램 설치	2011.3.22. 12:57:51	
공격명령파일 설치	2011.4.12. 08:20:14	
공격명령실행(파괴 시작)	2011.4.12. 16:50:10	
	2011.4.12. 16:51:53	서버장애발생 최초인지(SMS수신)
	2011.4.12. 17:00 경	서버장애발생 확인(rm,dd명령 실행확인)
	2011.4.12. 17:10 경	공격노트북 IP 파악(9.43.216.108)
노트북 공격악성코드 삭제	2011.4.12. 17:20:56	
	2011.4.12. 17:29:58	서버 Shutdown 시작(HMC콘솔 이용)
	2011.4.13. 12:40 경	각 농협지점 창구거래 정상화
	2011.4.14. 02:00 경	자동화기기 거래 복구
	2011.4.30.	신용카드 대고객서비스완전 복구

검찰
PROSECUTION SERVICE

<그림 3> 키로깅

○ IP, 비밀번호 취득

[2011.04.08 17:24:50] - "9[redacted]0 - SecureCRT"
pe[redacted]1f3a<Enter>
[[redacted]0<Enter>
su -<Enter>
a[redacted]34<Enter>
su -<Enter>
p[redacted]rd<Enter>

IP

암호

○ 채팅내용 파악

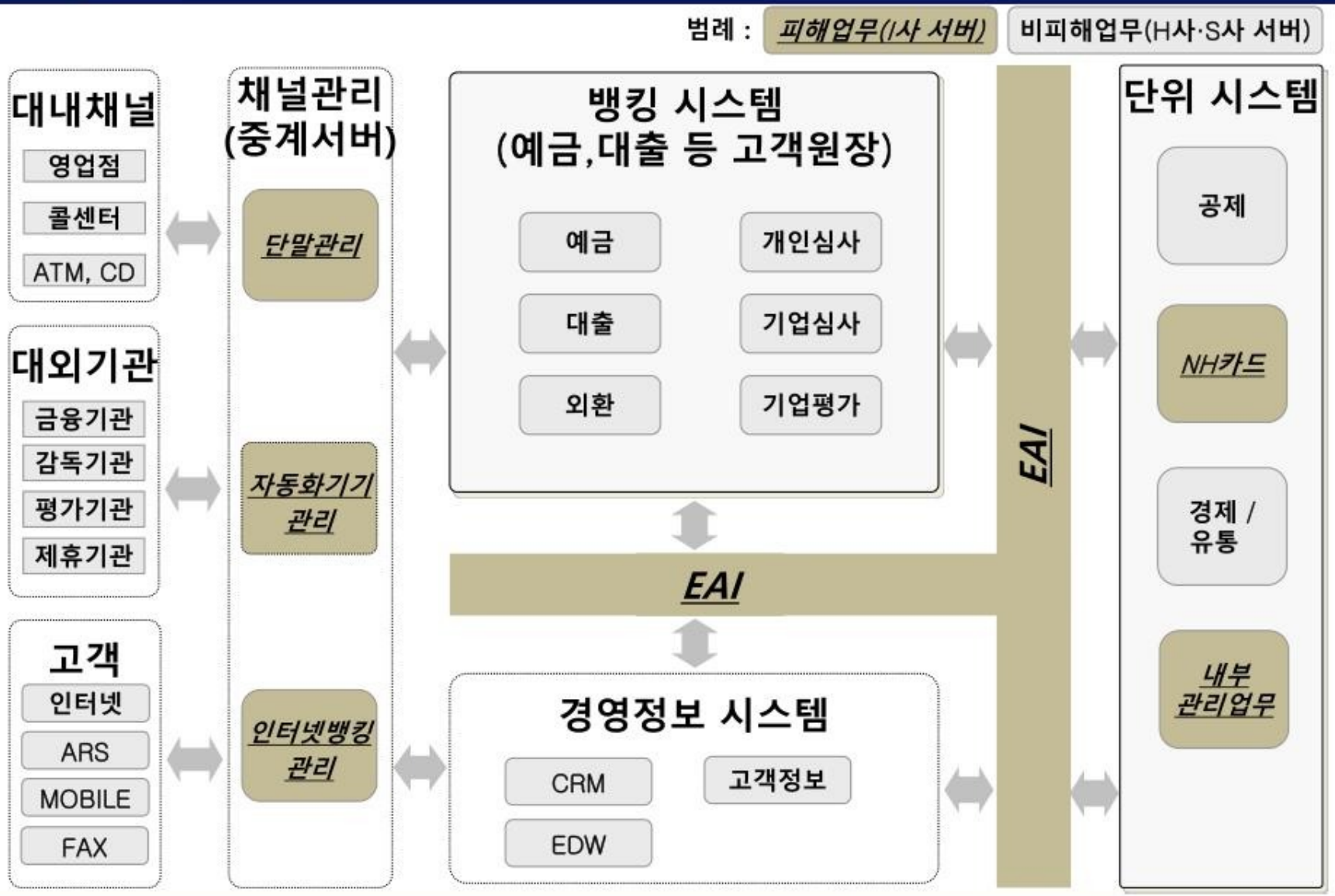
2011. 3. 12. ~ 4.12. 키로깅 결과 : 1,073 페이지

[2011.03.14 16:58:50] - "
네, 차장님<Enter>
헐.. ㅇ<Enter>
네.. <Enter>
pmr 아직 진행 못했습니다, 농번기로.. ^^<Enter>
nmon data는 확보했고.. <Enter>

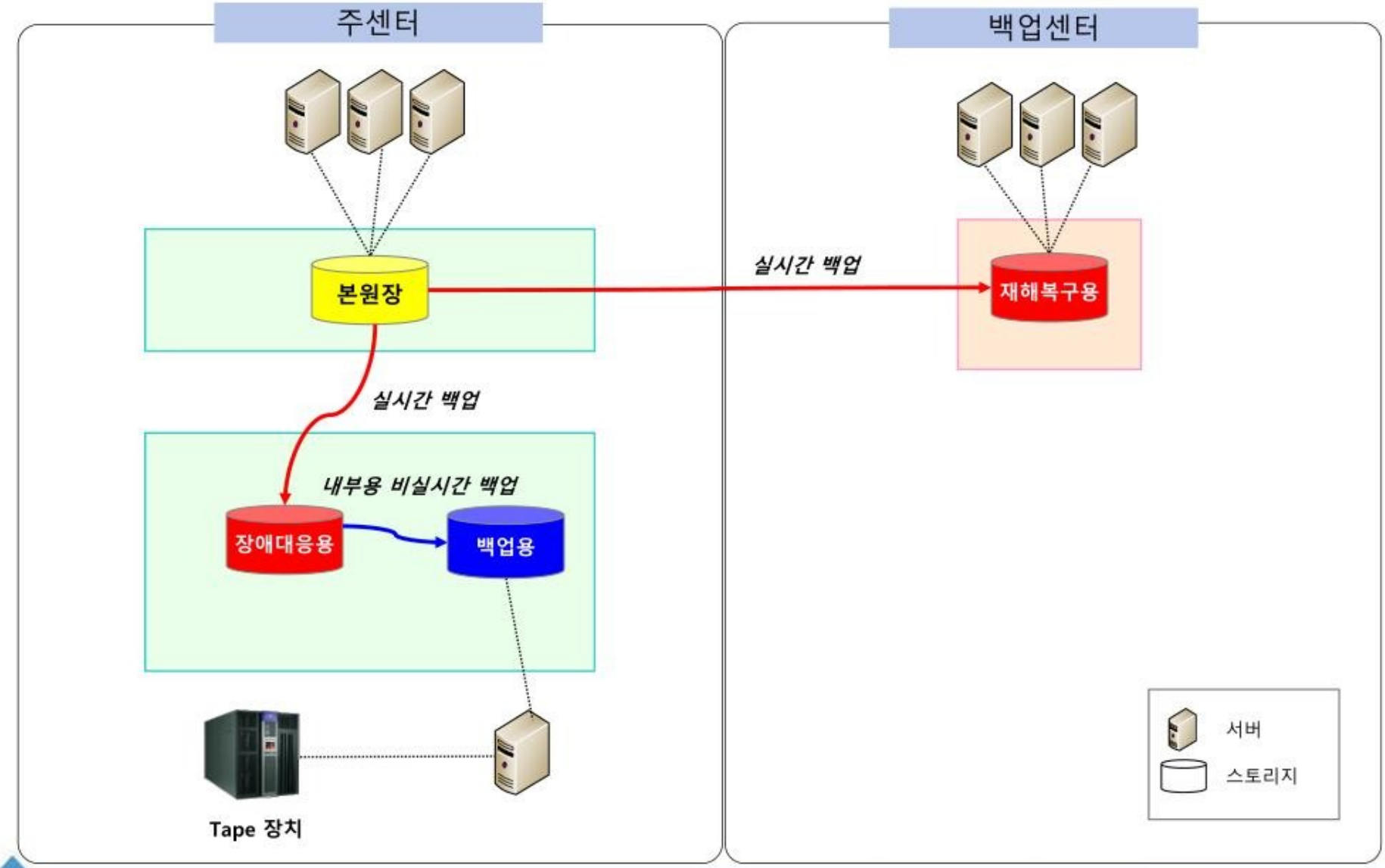
[2011.03.14 17:00:41] - "jm[redacted]kr,it[redacted]m - Je[redacted]ng Oh/Ko[redacted]M [시작: 오후 04시 58분]"
perfpmr 이나.. 다른 건 아직 답보에요.

[2011.03.14 17:00:44] - "j[redacted]kr[redacted]com - Je[redacted]ng Oh/Kor[redacted]M [시작: 오후 04시 58분]"
지켜보자는 그 건이구요.<Enter>
오[redacted]과장님, 협박은 제가 받은 걸로 하고.. 발리 PMR진행하겠습니다. <Enter>
결국 이건은 misc heap이 아닐수도 있습니다.<Enter>
nmon 전체를과장님, 수고하십시오 ^^ 박[redacted]차장님 협박은 감사합니다. ㅋ<Enter>

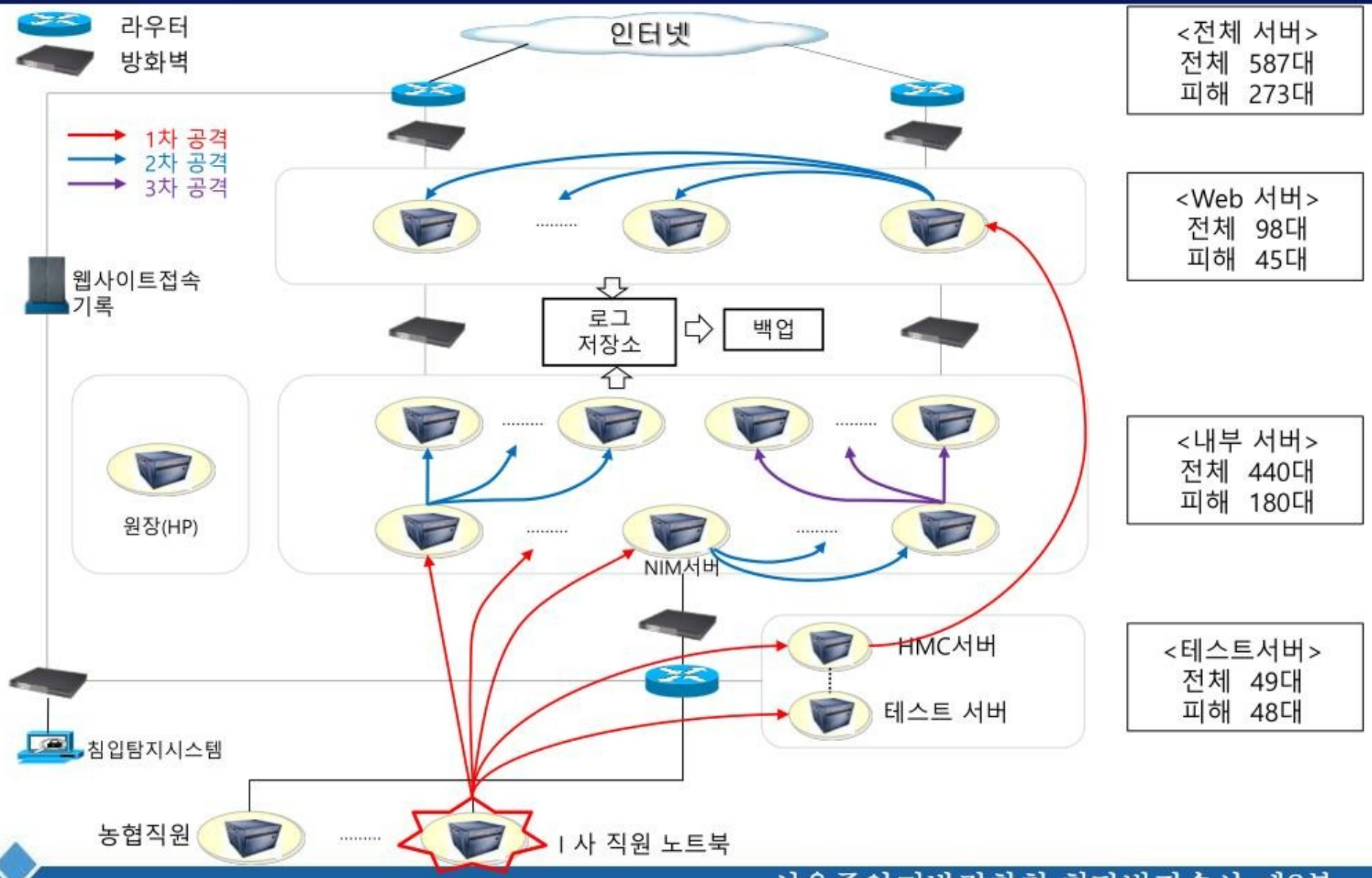
<그림 4> 전체시스템 구성도



<그림 5> 백업 기본 구성도


주센터
백업센터
본원장
실시간 백업
재해복구용
실시간 백업
내부용 비실시간 백업
장애대응용
백업용
Tape 장치
서버
스토리지

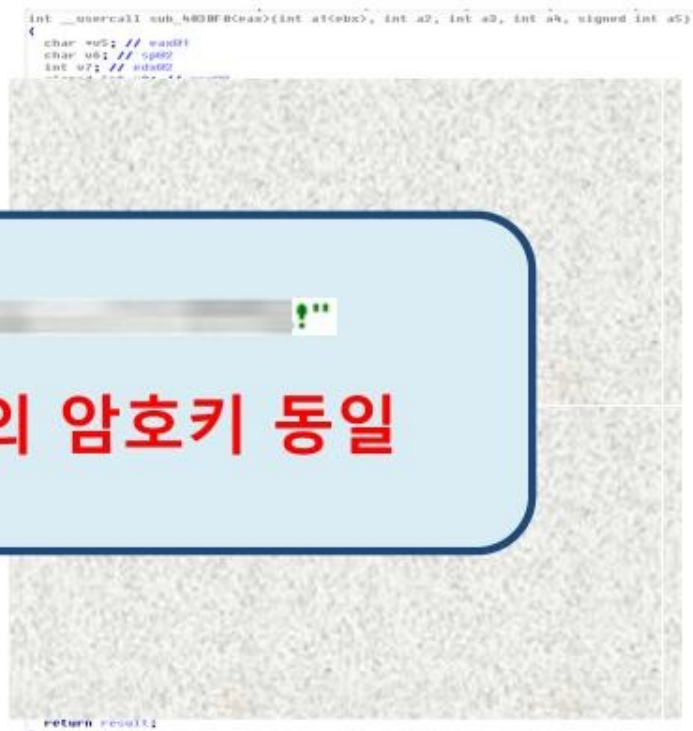
<그림 6> 공격 체계도


라우터
방화벽
인터넷
1차 공격
2차 공격
3차 공격
웹사이트접속 기록
로그 저장소
백업
원장(HP)
NIM서버
HMC서버
테스트 서버
침입탐지시스템
농협직원
I 사 직원 노트북
<전체 서버>
전체 587대
피해 273대
<Web 서버>
전체 98대
피해 45대
<내부 서버>
전체 440대
피해 180대
<테스트서버>
전체 49대
피해 48대

<그림 7> 암호화 방식

3.4 DDoS

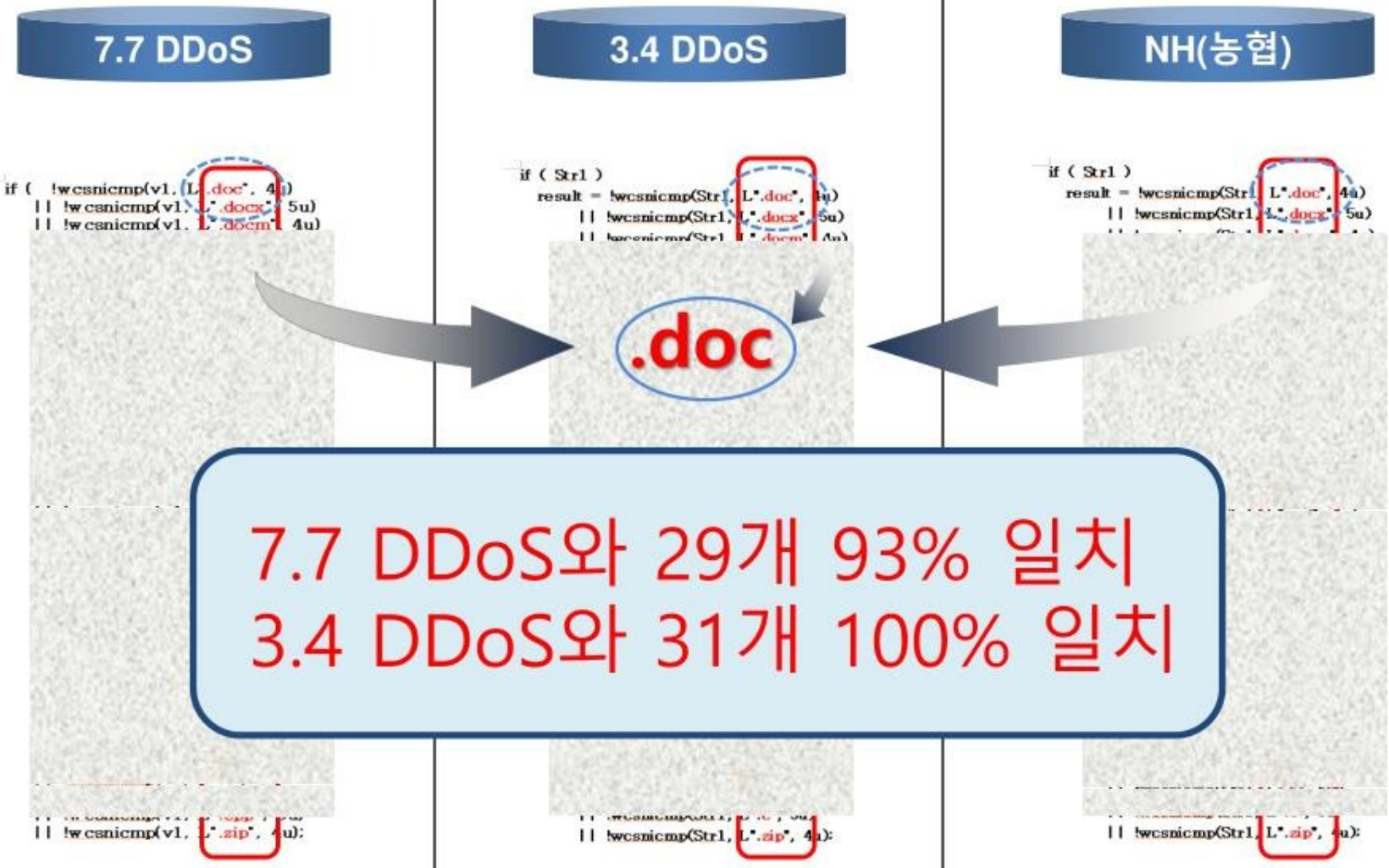
NH(농협)



"A3[redacted]!"

A로 시작하는 45자의 암호키 동일

<그림 8> 삭제 대상 파일 확장자 비교



<그림 9> 분석 방해 수법

7.7 DDoS

```
p                                   ; "x
p                                   ; "c
le                                  st]
p                                   ; "%s                    ₩""
```

3.4 DDoS

```
p
le                                  dLine]
p                                   ; "c                     >%s"
p                                   ; Dest
```

NH(농협)

```
p                                   ; "x
p                                   ; "c
le                                  ommandLine]
p                                   ; "%s                    s₩""
```

검찰
PROSECUTION SERVICE

<표> 7.7, 3.4 DDoS 와 비교

구분	악성코드 감염경로	악성코드 유포수법	공격명령 IP	공격구조	프로그램 유사성		
					비교대상 확장자	분석방해 수법	암호화 기법
7.7 DDoS	웹하드 사이트	웹하드 사이트 자동 업데이트 위장	59개국 538개	공격프로그램과 공격명령 서버목록 분리	총 37개	문자열 조합	확인 안됨
3.4 DDoS	동일	동일	7.7 과 3개 일치 (70개국 748개)	동일	총 31개 (7.7과 93% 동일)	치환이 없음	자체 제작 암호 기법
NH (농협)	동일	동일	3.4 와 1개 일치 (13개국 27개)	동일	총 31개 3.4와 100% 동일	문자열 조합 7.7과 동일	3.4와 동일
비고	S웹하드 사이트에서 감염 (3.4 DDoS 와 동일)			통상 공격프로그램에 공격명령 서버목록 포함		분석을 곤란하게 하기 위함	