

2006 Security Trend & Threat

중국발 해킹의 발전과 대응

2006.10.24

전 상훈 [p4ssion]

– Agenda –

I. Security Trend

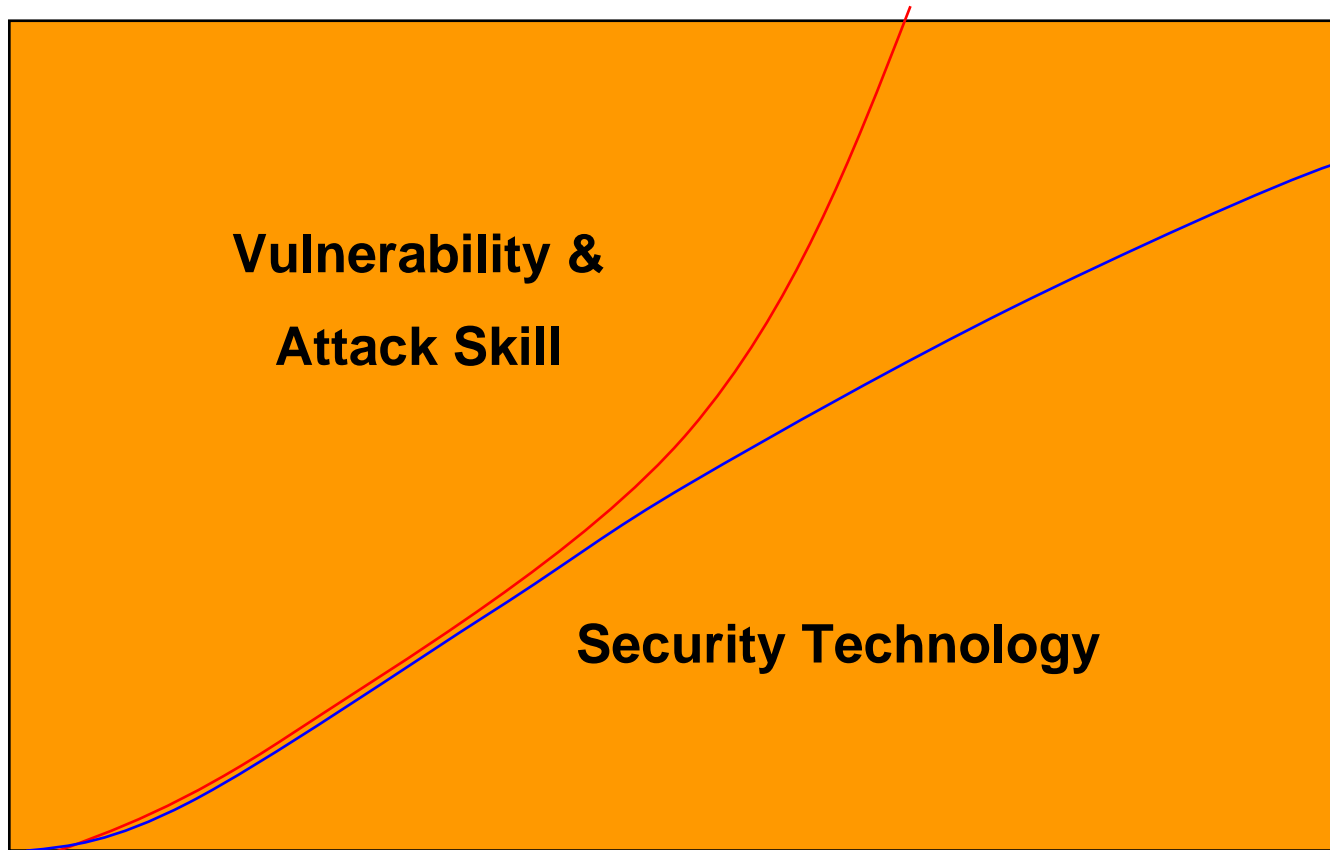
- 환경의 변화
- 위협요소
- Security의 변화
- 공격유형의 변화

II. 대응

I. Security Trend

-환경의 변화

취약성 및 공격 기술 발전에 따른 정보보호 기술의 발전 유형

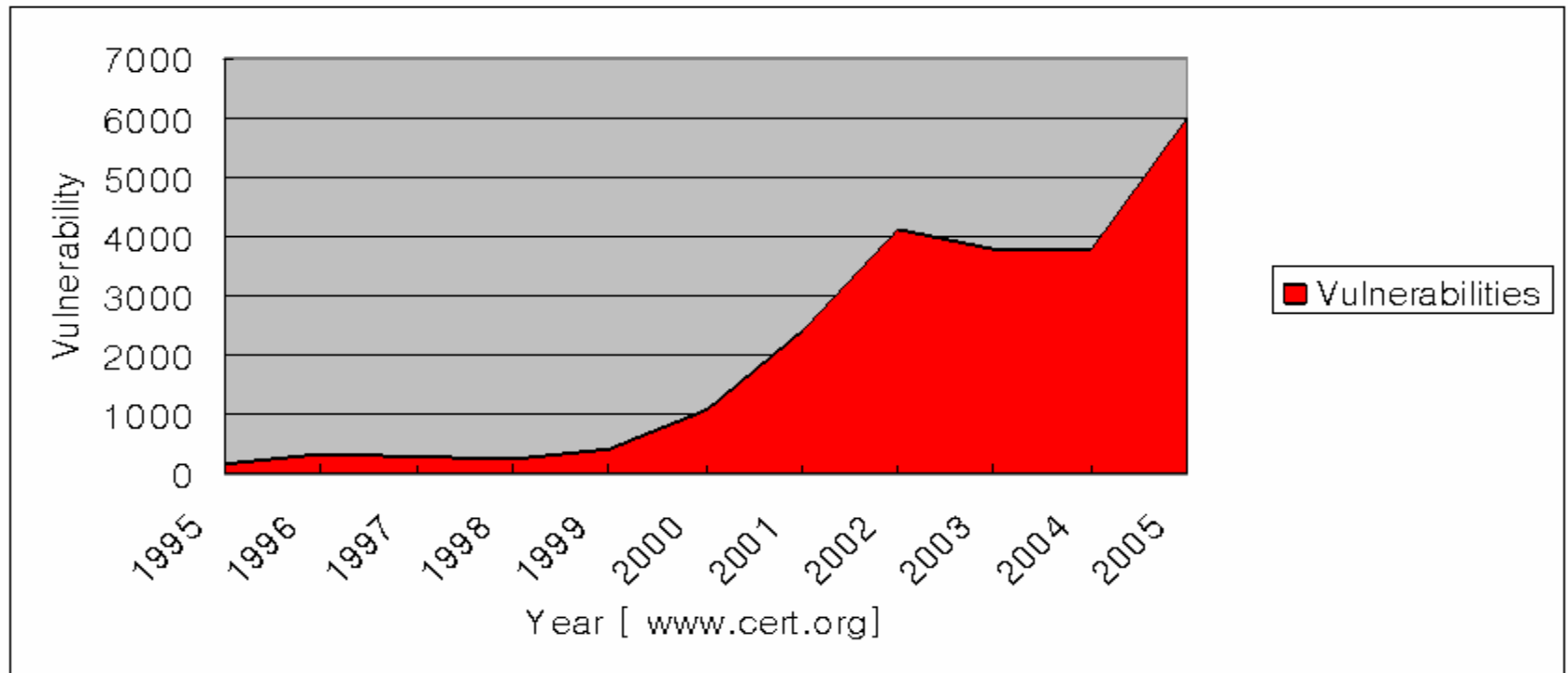


I. Security Trend

- 위협요소

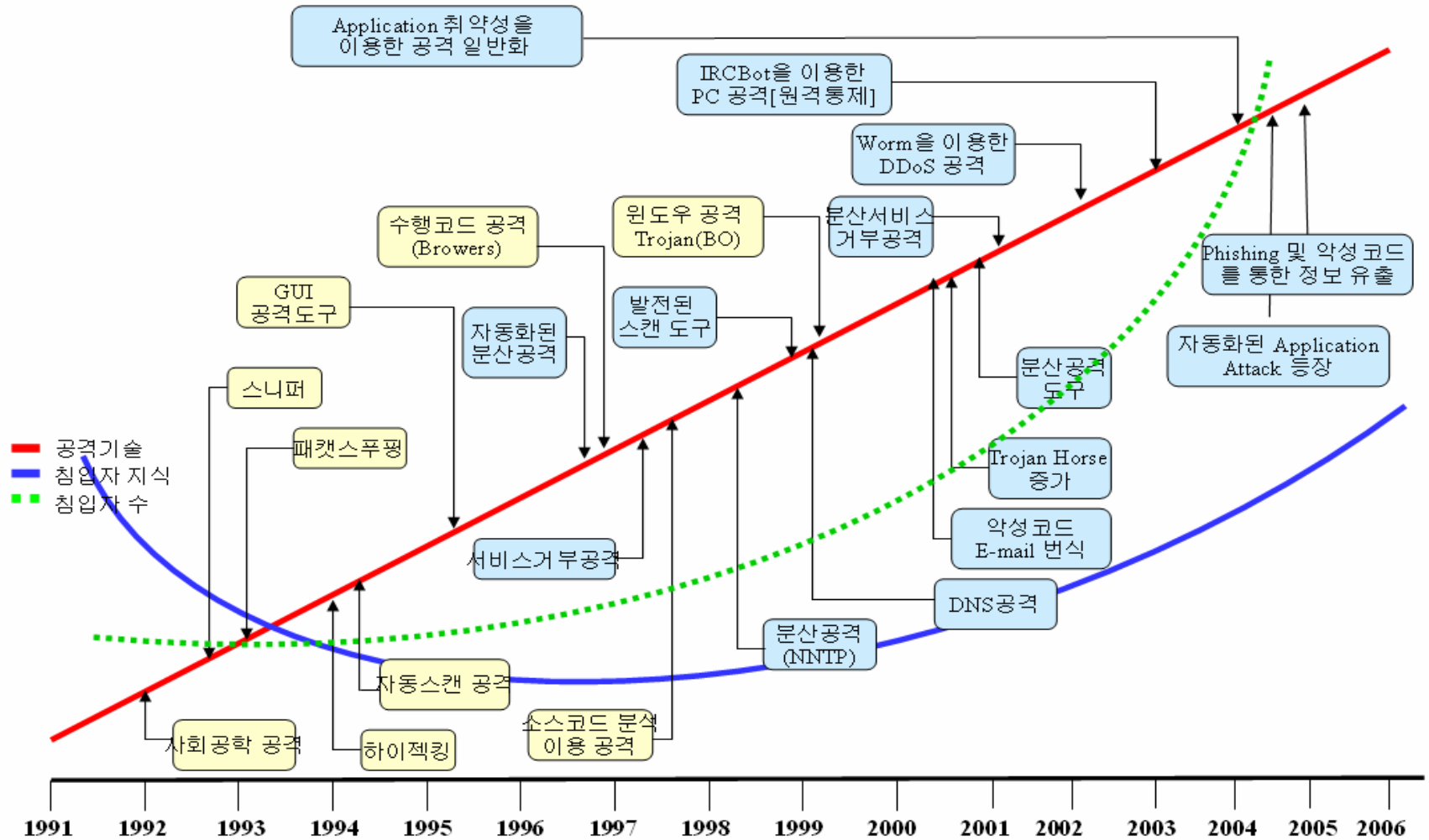
Vulnerability

- 취약성은 계속 증가하며 Application의 발달에 따라 더욱 많은 취약성들이 출현하게 될 것이다.



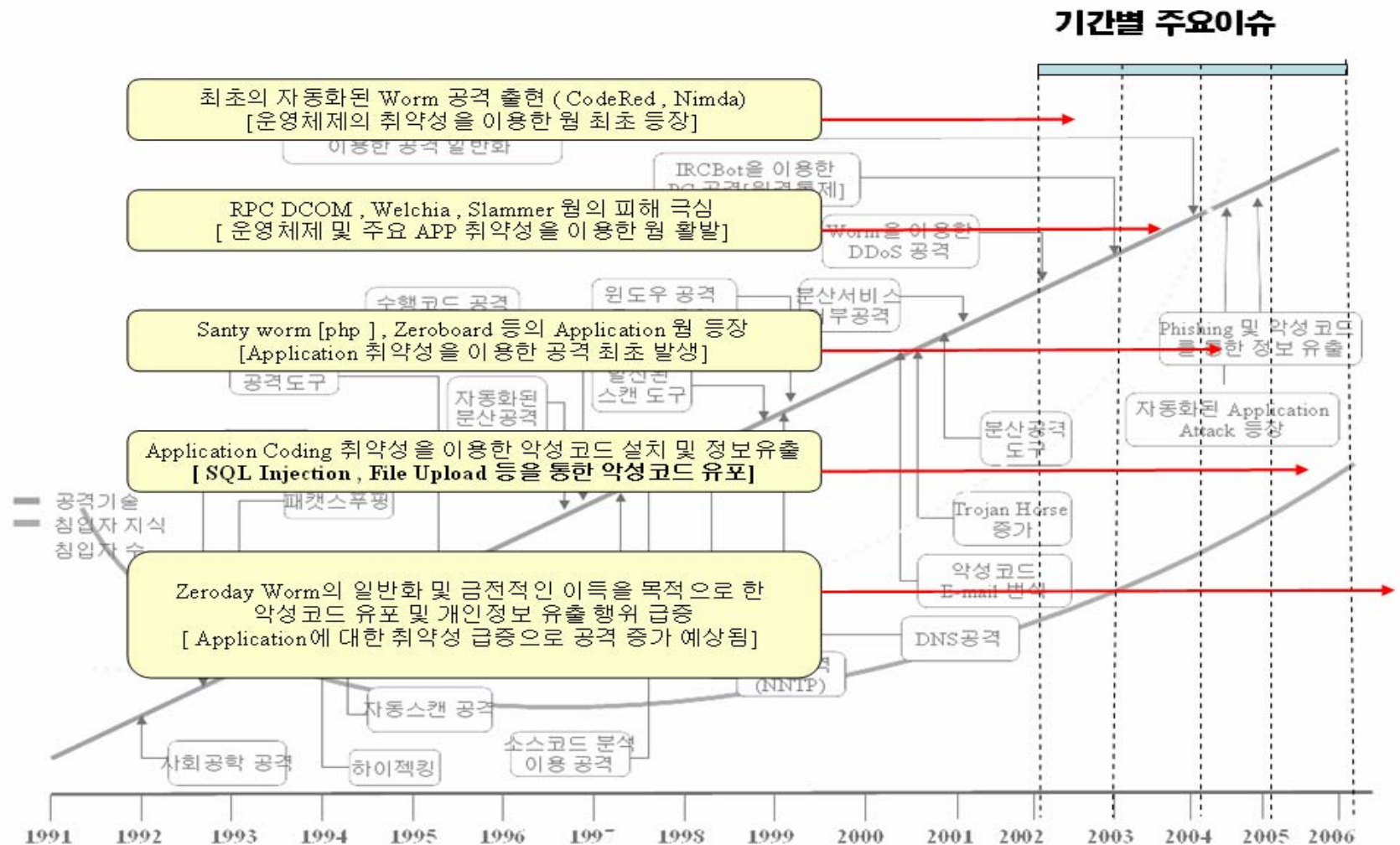
I. Security Trend

-위협요소



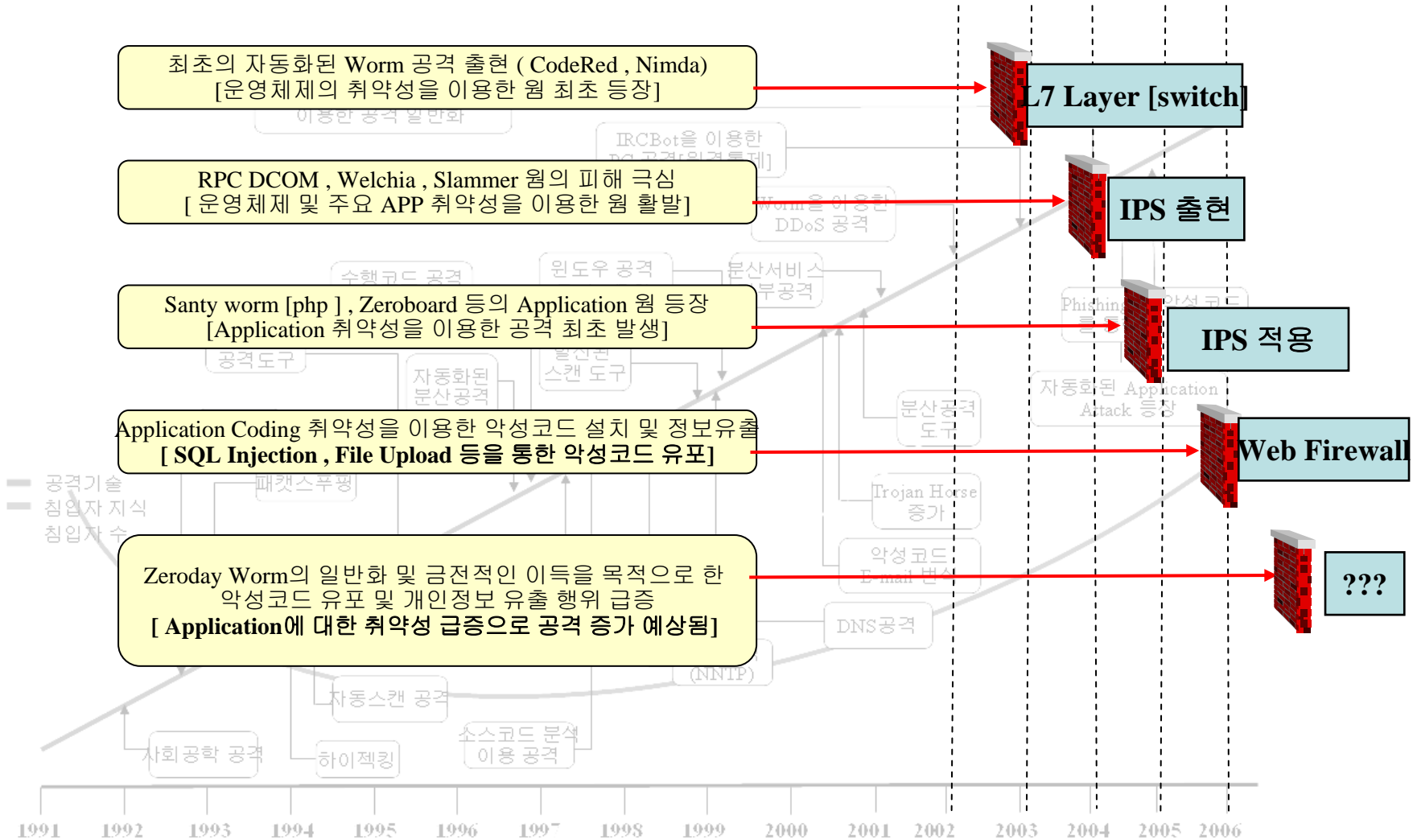
I. Security Trend

-위협요소



I. Security Trend

-위협요소



I. Security Trend

-공격 유형의 변화

1. APP 취약성을 이용 최초공격



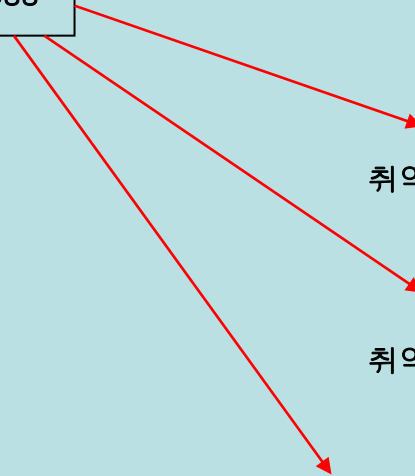
Attacker



취약 Application 서버 -A

Worm Process

2. 특정 Exploit 자동 생성 후 임의의 IP 대역에 대한 재 감염 시도



취약 Application 서버

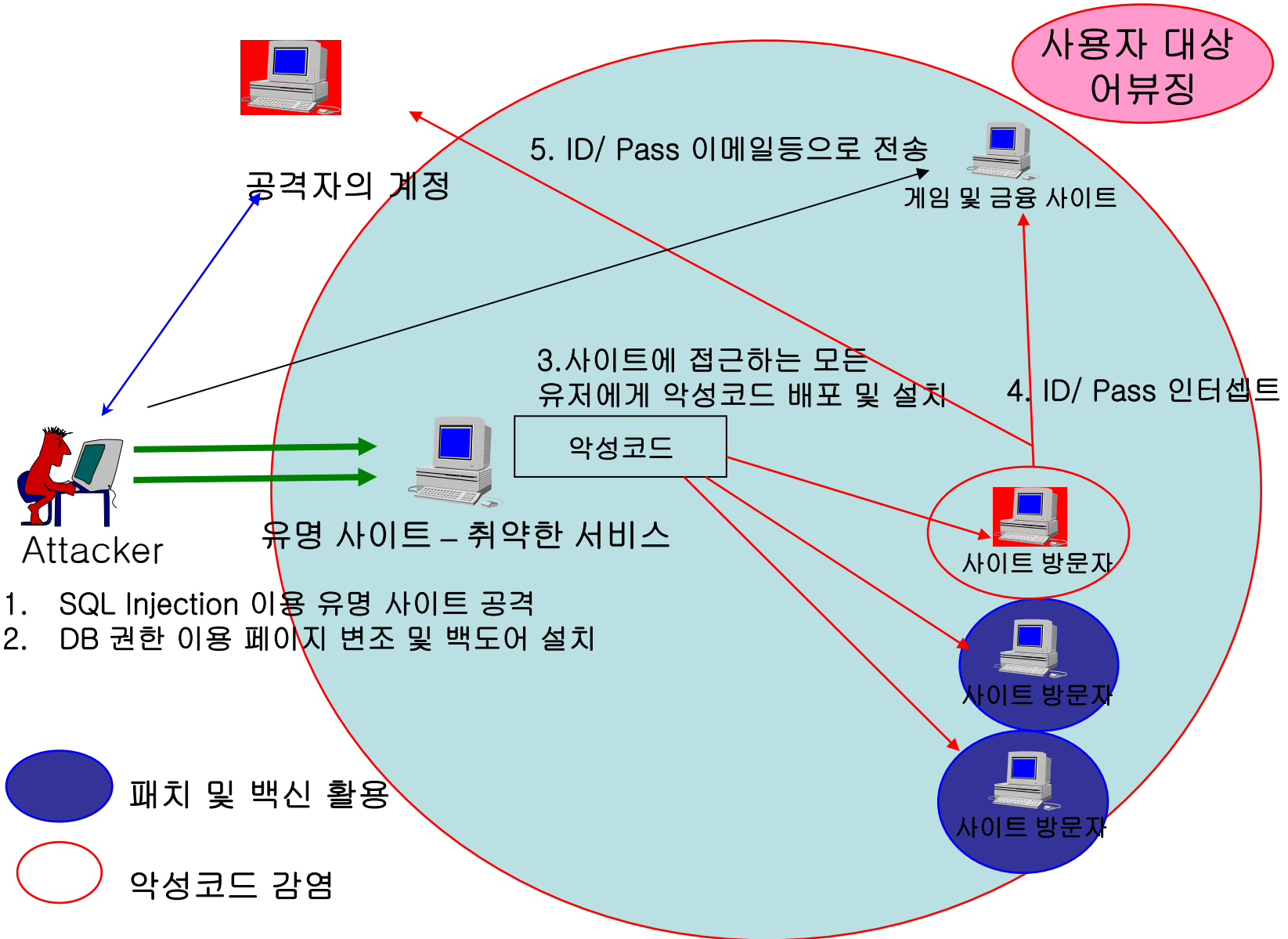
취약 Application 서버

취약 Application 서버

3. 추가 감염된 사이트 공격 계속

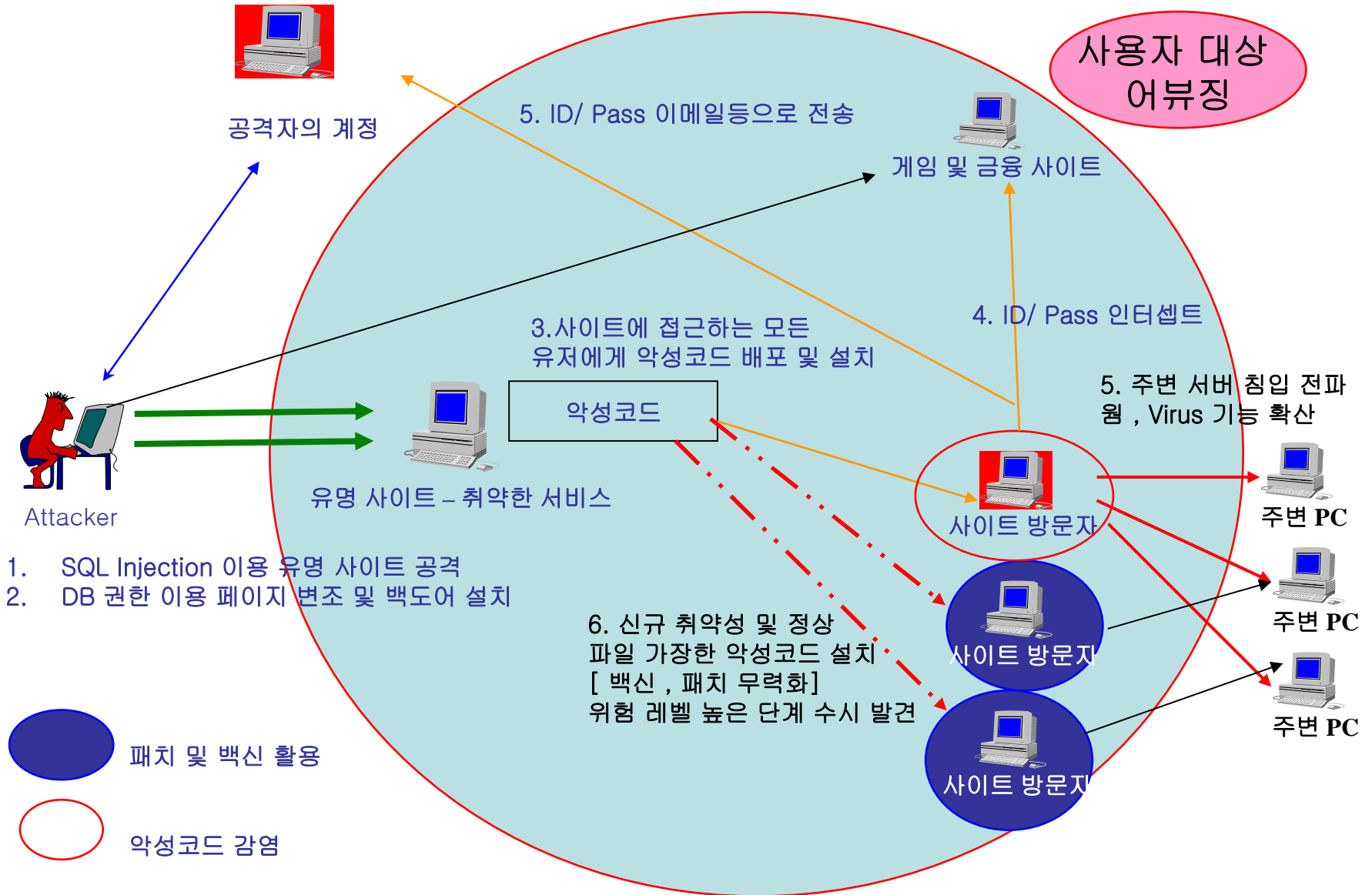
I. Security Trend

-공격 유형의 변화 [2006.9]



I. Security Trend

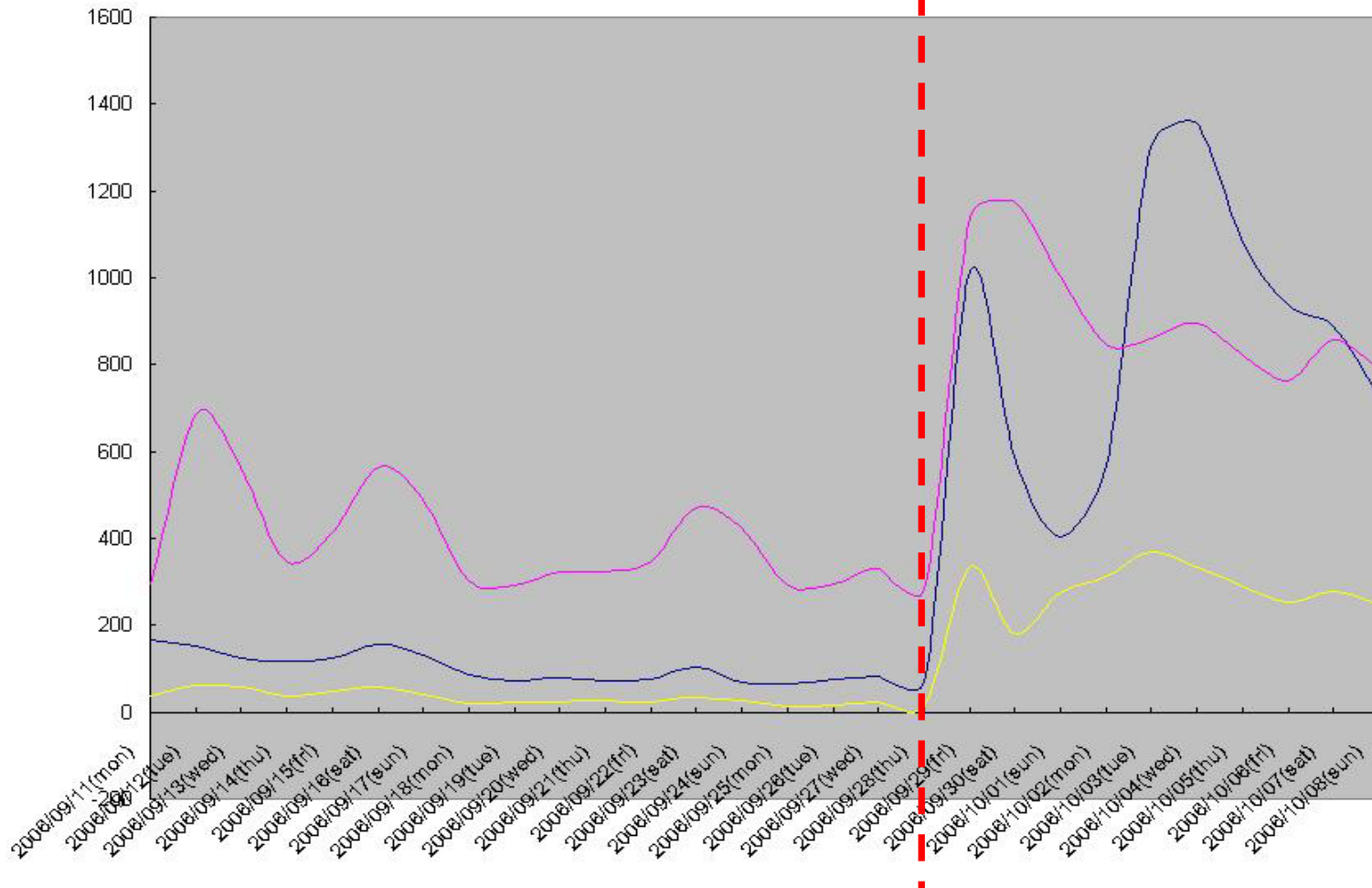
-공격 유형의 변화 [2006.10]



I. Security Trend

-Security의 변화

- 악성코드 흐름 – 전용백신 탐지 데이터 기반 [특정 게임 기반 -> 전체 온라인 서비스 기반으로 확산 조짐]



I. Security Trend

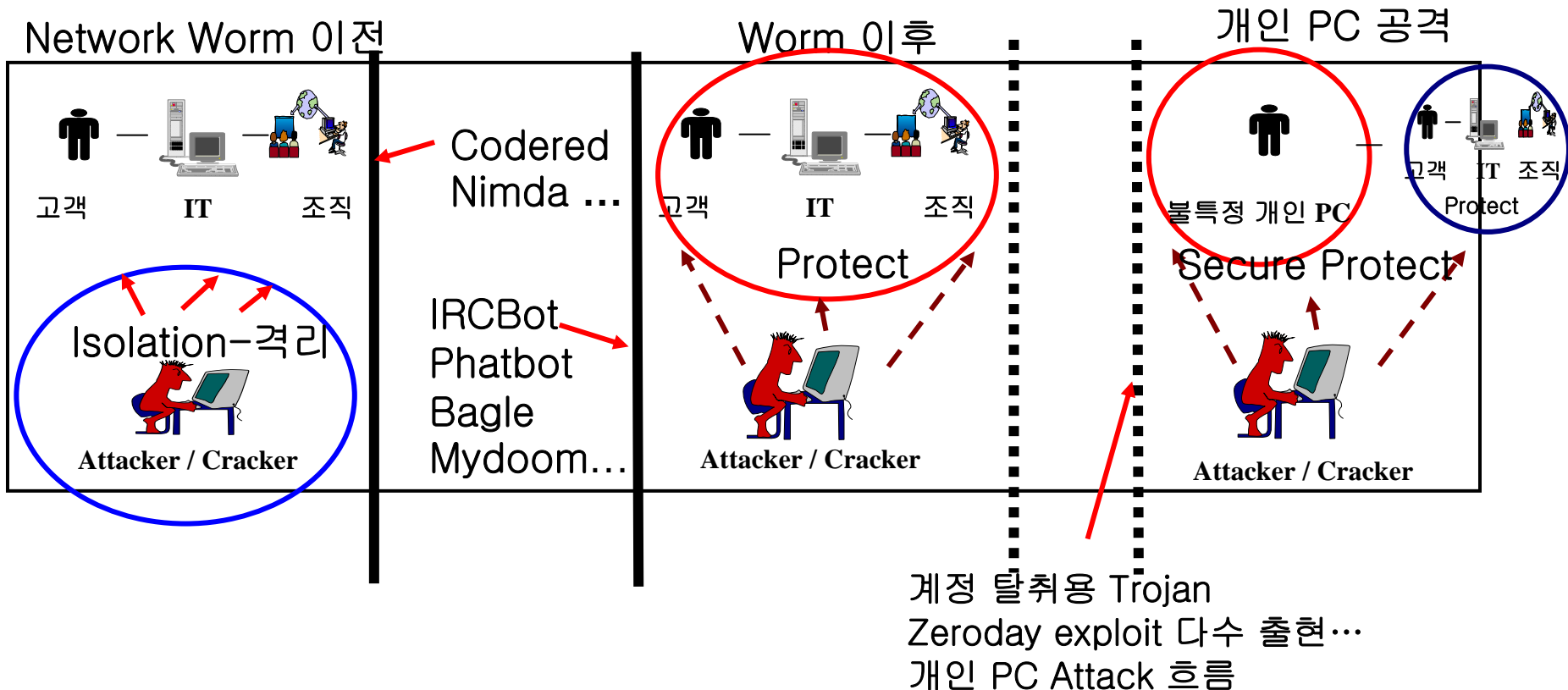
-Security의 변화

Security 패러다임은 worm의 출현을 기준으로 구분할 수 있으며 worm 발생 이전의 공격자의 격리를 주된 목적으로 하는 보안 정책에서 worm의 활성화 이후 자산의 보호로 급격하게 선회하였음. 현재는 개인 PC에 대한 공격으로 전환

- Red Zone의 이동 : 기업 -> 개인 PC (대응이 빠른 조직에만 이동 그외는 유효)

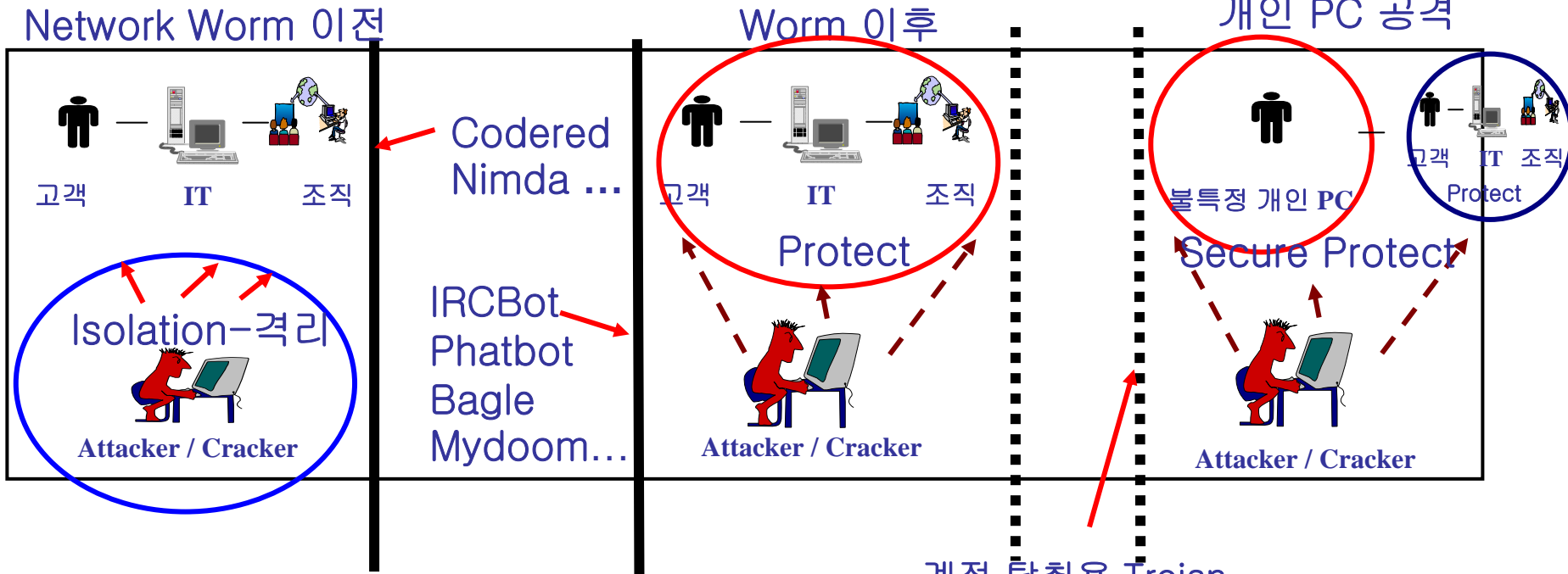
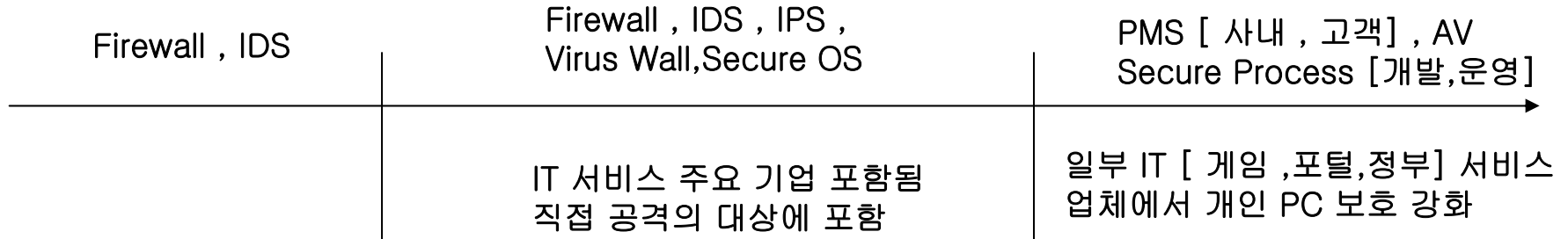
* 최근 IT 서비스 업체의 보안 분야 협력은 필연적인 프로세스임

* Secure Protect : Anti Virus, Personal Firewall, 보안 패치, Key board 보안 ...



I. Security Trend

-Security의 변화



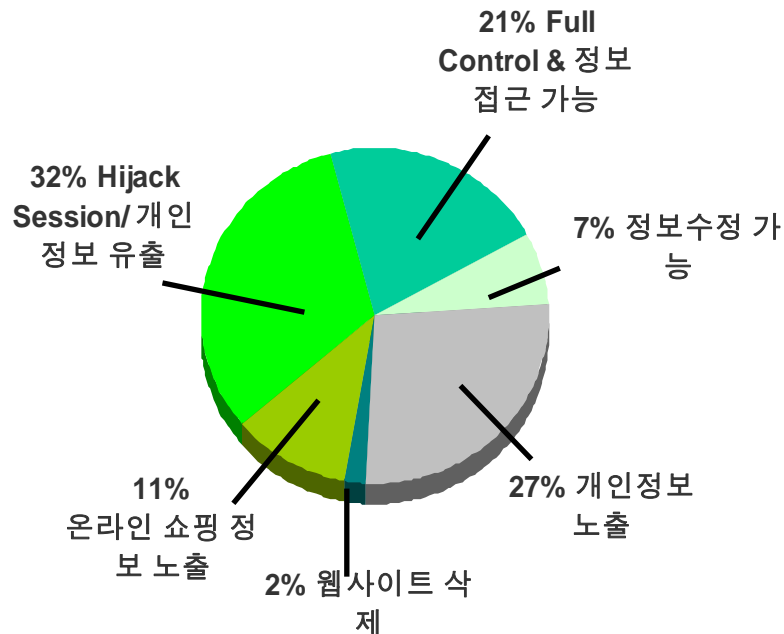
Codered
Nimda ...

IRCBot
Phatbot
Bagle
Mydoom...

계정 탈취용 Trojan
Zero day exploit 다수 출현...
개인 PC Attack 흐름

Web Application의 위기

Web Application Vulnerability



특정 **Web Application Scanner**를 이용해 **1000여개의 Site scan**시 **98%**의 사이트에 문제가 존재함...

Frequent

4개중 3개의 Website가 취약성을 지니고 있다. (Gartner)

Pervasive

75%의 해킹이 Application Level에서 발생한다. (Gartner)

Undetected

품질관리를 위한 도구들은 Security 문제점을 찾아내기 위한 도구들이 아니다.

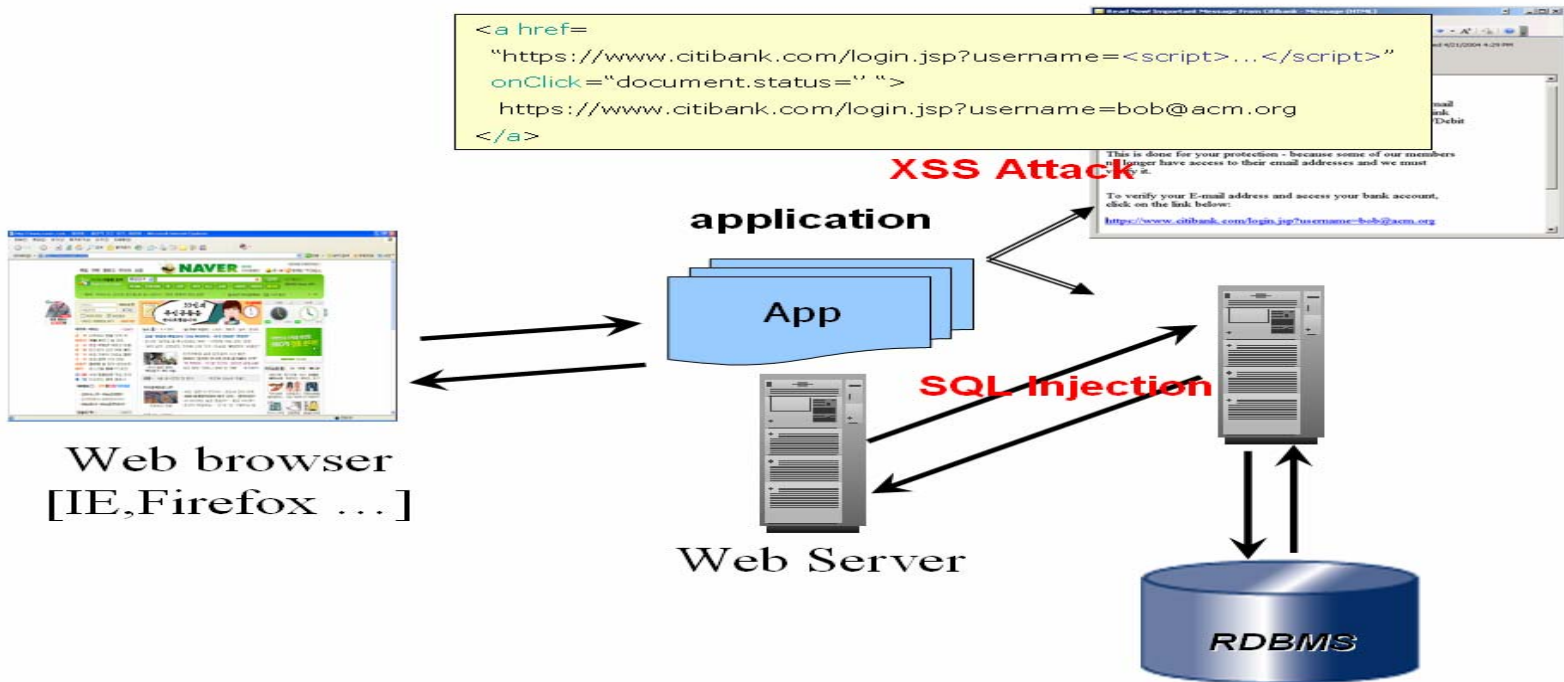
수작업에 의존한 탐색은 비용과 시간이 매우 많이 소요된다.

Dangerous

취약성을 통한 공격으로 위험이 노출 되었을때 회사의 신뢰도 및 고객의 믿음에 영향을 끼친다.

II. 대응

-Web상의 주요 위험요소[한국]



- Attack A: SQL injection

- Scenario:

- 공격자가 SQL 구문의 일부인 것 처럼 하여 DB 서버에 직접 쿼리를 실행 시키도록 함

- 피해:

- Read unauthorised data, update or remove DB records, etc.

- Attack B: Cross-site scripting [XSS Attack]

- Scenario:

- 웹페이지 링크를 속이거나 스크립트를 실행 시키는 게시물등을 작성하여 유포함

- Potential damage:

- 사용자의 쿠키 정보 및 악성코드를 실행 할 수 있다.

II. 대응

-Web상의 주요 위험요소[한국]

- SQL Injection 설명

‘ 특수문자에 대한 필터링 부족 및 DB Query 문의 실행 , 입력 문자열 길이의 제한 부재로 인해 발생한 문제

실행 원리:

- 대부분의 웹서버 사용자 인증 과정

- Select * from member where id="txtid" and pw="txtpw"

- 위의 쿼리 문에서 POST 방식으로 txtid , txtpw 인자값을 전송하는 방식

- 문자를 내부적으로 처리시에 ‘ ‘ 인용부호를 붙여서 사용함

- ‘ 문자 입력시 SQL 문이 제대로 구성되지 않는 점을 이용

- URL의 인자 단위에서 Validation 체크 부족으로 인하여 문제 발생됨

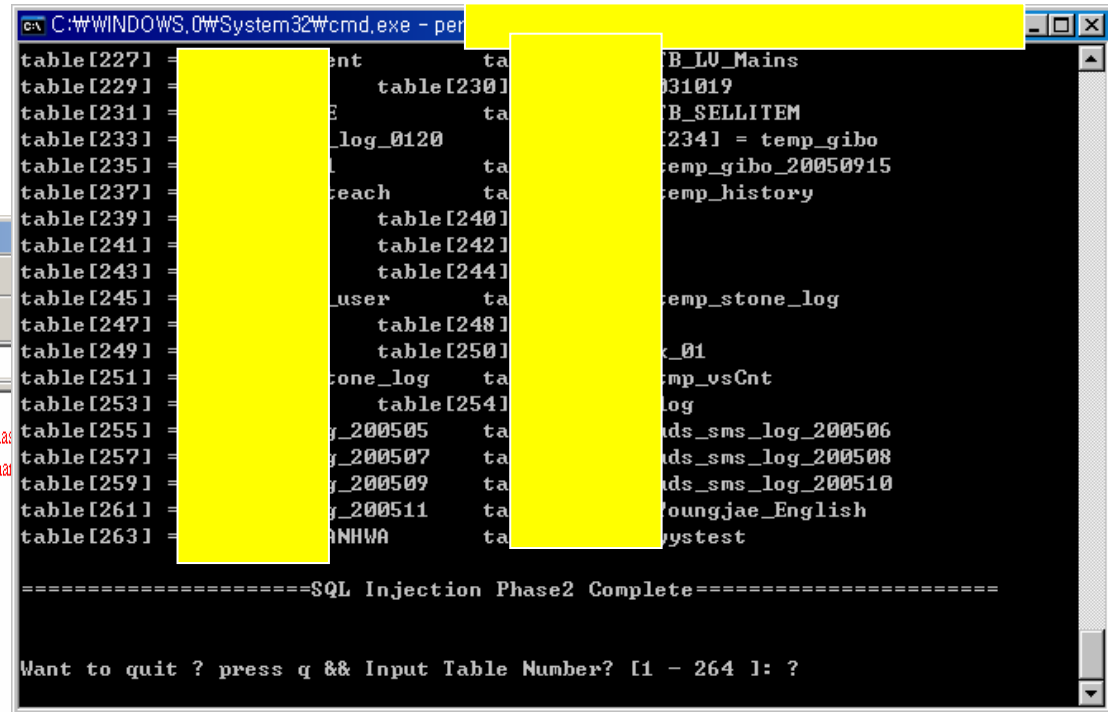
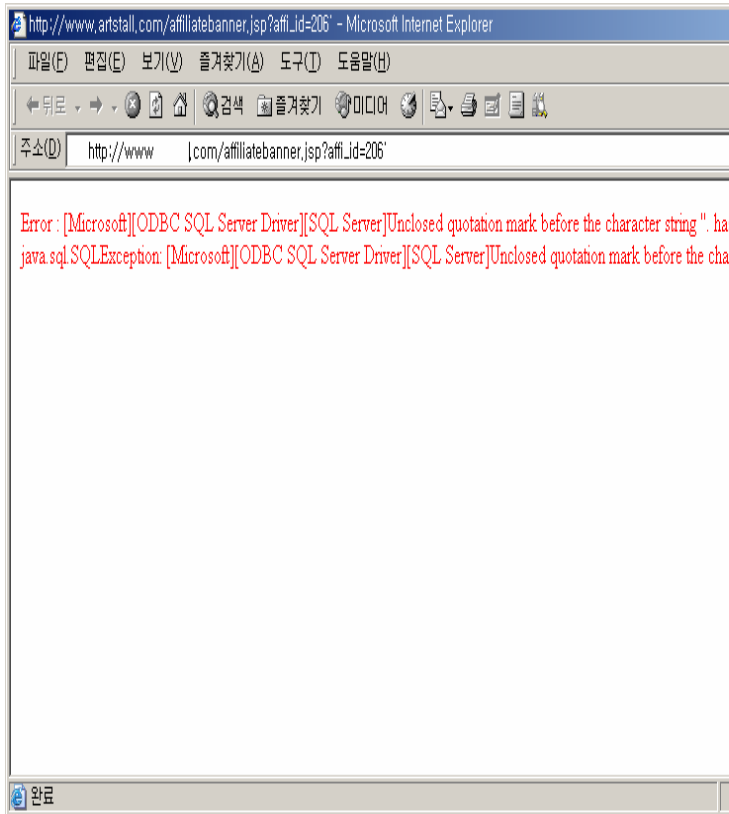
- <http://xxx.xxx.co.kr/board/view.asp?bid=C060201&no=116895> 정상쿼리

- <http://xxx.xxx.co.kr/board/view.asp?bid=C060201&no=116895> ' and db_name() 와 같이 bid ,no 와 같은 인자 뒤에 SQL Query 구문 입력시 DB로 명령이 실행 되어 결과가 리턴 되는 문제 [DB에 대한 통제권을 잃게됨]

II. 대응

-Web상의 주요 위험요소

SQL Injection Sample [Input Validation Problem]



[Microsoft][ODBC SQL Server Driver][SQL Server]Unclosed quotation mark before the character string '訝??', SQL state 37000 in SQLExecDirect in E:\wnewwshow_database_info.php on line 19

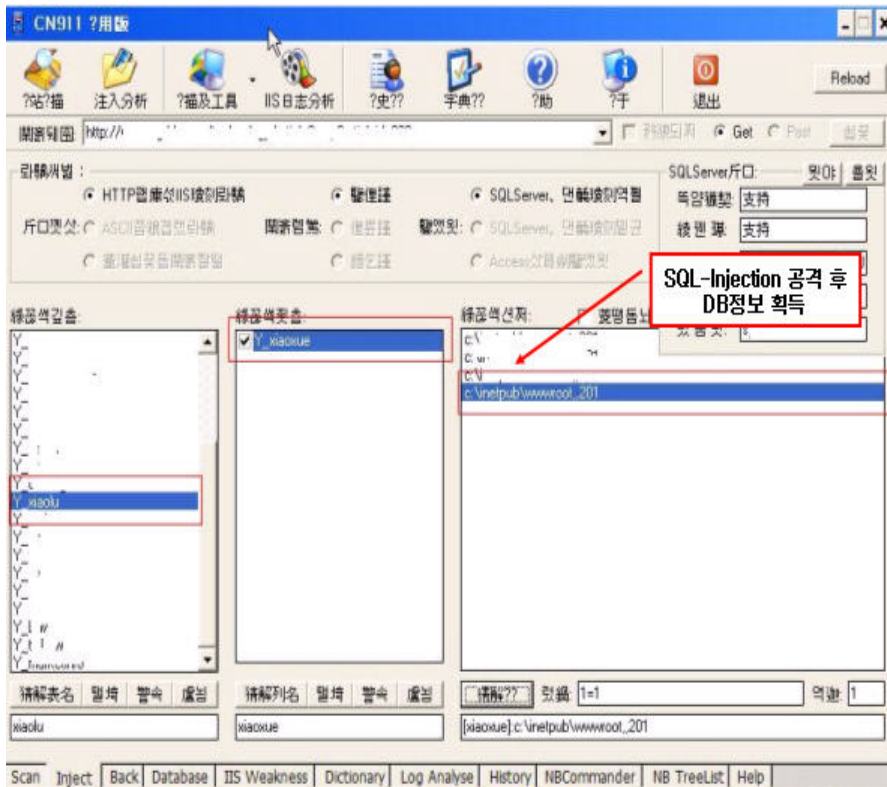
[Microsoft][ODBC SQL Server Driver][SQL Server]Unclosed quotation mark before the character string '訝??', SQL state 37000 in SQLExecDirect in E:\wnewwshow_database_info.php on line 24

argument is not a valid ODBC result resource in E:\wnewwshow_database_info.php on line 25

II. 대응

-Web상의 주요 위험요소

웹 소스의 Validation problem을 이용한 Database 직접 쿼리 [by china]



2005-06-11 17:23:02 xxx.xxx.xxx.xxx - Target_IP 80 GET /announce/new_detail.asp?

id=529|27|80040e14|[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]?

Unclosed_quotation_mark_before_the_character_string_... 500 Mozilla/4.0+
(compatible;+MSIE+6.0;+Windows+NT+5.2;+SV1;+.NET+CLR+1.1.4322)?

Stored procedure로
시스템 접근 가능?

2005-06-11 17:23:34 xxx.xxx.xxx.xxx - Target_IP 80 GET /announce/new_detail.asp?

id=529;DELETE%20bb;insert%20bb%20exec%20master..xp_dirtree%20C:\w\1,1--200
Microsoft+URL+Control+--+6.00.8862?

2005-06-11 17:23:02 xxx.xxx.xxx.xxx - Target_IP 80 GET /announce/new_detail.asp?

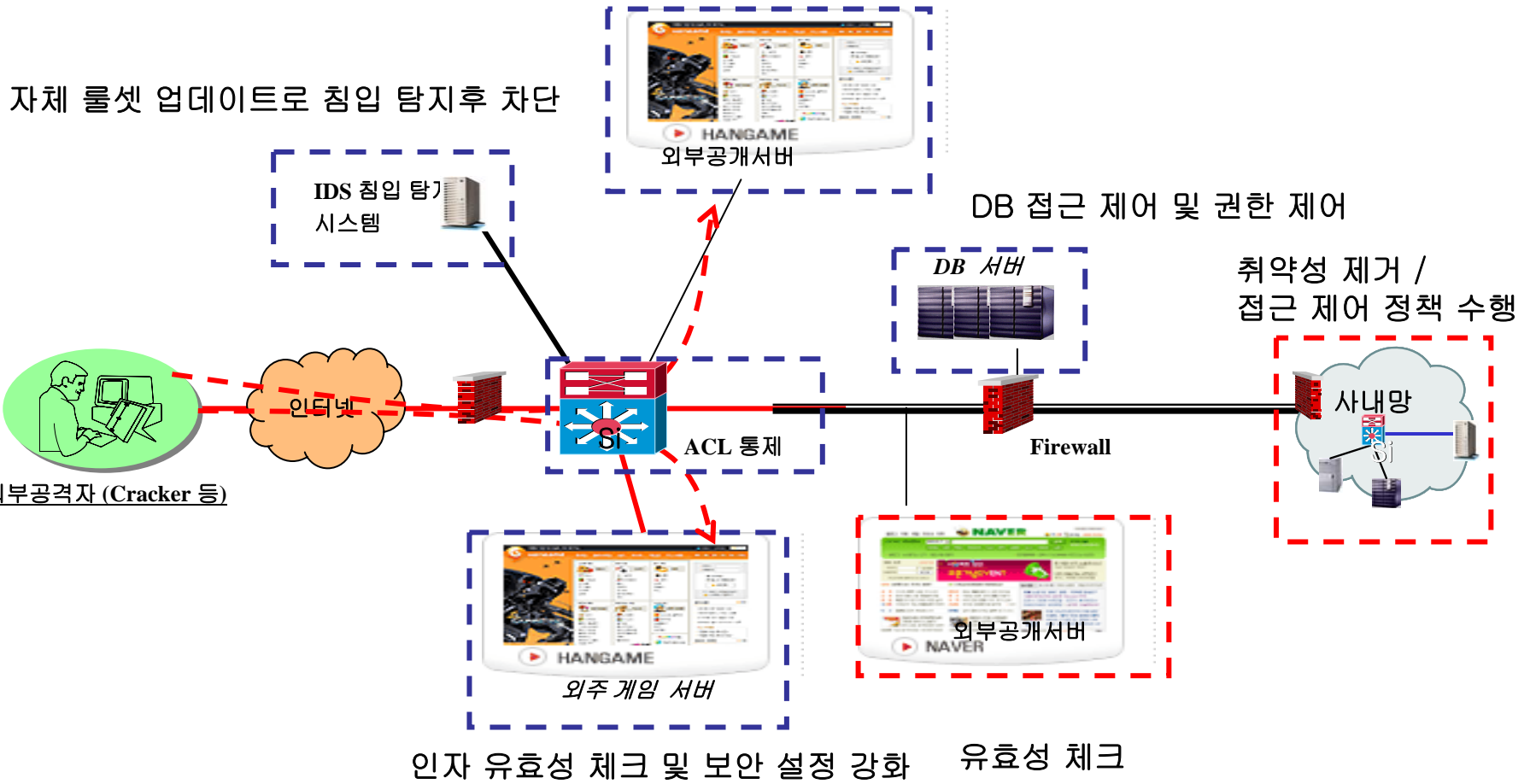
id=529|27|80040e14;DROP%20TABLE%20NB_TreeList_Tmp;CREATE%20TABLE%20NB_Tre
eList_Tmp(subdirectory%20nvarchar(256)%20NULL,depth%20tinyint%20NULL,[file]%20bit
%20NULL)-- 200 Microsoft+URL+Control+--+6.01.9782?

II. 대응

-Process에서의 대응

보안성검수 [Penetration Test]가 가장 중요한 최종 단계 역할 수행

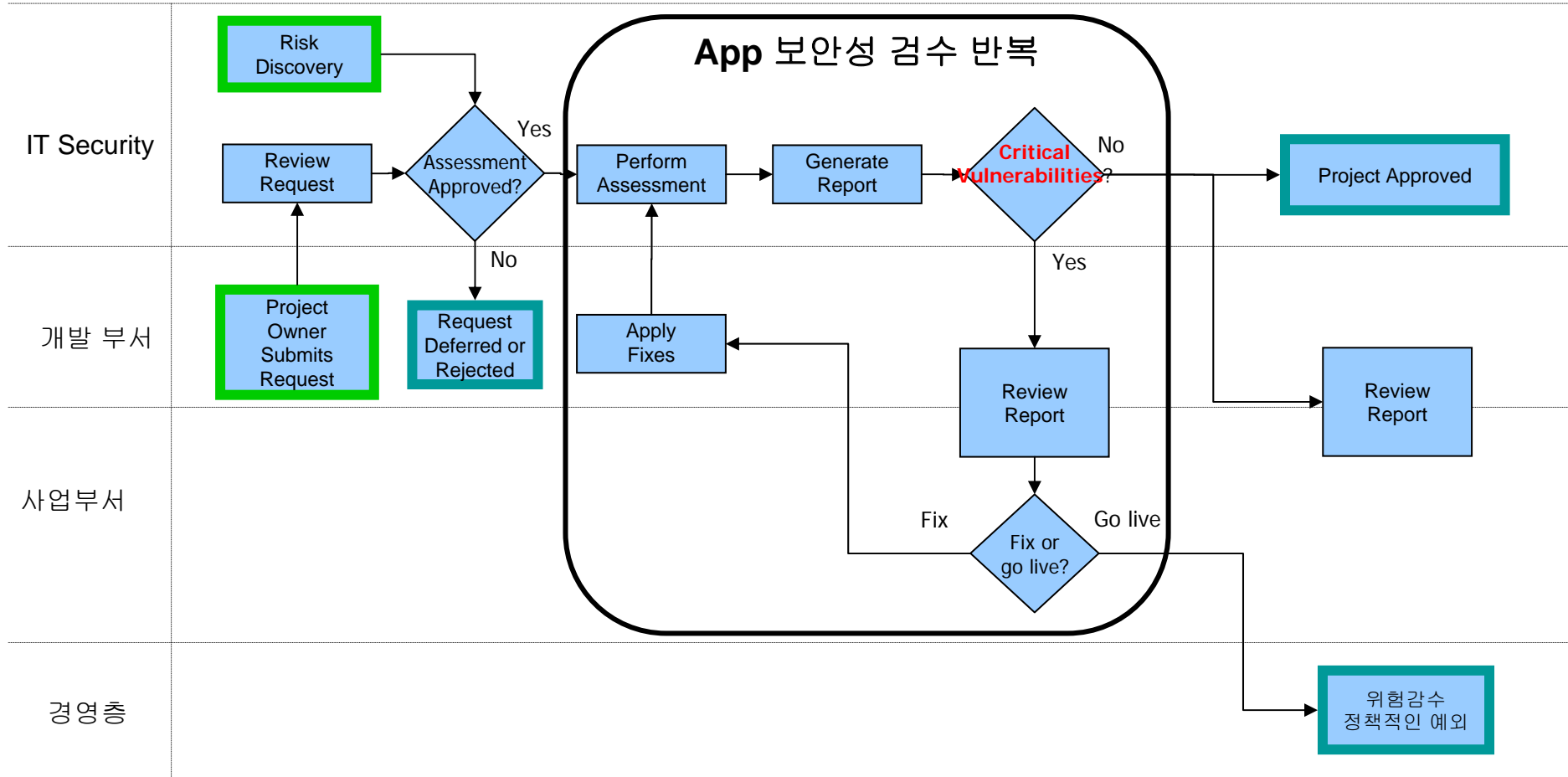
웹 서버 인자 유효성 체크 & Penetration Test



II. 대응

Secure Programming & Secure Inspection

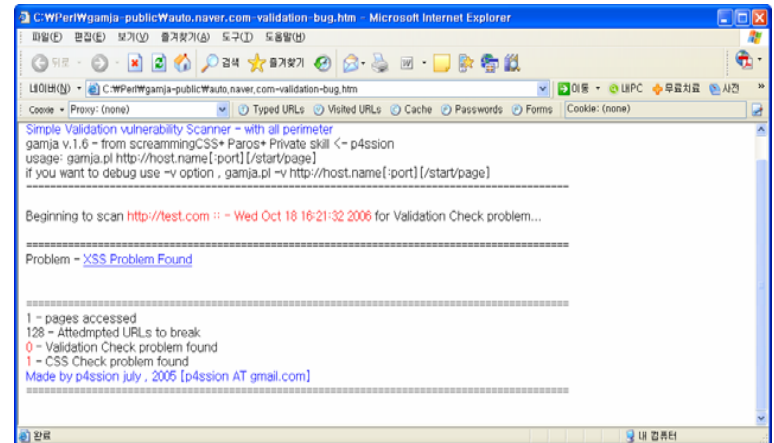
기본적으로 운영 서비스에 대한 보안성 검수는 반드시 이루어 져야 문제 방지됨



II. 대응

보안성 검수 중 Input validation check가 가장 위험요소가 높은 부분
국내 다수 웹서버에 문제 존재함 [상용 스캐너 및 공개용 사용 필요성 높음]
공개용 - Gamja download at <http://lastlog.com/p4ssion>
상용 - Appscan , Acunetix , Scando 등 다수 ..

```
C:\WINDOWS\system32\cmd.exe  
C:\Perl\gamja-public>gamja.pl "http://test.com/testpage"
```

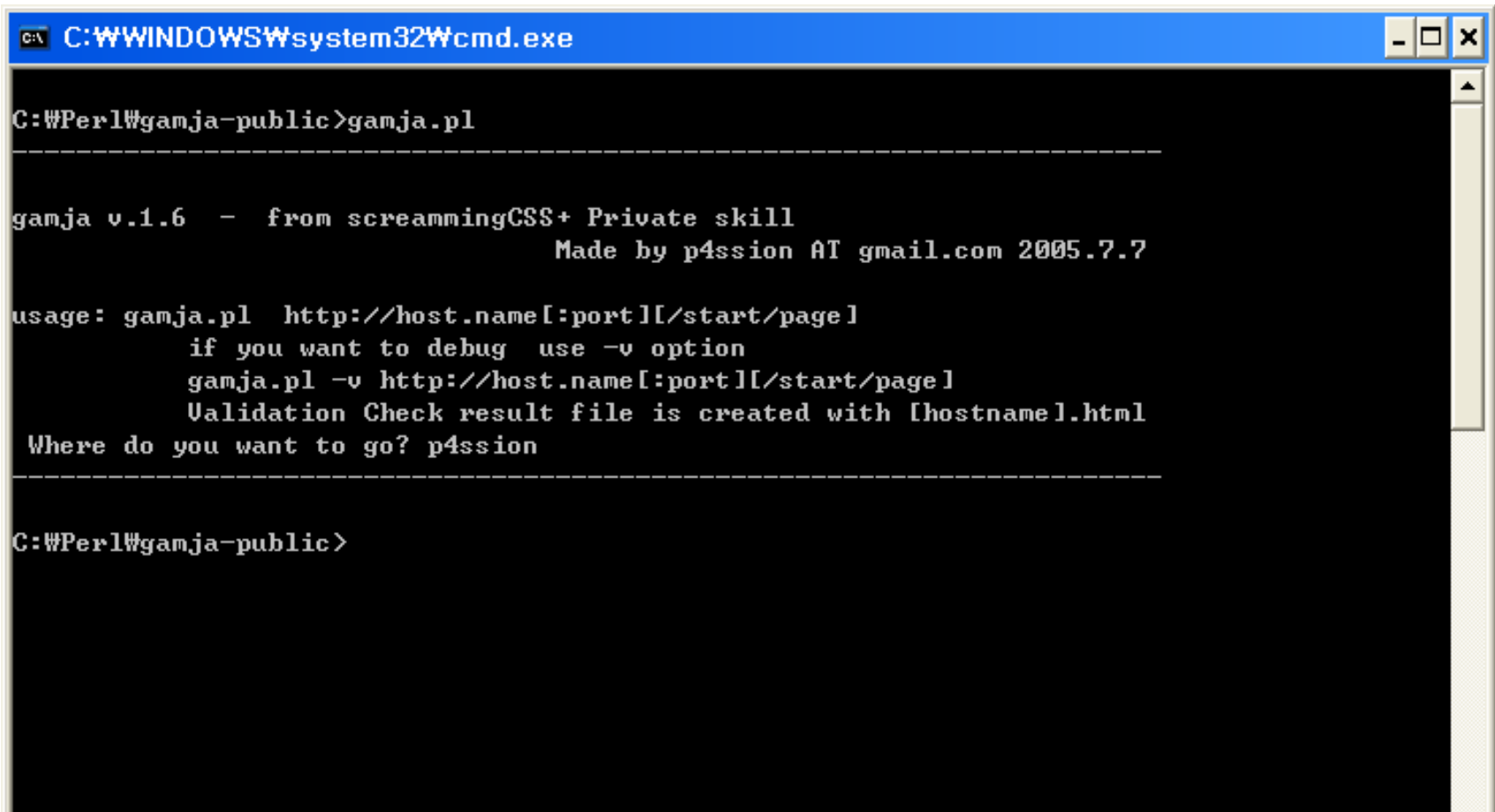


Problem Clear
[XSS , SQL Injection ...]

문제확인 및 수정
[XSS , SQL Injection ...]

II. 대응

Secure Programming & Secure Inspection For Web
Gamja.pl “http://target.host/start-page”
Requirement: Wget [Windows] + Perl



```
C:\WINDOWS\system32\cmd.exe

C:\Perl\gamja-public>gamja.pl

-----

gamja v.1.6 - from screamingCSS+ Private skill
                Made by p4ssion AT gmail.com 2005.7.7

usage: gamja.pl http://host.name[:port][start/page]
        if you want to debug use -v option
        gamja.pl -v http://host.name[:port][start/page]
        Validation Check result file is created with [hostname].html
Where do you want to go? p4ssion

-----

C:\Perl\gamja-public>
```

II. 대응

XSS 대책

● 텍스트 문장의 가운데에 특수 문자가 나올 경우 (HTML 로 문장이 표현될 경우)
“<” 태그를 시작하는 문자 , “&” 문자 속성을 나타내는 문자 , “>”

태그의 끝을 나타내는 문자의 경우 처리가 필요하다. -

● <script> </script> 의 body 부분에 위치하는 문자의 경우
세미콜론과 { } , [] 문자들은 필터링이 이루어 져야 한다.

● < , > 문자에 대한 치환 혹은 <script , </script> 문장이 HTML 입력 필드 내에 출현할 경우에는
반드시 치환이 되어 < = < ; , > = > ; 등의 문자로 치환하여 행위가 발생하지 않도록
처리할 것을 권고한다.

변환 대상(From)	변환값(To)
<	<
>	>
((
))
#	#
&	&

II. 대응

SQL Injection 대책

사용자가 숫자를 입력해야 한다면, ISNUMERIC 함수등을 이용해 입력을 검사한다.
문자열을 입력 시, '을 ' ' 로 바꾼다. (작은 따옴표 두개로 바꿔준다) 또한 '을 W' 로 바꾸는 방법도 있다.
PHP 응용 프로그램의 경우 php.ini 환경 설정 파일에서 magic_quotes_gpc 옵션을 on으로 설정한다.
사용자로부터 입력 받은 내용을 DBMS 서버에 query로 보내기 이전에
특수 문자를 제거하거나 특수 문자에 독특한 처리를 하는 함수
(예: PHP의 htmlspecialchars()와 addslashes())를 사용하도록 한다.

패턴	설명
'	문장 종료
--	주석 시작
,@variable	변수 처리시 사용, stored procedure 파악에 유용
+	URL의 space, SQL 구문 삽입에 이용
@@variable	SQL 변수 처리시 사용
PRINT	ODBC 에러 반환 통해 SQL 구문 삽입 공격 정보 수집
SET	SQL 구문 삽입에 이용
%	와일드 카드로 사용
OR 1=1	SQL 구문 삽입에 이용
UNION	SQL 구문 삽입에 이용
AND	SQL 구문 삽입에 이용
INSERT	SQL 구문 삽입에 이용

Q&A