업로드 취약점을 이용한 악성코드 유포 사례

2005. 10. 28

KrCERT/CC
인터넷침해사고대응지원센터

KISA 한국정보보호진흥원
Korea Information Security Agency

※ 본 보고서의 전부나 일부를 인용시 반드시 [자료: 한국정보보호진흥원(KISA)]를 명시하여 주시기 바랍니다.

1. 개요

최근 포털 등 유명 웹 사이트들이 연이어 해킹당해 악성코드가 삽입되는 사고가 지속적으로 발생되고 있다. 이러한 공격은 일반적으로 다음의 과정을 통해 이루어진다.

① 공격자는 홈페이지에 존재하는 SQL Injection 취약점을 주로 이용하여 해킹을 수행
② 해킹한 국내 웹사이트들의 초기 화면에 특정 iframe을 삽입
해당 iframe은 사용자 PC를 감염시킬 수 있는 특정 사이트(악성코드 유포 사이트)로 접속을 유도함
③ 인터넷 사용자가 해킹당한 웹사이트에 방문
④ 인터넷 사용자의 PC가 보안패치 되지 않았을 경우 악성코드 유포 사이트로부터 트로이목마 프로그램 등에 감염
⑤ 감염된 인터넷 사용자의 게임 ID와 패스워드 등 정보를 특정 주소로 유출

이러한 과정을 통해 최근 중국에 할당된 IP로부터 많은 공격이 발생되고 있으며 국내 유명 웹사이트들이 해킹을 당해 iframe이 삽입되어 악성코드 유포를 위한 경유지로 이용되고 있다.

다수개의 국내 악성코드 경유지 사이트들은 실제 인터넷 사용자 PC를 감염시킬 수 있는 특정 악성코드 유포사이트로 접속하도록 iframe이 설정되어 있다. 악성코드 경유지 사이트는 국내 인터넷 사용자들의 접속이 많은 국내 웹사이트들이 주로 이용되고 있으며, 악성코드 유포사이트는 중국 등 해외나 국내 웹사이트가 역시 해킹당해 유포사이트로 악용되는 경우도 있다.

본 보고서에서는 실제 악성코드 유포 사이트로 이용되고 있었던 국내 웹서버를 분석하였다. 악성코드 유포 경유지로 이용되었던 국내 웹 사이트들은 대부분 게시판에 존재하는 SQL Injection 취약점을 이용하여 공격을 받았으나, 이번에 분석한 유포 사이트의 경우 파일 업로드 취약점을 이

용하여 공격을 받았다. 또한, 1천명 이상의 인터넷 사용자들이 악성코드(트로이목마)가 다운로드 될 수 있는 특정 웹페이지에 접속한 흔적도 발견할 수 있었다.

2. 피해 분석

해당 피해 시스템은 홈페이지 제작 전문업체의 서버였으며, 윈도우즈 2000서버에 IIS 5.0을 사용하고 있었다. 이 웹서버는 수십개 가량의 웹 사이트를 호스팅하고 있는 웹호스팅용으로 사용되고 있었다.

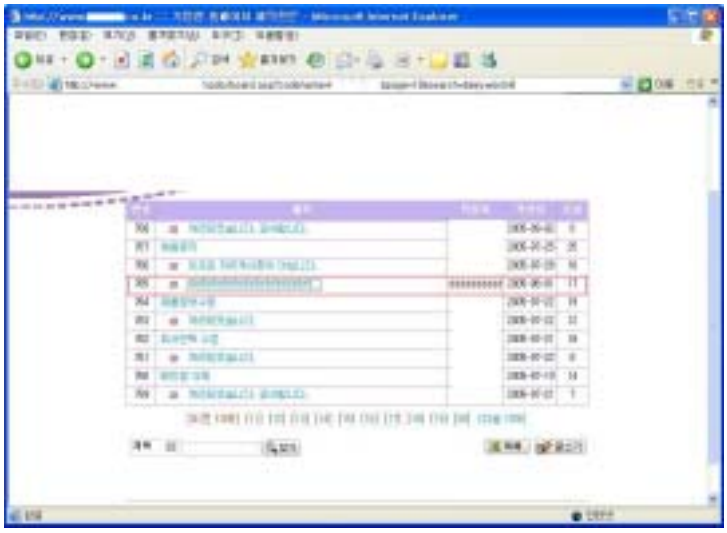
해당 피해 시스템이 악성 코드 유포사이트로 사용되고 있다는 사실은 인터넷침해사고대응지원센터에서 자체 개발한 악성코드 삽입 여부를 모니터링할 수 있는 도구를 통해 알게 되었으며, 인터넷침해사고대응지원센터에서 연락했을 당시 시스템에 평소 시스템의 이상현상은 느끼고 있었으나, 악성코드가 삽입된 사실은 모르고 있었다.

해당 시스템은 파일 첨부 기능을 가진 게시판의 업로드 취약점을 이용하여 원격에서 피해 시스템을 마음대로 제어할 수 있는 해킹 프로그램을 설치한 후 이 프로그램을 이용하여 인터넷 사용자들을 감염시킬 수 있는 악성코드(icyfox.js)를 설치하였다.

□ 업로드 취약점을 이용한 해킹 프로그램 설치

해당 피해 시스템은 2005년 8월 1일경 웹 사이트에서 제공하는 게시판의 업로드 취약점으로 인해 공격을 받았다. 해당 게시판은 그림 파일 등을 첨부하여 글을 게시할 목적으로 만들어졌으나, 공격자는 해킹 프로그램(파일명 : svnge.asa)을 첨부하여 글을 게시한 후 이 해킹 프로그램을 웹 브라우져를 통해 실행함으로써 해당 피해 시스템을 장악하였다.

아래 그림은 공격자가 해킹 프로그램을 게시한 화면이다.



공격자가 이처럼 게시판을 이용하여 해킹을 할 수 있었던 것은 해당 피해 시스템이 다음과 같은 3가지 취약점을 가지고 있었기 때문으로 볼 수 있다.

첫째, 게시판을 통해 업로드되는 첨부파일을 확장자에 따라 필터링하지 않았다.
본 사고에서 공격자는 스크립트 파일 업로드 차단을 우회하기 위해 *.asa라는 확장자를 사용하여 파일을 첨부하였다. 따라서, 게시판 등에서 그림 파일 등 일부 업로드를 허용하는 파일 종류를 정의한 후 나머지는 모두 차단하는 것이 바람직할 것이다.

둘째, 업로드된 파일의 경로를 쉽게 공격자가 확인할 수 있었다.
업로드된 파일이 시스템상의 어디에 위치하는지 알 수 있을 경우 웹브라우저를 통해 이 파일을 직접 실행할 수 있다. 해당 피해 시스템의 경우도 첨부파일의 절대경로가 상태 표시줄에 고스란히 표시되어 쉽게 그 경로를 알 수 있도록 되어 있었다.

셋째, 파일들이 업로드되는 폴더에서 실행 권한이 주어져 있었다.
일반적으로 업로드 폴더에는 스크립트 프로그램들이 실행될 수 없도록 실행권한을 주지 않는 것이 안전하다.

위의 취약점으로 인해 해당 피해 시스템은 공격이 가능하였으며, 해킹 프로그램이 업로드된 시점의 웹로그는 아래와 같이 남았다(웹로그의 시간은 시스템 시간에 비해 9시간 느렸음).

2005-08-01 02:36:37 xxx.173.159.175 - victim_IP 80 GET /xxx/xpds/content.asp codename=tbxxxpds&number=1097&ref=440&page=1&startpage=1 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+TencentTraveler+)
2005-08-01 02:36:37 xxx.173.159.175 - victim_IP 80 GET /xxx/xpds/font.css - 404 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+TencentTraveler+)
2005-08-01 02:36:51 xxx.173.159.175 - victim_IP 80 GET /xxx/xpds/data/svnge.asa action=login 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+TencentTraveler+)
2005-08-01 02:37:03 xxx.173.159.175 - victim_IP 80 POST /xxx/xpds/data/svnge.asa - 302 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+TencentTraveler+)

2005-08-01 02:37:05 xxx.173.159.175 - victim_IP 80 GET /xxx/xpds/data/svnge.asa - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+TencentTraveler+)
2005-08-01 02:37:05 xxx.173.159.175 - victim_IP 80 GET /index.asp - 302 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+TencentTraveler+)
2005-08-01 02:37:05 xxx.173.159.175 - victim_IP 80 GET /xxx/xpds/data/svnge.asa Action=MainMenu 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+TencentTraveler+)
2005-08-01 02:37:08 xxx.173.159.175 - victim_IP 80 GET /xxx/xpds/data/svnge.asa Action=ShowFile 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+TencentTraveler+)

위의 로그를 통해 공격자가 해킹 프로그램(svnge.asa)을 첨부파일로 업로드 하고, 해당 해킹 프로그램을 웹 브라우져를 통해 실제 실행해 본 것을 확인해 볼 수 있다.

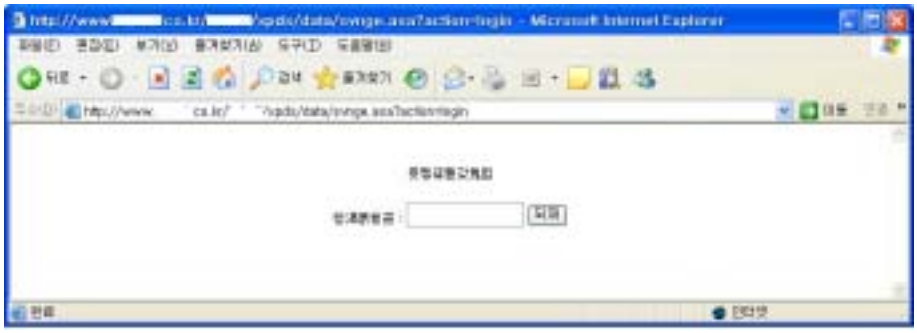
공격지 IP는 중국에 할당된 IP였으며, 8월 1일 이후 10월까지 해당 IP 블록에서 지속적으로 피해 시스템에 접속한 흔적이 남아 있었다.

inetnum:	xxx.173.0.0 - xxx.173.255.255
netname:	CHINANET-GX
descr:	CHINANET guangxi province network
descr:	China Telecom
descr:	No.31,jingrong street
descr:	Beijing 100032
country:	CN

□ 해킹 프로그램(svnge.asa) 분석

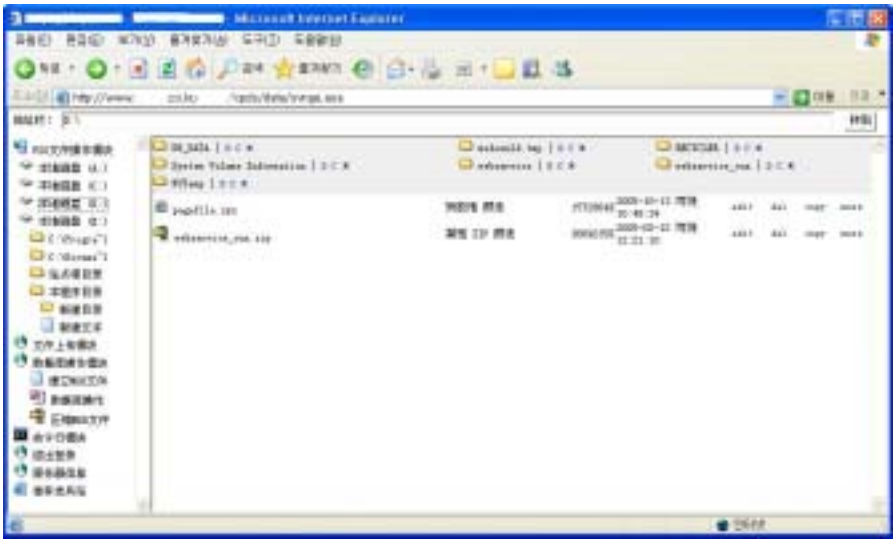
svnge.asa라는 해킹프로그램은 실제 실행가능한 ASP 프로그램으로 원격지에서 웹 브라우져를 통해 접속하여 피해 시스템을 자유로이 제어할 수 있는 일종의 백도어 역할을 한다. 최근 중국 IP 블록으로부터 해킹 피해를 받은 많은 시스템들에서 이와 유사한 백도어 기능을 가진 해킹 프로그램들을 찾아볼 수 있다.

svnge.asa라는 해킹프로그램은 상당히 정교하고 지능적으로 만들어져 있었는데, 웹 브라우져를 통해 이 프로그램에 접속시 패스워드 입력을 요구하여, 패스워드를 알고 있는 공격자만이 해당 프로그램을 사용할 수 있도록 하였다.



패스워드 없이 해당 프로그램을 실행하거나 패스워드가 틀릴 경우 피해시스템의 메인 화면으로 리다이렉션되도록 설정되어 있었다.

해킹 프로그램에 정상적으로 패스워드를 입력하고 로그인한 후의 화면은 다음과 같다.



해당 프로그램의 UI(사용자 인터페이스)는 중국어로 되어 있으며, 주요 기능은 다음과 같다.

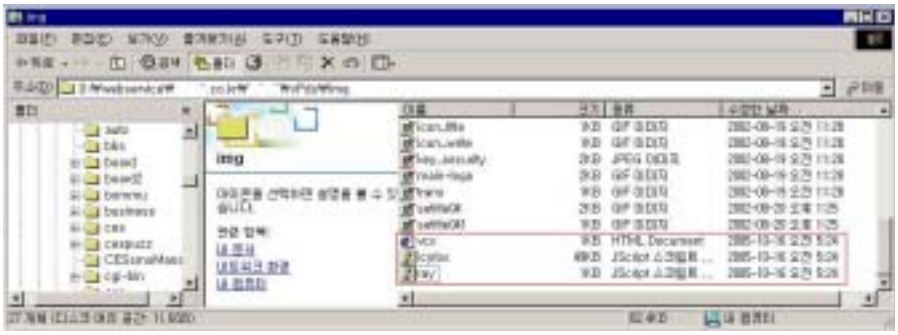
- 시스템내의 파일 및 폴더의 편집, 삭제, 복사, 이동
- 파일 업로드(추가 해킹관련 프로그램 설치 가능)
- 쉘(Shell)을 통해 임의의 명령 실행 가능
- DB 생성 및 임의의 SQL 명령 입력

로그파일에 남은 흔적에서 중국 IP 블록에서 8월 1일 이후 10월까지 지속적으로 svnge.asa 해킹 프로그램을 통해 피해 시스템에 침입한 것이 관찰되었다.

□ 일반 PC 사용자 감염을 위한 악성코드 삽입

피해시스템에는 해당 홈페이지를 방문한 일반 PC 사용자들을 감염시키기 위한 악성코드(vcx.htm, ray.js, icyfox.js)들이 설치되어 있었다.

vcx.htm 파일은 ray.js라는 이름의 자바스크립트를 실행시키고, 이 파일은 다시 icyfox.js 파일을 실행시키도록 되어 있었다. icyfox.js는 Encoding된 형태였으며, 웹 접속한 일반 PC를 감염시키는 역할을 한다.



다수의 웹사이트들이 중간 경유지로 이용당해 본 시스템과 같이 실제 사용자들을 감염시키는 악성코드 유포사이트로 접속하도록 유도한다. 본 피해 사이트에 설치된 vcx.htm, ray.js, icyfox.js는 홈페이지를 방문한 사용자 PC가 적절한 보안패치가 이루어져 있지 않을 경우 게임관련 아이디, 패스워드를 유출할 수 있는 악성 프로그램(트로이목마)을 설치하도록 한다.

피해시스템 로그에는 공격자가 설치한 vcx.htm에 접속했던 다수의 사용자를 발견할 수 있었다.

2005-10-15 20:29:15 xxx.78.122.60 - victim_IP 80 GET /xxx/xpds/img/vcx.htm - 200 Microsoft+URL+Control+-+6.01.9782
2005-10-15 20:48:59 xxx.212.180.144 - victim_IP 80 GET /xxx/xpds/img/vcx.htm - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1)
2005-10-15 21:28:23 xxx.51.100.192 - victim_IP 80 GET /xxx/xpds/img/vcx.htm - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0)
2005-10-15 21:49:22 xxx.154.195.111 - victim_IP 80 GET /xxx/xpds/img/vcx.htm - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1)
2005-10-15 22:07:15 xxx.145.199.99 - victim_IP 80 GET /xxx/xpds/img/vcx.htm - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1)
2005-10-15 22:09:34 xxx.138.246.51 - victim_IP 80 GET /xxx/xpds/img/vcx.htm - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.4322)
2005-10-15 22:36:48 xxx.40.120.99 - victim_IP 80 GET /xxx/xpds/img/vcx.htm - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1)
2005-10-15 22:42:16 xxx.114.182.18 - victim_IP 80 GET /xxx/xpds/img/vcx.htm - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1)
2005-10-15 22:50:54 xxx.226.99.6 - victim_IP 80 GET /xxx/xpds/img/vcx.htm - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1)
...

웹로그의 시간이 실제 시스템 시간에 비해 9시간 늦은 것을 감안할 때 vcx.htm 파일이 생성된 10월 16일 오전 5시경 이후 바로 사용자들이 해당 페이지를 방문한 것을 볼 수 있다. 다수개의 악성코드 경유지 사이트에서 본 시스템의 vcx.htm 파일에 접속하도록 한 것을 추측할 수 있다.

또한, 해당 페이지는 앞서 svnge.asa 해킹 프로그램을 이용하여 업로드 한 것으로 추정된다. 다음 로그는 vcx.htm, ray.js, icyfox.js 등 3개의 파일이 생성된 시간대에 svnge.asa 프로그램을 이용하여 파일을 3차례 업로드 한 흔적이다.

2005-10-15 20:23:29 xxx.173.161.60 - victim_IP 80 GET /xxx/xpds/data/svnge.asa Action=UpFile 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1)
2005-10-15 20:24:18 xxx.173.161.60 - victim_IP 80 POST /xxx/xpds/data/svnge.asa Action=UpFile&Action2=Post 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1)
2005-10-15 20:24:19 xxx.173.161.60 - victim_IP 80 GET /xxx/xpds/data/svnge.asa Action=UpFile 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1)
2005-10-15 20:24:31 xxx.173.161.60 - victim_IP 80 POST /xxx/xpds/data/svnge.asa Action=UpFile&Action2=Post 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1)
2005-10-15 20:24:33 xxx.173.161.60 - victim_IP 80 GET /xxx/xpds/data/svnge.asa Action=UpFile 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1)

2005-10-15 20:24:39 xxx.173.161.60 - victim_IP 80 POST /xxx/xpds/data/svnge.asa Action=UpFile&Action2=Post 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1)
2005-10-15 20:24:40 xxx.173.161.60 - victim_IP 80 POST /xxx/xpds/data/svnge.asa - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1)

□ 일반 PC 사용자 감염 가능성

피해시스템에 설치된 vcx.htm에 접속할 경우 PC 보안패치가 되어 있지 않으면 트로이목마 프로그램이 설치될 수 있다.

vcx.htm 파일이 생성된 10월 16일 오전 5시경부터 사고분석을 진행한 10월 17일 15시경 동안 해당 파일에 접속한 사용자 PC는 총 1,217명으로 추정된다. 이 추정치는 웹로그에서 vcx.htm에 접속한 unique IP로 산출한 수치이다. 1,217명 중 자신의 PC가 보안패치되지 않았을 경우 트로이목마에 감염되었을 것이다. 불과 34시간정도의 짧은 기간동안 1천여명 이상 해당 페이지를 방문하여, 만일 해당 파일이 삭제되지 않고 방치되었을 경우 수많은 인터넷 사용자들이 트로이 목마 감염 위협에 놓였을 것이다.

3. 보안 대책

최근 중국에 할당된 IP 블록으로부터 공격받은 국내 피해 웹사이트들은 SQL Injection 뿐만 아니라 본 사고와 같이 파일 업로드 취약점을 이용하여 공격을 당한 경우도 종종 찾아 볼 수 있다. 따라서, 홈페이지 관리자들은 다음과 같이 업로드 취약점에 대한 대책 마련이 필요하다.

업로드 취약점을 막기위해서는 첨부 파일 업로드 기능을 통한 스크립트 업로드 및 실행을 금지시켜야만 한다.

게시판 첨부파일 업로드, 사진 업로드 모듈 등 사용자가 임의의 파일을 서버로 전송할 수 있는 기능을 이용해서 공격자가 작성한 악의적인 스크립트를 서버에 업로드 한 후, 이를 실행시킬 수 있다면 해당 서버는 물론 해당 Application Server와 신뢰관계를 맺고 있는 서버들(예, Web DB서버, 내부 연동서버 등)이 공격당할 수 있는 가능성이 있다. 본 취약점은 게시판 업로드 모듈뿐 아니라 그림 파일을 올리는 기능을 통해서도 발견되고 있기 때문에, 사용자가 파일을 업로드 할 수 있는 모든 모듈에 적용된다.

o 첨부파일의 확장자 필터링 처리
사용자가 첨부파일의 업로드 시도 시, 업로드되는 파일의 확장자를 검토하여 적합한 파일인지를 검사하는 루틴을 삽입하여, 적합한 파일의 확장자 이외의 파일에 대해서는 업로드 되지 않도록 함

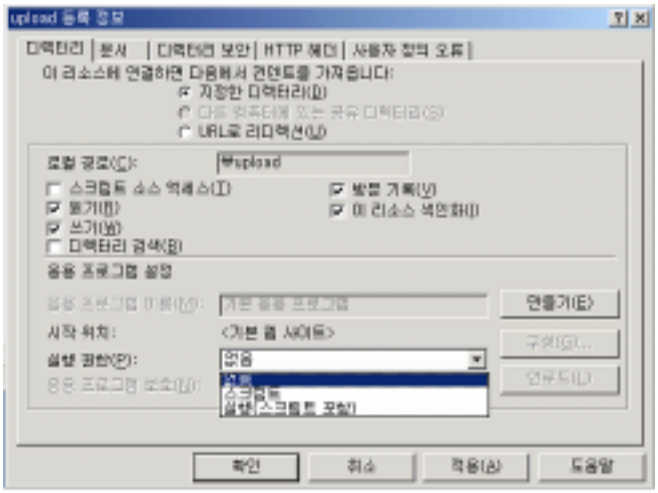
o 업로드 파일을 위한 디렉토리의 실행설정 제거
업로드 파일을 위한 전용 디렉토리를 별도 생성하여 웹 서버 설정파일에서 실행 설정을 제거

함으로써, Server Side Script가 업로드되더라도 웹 엔진이 실행하지 않게 환경을 설정함

업로드 된 디렉토리에서 실행 권한을 제거하는 방법은 임시적이기는 하지만 소스 코드의 수정 없이 간단히 수행 될 수 있다. IIS 웹서버에서는 다음의 절차를 통해 설정할 수 있다.

[설정]→[제어판]→[관리도구]→[인터넷 서비스 관리자] 선택

해당 업로드 폴더에 오른쪽 버튼을 클릭을 하고 등록정보→디렉토리→실행권한을 "없음"으로 설정



또한, 게시판 등 웹 프로그램 개발시 다음 사항들을 고려하여 개발한다.

o 첨부 파일에 대한 검사는 반드시 Server Side Script에서 구현해야 한다.

o 첨부파일을 체크하여 특정 종류의 파일들만 첨부 가능하도록 하고 첨부 파일을 처리하는 파일 업로드 프로그램(php, php3, cgi, html, jsp 등)에서 모든 실행 가능한 파일은 첨부할 수 없도록 한다.

o 프로그램에서 필터링을 할 경우 단순히 파일이름 기준으로 점검하지 말고 확장자 명에 대하여 검사하되 대소문자를 모두 검사하도록 한다.

o 너무 작거나 큰 파일을 처리하는 로직을 포함해야 하고, 임시 디렉토리에서 업로드 된 파일을 지우거나 다른 곳으로 이동시켜야 한다.

o 웹 서버 엔진 설정 시 업로드 된 디렉토리의 Server Side Script 언어의 실행 권한을 제거하고 업로드 된 파일이름을 임의로 변경하여 저장하는 것도 안전한 방법이다.

4. 결론

본 사고분석 사례는 실제 사용자 PC를 감염시킬 수 있는 악성코드가 삽입되어 있는 웹 사이트에 대해 분석을 실시하였으며, 웹 환경에서 일반 PC 사용자들의 보안 위협을 실감할 수 있었다. 이번 사고 사례를 통해 다음과 같은 몇 가지 사항에 주목할 필요가 있을 것 같다.

첫째, 악성코드 유포사이트 및 경유지 사이트에 대한 모니터링 강화가 절실하다.

본 피해 분석 시스템에서 불과 34시간정도의 짧은 시간동안 1천여명 이상이 공격자가 만들어 놓은 특정 웹 페이지를 방문하였다. 1천여명의 사용자 PC 중 보안패치가 되지 않은 상당수의 PC가 감염되었을 것으로 추정된다.

더욱 심각한 문제는 본 사례에서 분석한 악성코드 유포 사이트나 경유지 사이트들이 수백개에 달해 이들 웹 사이트를 방치할 경우 인터넷 이용자들에게 엄청난 보안위협이 될 수 있다.

따라서, 악성코드를 실제 유포하거나 유포사이트로 접속을 유도하는 경유지 사이트에 대한 신속한 검색 및 관련 코드에 대한 삭제가 중요할 것으로 생각된다.

한국정보보호진흥원 인터넷침해사고대응지원센터에서는 이들 악성코드 유포사이트나 경유지 사이트에 대한 자동화된 모니터링을 실시하고 있으며, 일반 웹서버 관리자들도 주기적인 로그 검사 및 시스템 분석을 통해 악성코드 유포에 악용되고 있는지 점검할 필요가 있을 것이다. 또한, 일반 PC 사용자들은 최신 보안패치를 항상 유지하여 악성코드 감염을 방지하여야 한다.

둘째, 웹서버 관리자들은 다양한 홈페이지 취약점에 대한 점검 및 제거가 필요하다.

지금까지 중국에 할당된 IP 블록으로 부터의 공격이 주로 SQL Injection 취약점을 이용하였지만 이번 사고와 같이 파일 업로드 취약점 등 다양한 취약점을 이용하여 공격하고 있는 것을 확인할 수 있었다. 특히, 최근 웹 피해 사이트에서 파일 업로드 취약점을 이용한 공격이 종종 발견되고 있다. 따라서, 파일업로드 취약점, SQL Injection 취약점, XSS 관련 취약점 등 홈페이지 개발 과정에서 발생될 수 있는 다양한 취약점을 제거할 필요가 있다. 지난 4월에 개발한 「홈페이지 개발 보안 가이드」에 홈페이지 개발시 발생될 수 있는 다양한 취약점에 대한 설명과 보완방법을 소개하고 있으므로 이를 참조하여 홈페이지 점검 및 보안대책 마련이 필요하다.

o 홈페이지 개발 보안 가이드 다운로드 :
http://www.kisa.or.kr/news/2005/announce_20050427_submit.html

최근 웹서버 해킹은 단순히 홈페이지 변조 수준에서 그치지 않고, 게임 비밀번호 유출과 같이 특정 목적을 달성하기 위해 해킹을 하는 사례가 늘고 있다. 이번 사고의 경우도 이미 8월부터 중국에 할당된 IP로부터 해킹을 당해 백도어가 생성된 후 동일한 공격자가 10월까지 수시로 침입하여 사용자 PC를 감염시켜 게임 관련 정보를 빼내기 위해 피해 시스템을 사용하였다. 대부분 게임 관련 정보를 유출하기 위해 이러한 해킹이 이루어지고 있지만, 개인의 금융정보나 기업의 산업정보 또는 국가의 기밀정보도 같은 방법으로 유출가능할 것으로 보여진다.

이처럼 해킹의 목적이 범죄화 됨에 따라 해킹 수법도 갈수록 지능화되어 가고 있으므로 홈페이지 관리자들의 홈페이지 보안관리와 일반 PC 사용자들의 보안패치에 각별히 신경을 써야 할 것이다.