디렉토리 리스팅 취약점을 이용한 게임 DB서버 해킹사고

2006. 8. 3

KrCERT/CC 인터넷침해사고대응지원센터

KISA 한국정보보호진흥원 Korea Information Security Agency

1. 개 요

중국 발 해킹의 표적이 온라인 게임서버에까지 이어지고 있다. 특히 중국에는 현재 수많은 게임 작업장이 있으며, 이곳에서는 많은 중국인들이 단순히 게임을 즐기는 것이 아니라 아이템 매매로 인한 금전적인 이득을 목적으로 한 범죄행위를 하고 있다.

최근 정보보호진흥원에 게임서버 해킹신고 건에 대한 게임사 서버 관리자를 통해 피해신고내용을 파악한 결과, 다음과 같았다.

. 6월말, 7월 초부터 바이러스나 백도어가 많이 탐지됨.
. 게임 서버가 계속 다운되거나 원격제어관리 프로그램(VNC)이 삭제
. 누군가 서버로 들어와서 명령어를 실행시키는 것을 목격
. 20여개 계정의 사이버머니가 급속하게 증가

이번 게임서버 해킹 피해사례를 통하여 그 원인을 파악해보고 대비책을 정리하였다.

2. 피해 시스템

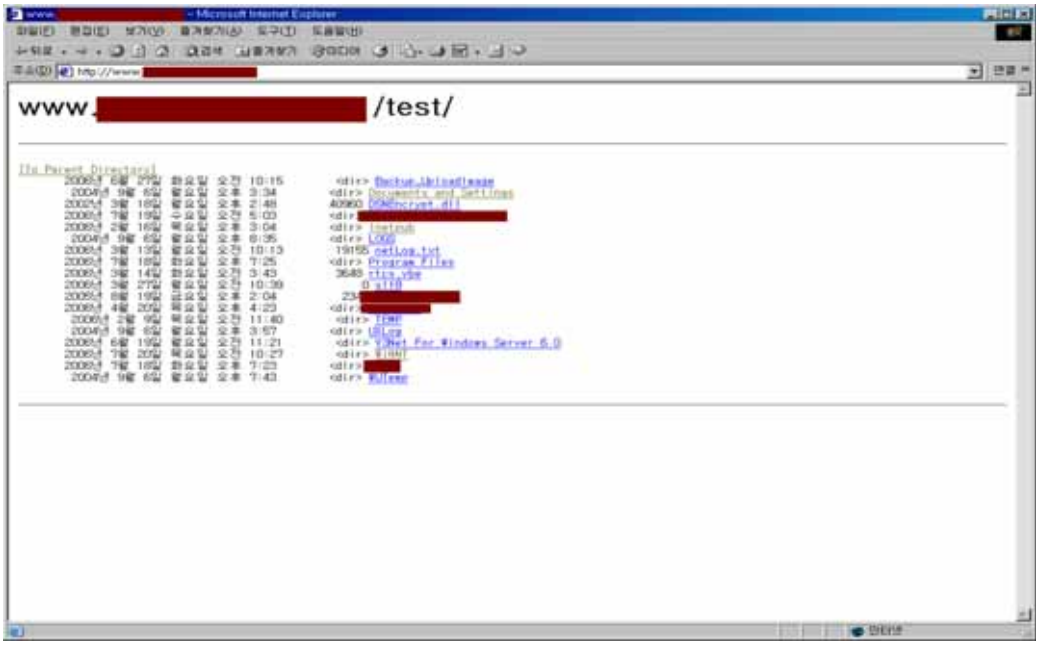
o 용 도 : 게임 서버, 웹서버, DB서버
o 운영체제 : Windows 2003 Server/SP1 또는 Windows 2000 Server/SP4

3. 시스템 패해 분석

각각의 게임 서버와 웹 서버에는 원격제어관리 프로그램인 RealVNC를 설치하여 접근 제어정책 없이 운영되고 있었으며, 웹 서버에는 존재하는 디렉토리 리스팅 취약점이 존재하였으며, 해커는 이를 악용하여 게임서버와 DB서버에 접속 가능한 계정 및 패스워드 정보를 획득한 것으로 확인되었다.

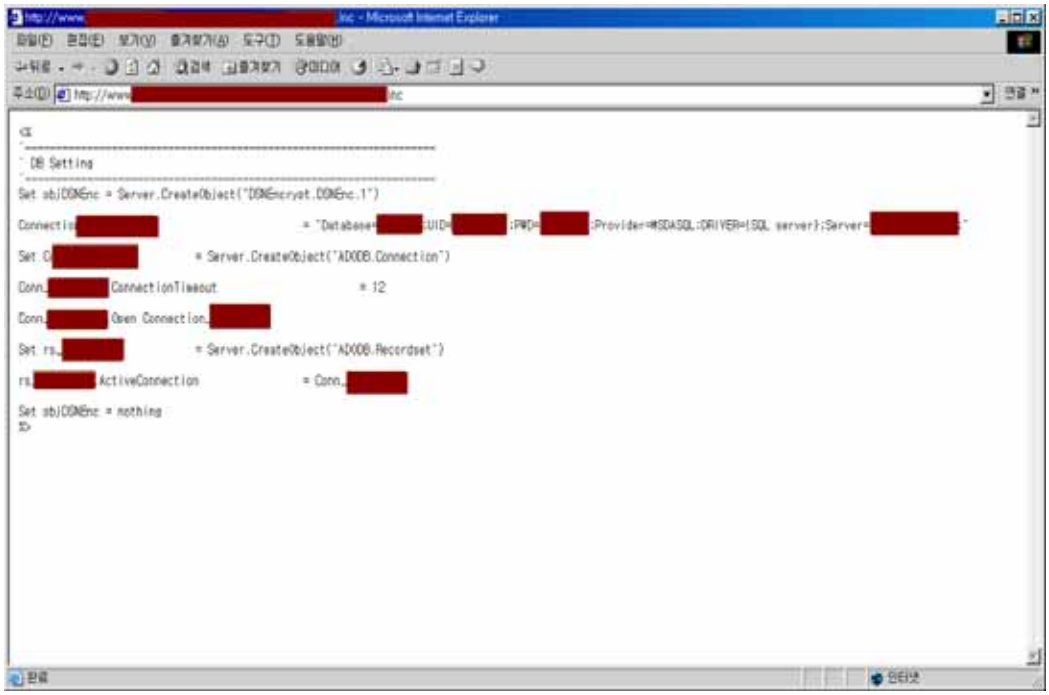
1) 웹 서버 내 디렉토리 리스팅 취약점 존재

웹 서버의 공개된 취약점을 분석한 결과, 디렉토리 리스팅 취약점이 존재하였으며, 웹사이트 의 TEST폴더 아래에 DB.INC, DB_XXXXX.inc 파일 내에 게임 및 DB 서버 IP, 웹 및 DB 접속계정과 패스워드가 고스란히 노출되어 있었다.

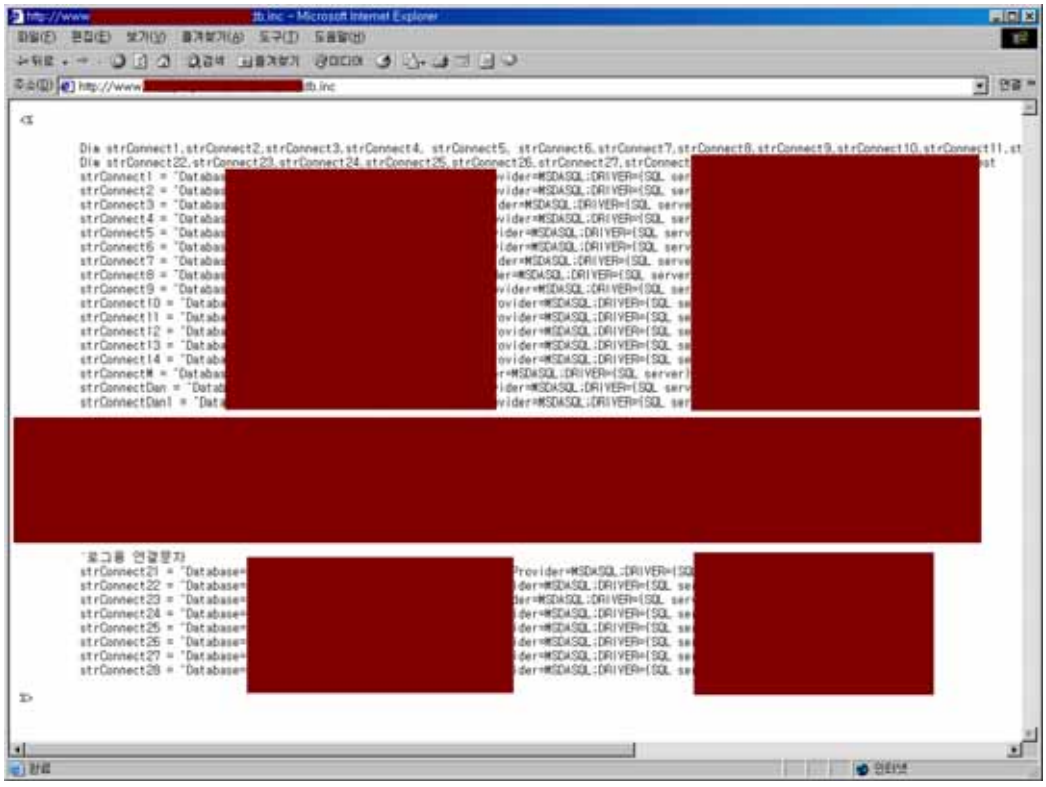


(그림 1) 디렉토리 리스팅 취약점 존재 웹페이지 화면

다음은 DB 환경설정 파일과 접속할 서버와 계정 및 패스워드 내역이다.



(그림 2) 웹에 노출된 DB 환경 설정파일

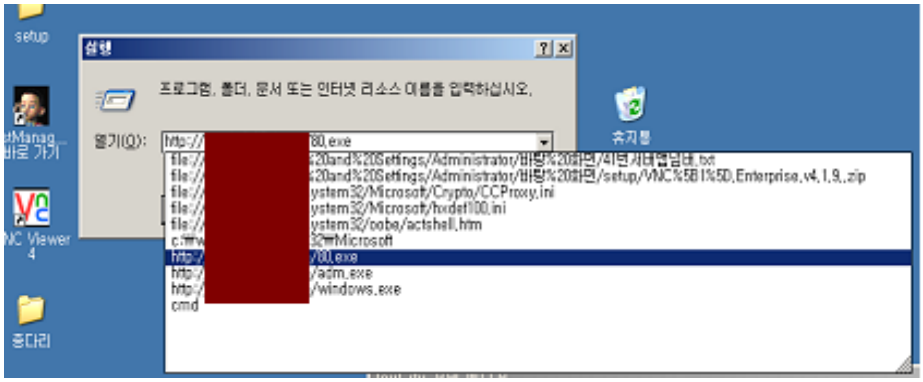


(그림 3) 웹에 노출된 게임 서버, 계정, 패스워드 정보

2) 게임서버 침입 후 행위

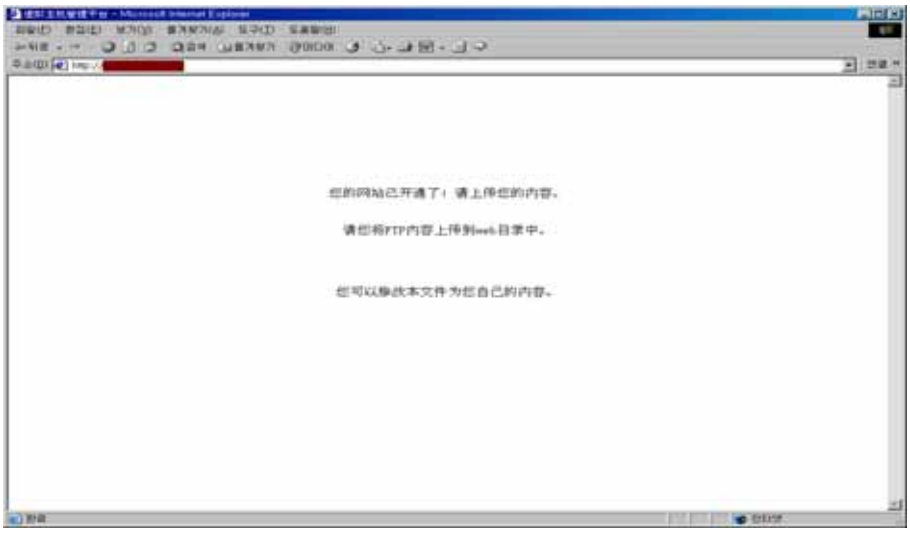
게임 서버 내에는 원격제어 프로그램인 RealVNC를 설치하여 운영하고 있었지만 해킹당한 사실을 인지하기 전까지는 접근 제어정책 없이 운영하고 있다가 최근 최신 버전으로 설치 후 접근제어정책을 적용하였다. 이것으로 미루어보아 해커가 인증우회 취약점을 이용하여 게임서버에 침입한 것으로 추정되었다.

해커는 게임서버를 침입한 후 중국 사이트에서 '80.exe', 'adm.exe', 'windows.exe' 파일을 다운로드 받았다. 위 파일들은 모두 실행 압축되어 있었으며, 압축을 해제한 결과 'Hackerdefender100'라는 루트킷과 'Radmin' 원격제어관리 프로그램, 우회 접속용 PROXY 프로그램(CCProxy)들로 확인되었다.



(그림 4) 최근 실행한 명령어 확인

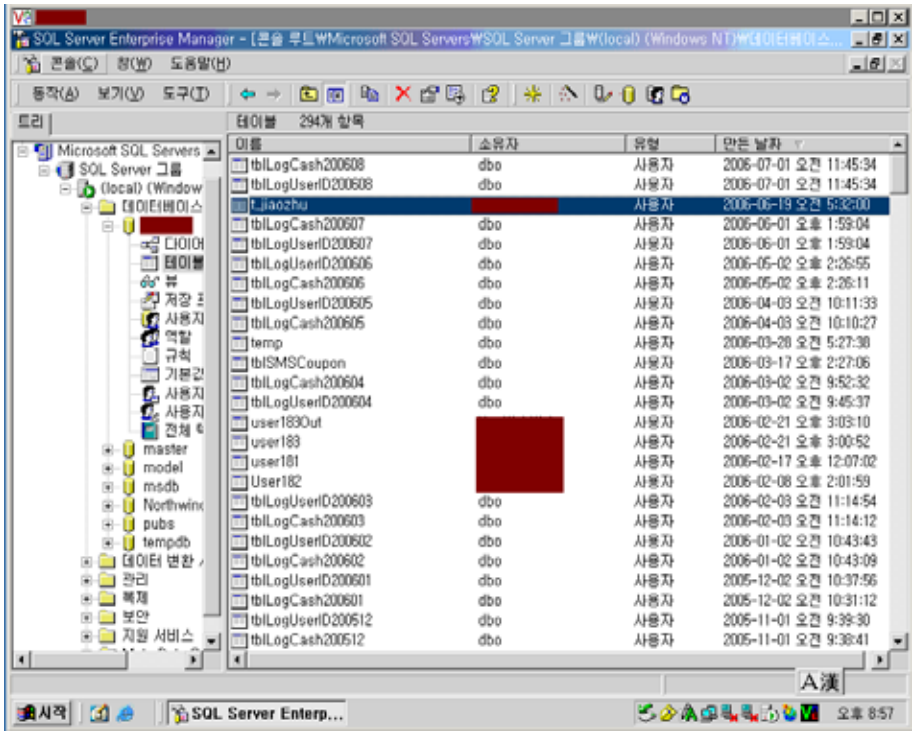
다음은 해커가 서버에 침입 후 접속하여 해킹 툴을 다운로드 받았던 중국 사이트의 홈페이지이다.



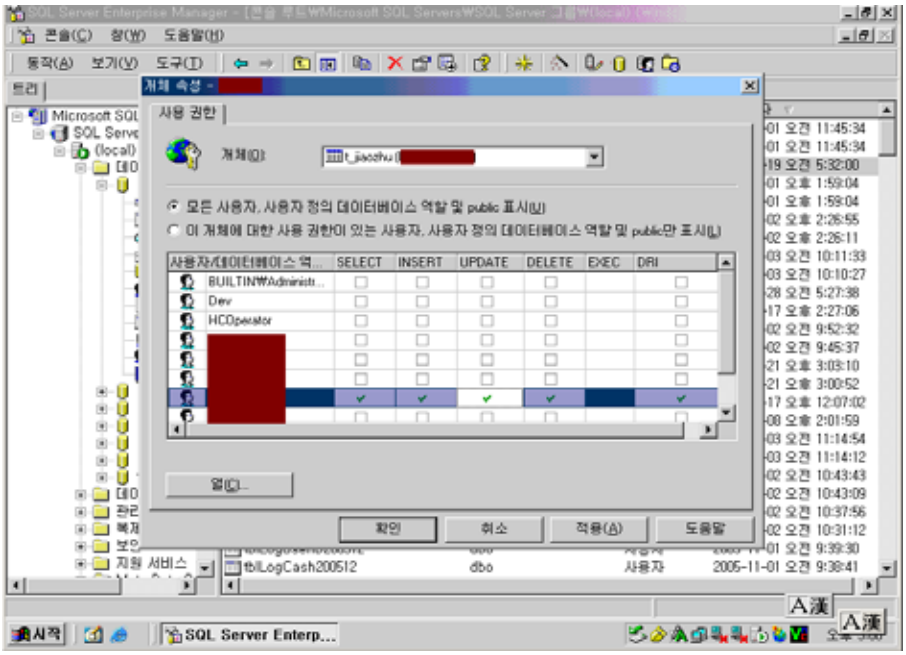
(그림 5) 중국 사이트 홈페이지

3) 게임 DB 서버 분석

외부의 게임이나 웹 서버 IP에서 DB 접속 계정과 패스워드를 알면 내부에 있는 DB 서버에 접속이 가능하였다. 계정과 패스워드는 웹 디렉토리 리스팅 취약점을 악용하여 쉽게 획득이 가능하였으리라 생각된다. 게임 DB 서버 테이블 중 ‘t_jiaozhu’ 라는 이름의 테이블이 2006-6-19 오전 5:32 경에 생성되어 있었으며, 테이블 명으로 추측하건데 중국 해커의 의한 것으로 보여 진다.



(그림 6) DB내 't_jiaozhu' 라는 테이블이 생성된 화면



(그림 7) DB 내 't_jiaozhu'의 테이블 속성

4) 게임 플레잉 로그분석 결과

또한, 사이버머니가 급속하게 증가된 20여개 불법 계정의 게임 접속 로그를 분석한 결과, 모두 중국 IP로 확인되었다.

[표 1] 불법 계정의 게임 접속 내역

UserId	Password	Logintime	IPaddress
467XXX	XXX	2006-07-07 오전 12:47:27	218.62.XXX.XXX
467XXX	XXX	2006-07-07 오전 1:32:41	218.62.XXX.XXX
49XXX	XXX	2006-07-06 오후 7:21:07	219.148.XXX.XXX
100XXX5	XXX	2006-07-06 오후 11:34:53	219.148.XXX.XXX
100XXX5	XXX	2006-07-06 오후 11:35:32	219.148.XXX.XXX
cdpXXX0	XXX	2006-07-10 오후 6:49:36	219.148.XXX.XXX
cdrXXX1	XXX	2006-07-10 오후 6:59:50	219.148.XXX.XXX
cdsXXX3	XXX	2006-07-10 오후 7:00:28	219.148.XXX.XXX
cds3XXX알	XXX	2006-07-10 오후 7:01:39	219.148.XXX.XXX
helXXX9	XXX	2006-07-10 오후 7:02:20	219.148.XXX.XXX
helXXX6	XXX	2006-07-10 오후 7:03:54	219.148.XXX.XXX
helXXX26	XXX	2006-07-10 오후 7:05:02	219.148.XXX.XXX
helXXX41	XXX	2006-07-10 오후 7:05:55	219.148.XXX.XXX
cdXXXp	XXX	2006-07-10 오후 7:07:12	219.148.XXX.XXX
cdXXX	XXX	2006-07-10 오후 7:07:53	219.148.XXX.XXX
cecXXX86	XXX	2006-07-10 오후 7:09:21	219.148.XXX.XXX
ceXXX38	XXX	2006-07-10 오후 7:09:47	219.148.XXX.XXX
dXXX	XXX	2006-07-13 오후 1:17:55	222.217.XXX.XXX

4. 결론 및 보안대책

해킹 시 관리자 계정과 패스워드를 알기위해서는 스니퍼나 키로깅 프로그램, 패스워드 크래킹 툴을 사용하면 되지만, 이번 사례에서 해커는 웹서버 내에 존재하였던 디렉토리 리스팅 취약점을 이용하여 손쉽게 계정정보를 알 수 있었을 것이다. 이 정보를 악용하여 게임 서버와 관련 DB 서버에 접속하여 비정상적인 테이블을 만들어진 것을 확인하였다.

이와 같이 서버 해킹에 대한 재발방지를 위해서는 시스템에 존재하고 있는 취약점을 제거하여야 하며, 아래와 같은 대비책들이 필요하다.

o 게임 서버와 웹서버에는 원격접속관리프로그램인 RealVNC을 사용하고 있었지만 접근제한 없이 사용하고 있어 누구나 서버에 접근할 수 있는 위험이 있었다. 이에 서버에 원격접속 가능한 IP대역 또는 IP만을 미리 지정하는 접근제어 정책을 사용하고 관련 프로그램에 대한 보안 취약점을 최신 패치 후 사용하도록 한다.

※ 다운로드 URL
- http://www.realvnc.com/upgrade.html

o 홈페이지의 속성을 설정하는 '웹사이트 등록정보'에 특정 디렉토리에 대하여 '디렉토리' 검색항목이 체크되어있으면 인터넷 사용자에게 모든 디렉토리 및 파일 목록이 보여지게 되고, 파일의 열람 및 저장도 가능하게 되어 DB 설정관련 자료가 유출되었다. 이에 웹 서버에 존재하는 디렉토리 리스팅 취약점을 다음과 같이 제거한다.

- 제어판 → 관리도구 → 인터넷서비스관리자 혹은 인터넷 정보 서비스 메뉴에서 기본 웹 사이트의 마우스 오른 쪽 클릭, '속성' 부분에서 '기본 웹사이트 등록정보' 확인한다.
- '기본 웹 사이트 등록정보'에서 '홈 디렉토리' 부분을 클릭하면 '디렉토리 검색(B)'이란 옵션 체크를 해지 후 적용버튼을 누른다.

o 네트워크 단에 침입차단시스템(F/W)이나 침입탐지시스템(IDS)을 설치하여 허가되지 않은 IP와 비정상적인 공격에 대응할 수 있도록 한다.

o 또한, 인터넷에 노출된 서버 관리자 및 DB 접속 계정에 대한 주기적으로 변경하는 것이 필요하다.