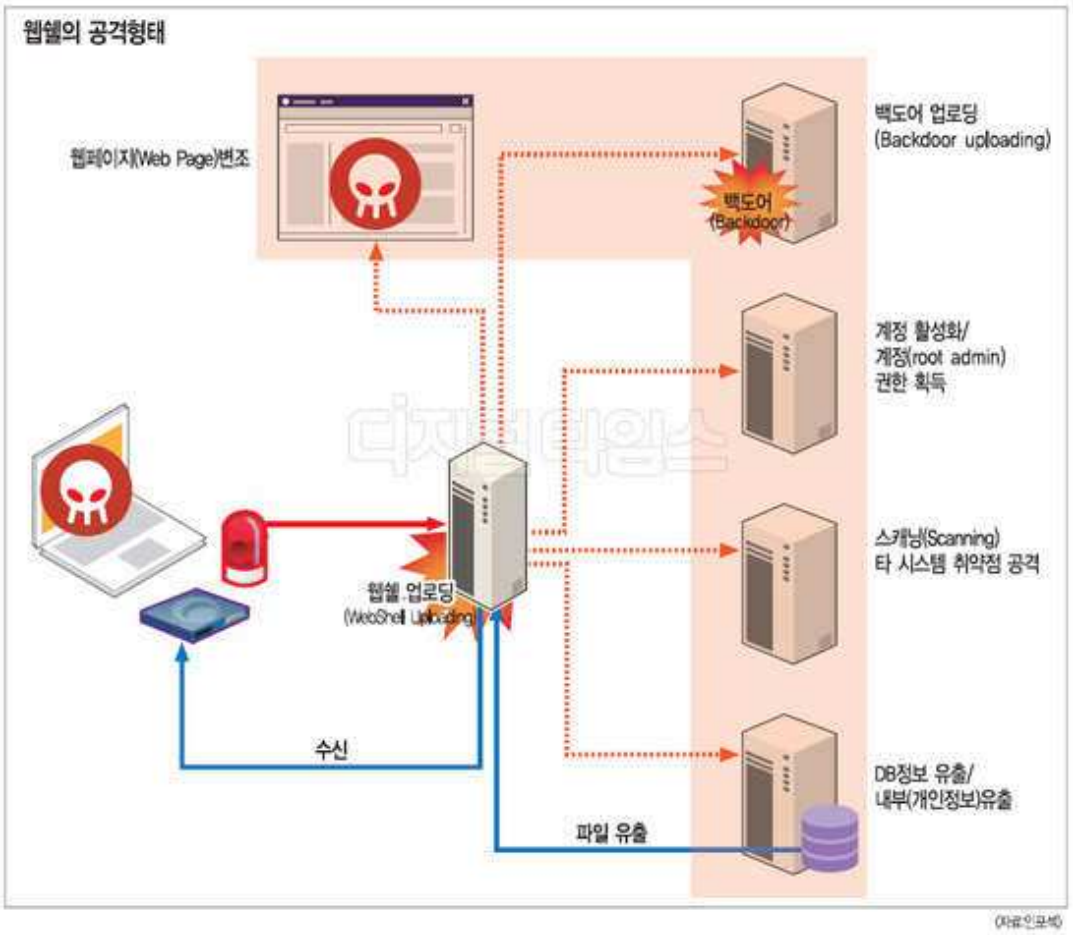
무심코 연 첨부파일, 해킹에 `속수무책`

스크립트 파일 악용 개인정보 유출 등 사이버공격 기승

강은성 기자 esther@dt.co.kr | 입력: 2014-06-10 18:58
[2014 년 06 월 11 일자 18 면 기사]



일반적으로 웹 게시판이나 자료실에는 사진이나 문서를 올리는 `파일 첨부' 기능이 포함돼 있습니다. 이때 txt, jpg, doc 와 같은 데이터 파일종류 이외에 악의적으로 제작된 스크립트 파일인 `웹쉘(Web- Shell)'을 업로드 해 사이버 공격을 하는 사고가 빈번히 발생합니다.

웹쉘이란 공격자가 원격에서 대상 웹서버에 명령을 수행할 수 있도록 작성한 웹 스크립트(asp, jsp, php, cgi) 파일을 말합니다. zip, jpg, doc 와 같은 데이터 파일종류 이외에 악의적으로 제작된 스크립트 파일인 웹쉘을 정상파일처럼 숨겨 업로드 해 웹 서버를 해킹하는 것이지요. 최근에는 파일 업로드뿐만 아니라 SQL 탈취(Injection)와 같은 웹 취약점을 공격한 후 지속적으로 피해시스템을 관리할 목적으로 웹쉘을 생성해 업로드하는 고도의 해킹도 발생하고 있습니다.

웹쉘은 서버 명령을 실행할 수 있는 asp, cgi, php, jsp 등과 같은 명령어 코드로 구성되기 때문에 해커가 웹 서버에 명령을 실행해 관리자 권한을 획득한 후

웹페이지 소스 코드 열람, 서버내 자료 유출, 백도어 프로그램 설치 등 각종 공격을 자행하기도 합니다.

공격자는 웹쉘을 대상 서버에 업로드한 후 웹을 이용해 시스템 명령어를 수행하므로 네트워크 방화벽의 영향을 받지 않고 서버를 제어할 수 있습니다.

최근 웹쉘은 단순한 쉘 권한 실행 뿐만 아니라 DB 조작 등을 포함하고 있으며 탐지를 어렵게 하기 위해 웹쉘의 아주 일부분만을 피해시스템에 업로드 하는 등 그 유형이 갈수록 교묘해지는 상황입니다. 이를 탐지해 방어하는 시스템을 우회하려고 웹쉘의 일부분만을 피해시스템에 업로드 하는 등 변종도 기승을 부리고 있습니다.

한국인터넷진흥원 인터넷침해사고대응지원센터에서 한 해 동안 분석했던 사이버공격 피해 웹서버 중 웹쉘이 발견된 웹서버는 총 91%에 달하기도 했습니다. 이것은 공격자들이 취약점을 공격한 후 웹쉘을 업로드해 시스템을 통제하기가 수월하다보니 해커가 웹쉘을 주요 공격수단으로 사용하고 있다는 점을 의미합니다.

웹 취약점을 통해 피해시스템에 접근한 공격자는 방화벽에서 접근을 허용하는 HTTP(80/tcp) 서비스를 통해 피해시스템을 제어하므로 웹쉘을 차단하기가 쉽지 않다는 것이 전문가들의 의견입니다.

인터넷진흥원 측은 "피해시스템에서 수집된 ASP 웹쉘 샘플을 바이러스 백신 엔진으로 탐지해내는지 확인해봤더니 웹셀의 악성활동을 탐지하지 못하고 있었다"면서 "공격자들은 스크립트 웹쉘을 빈번히 변경시켜 사용하기 때문에 백신이 이를 탐지하는 것은 쉽지 않다"고 설명합니다.

또한 일반적인 서버관리자들은 해킹여부를 확인하기 힘들고 피해를 인지하더라도 관리자들이 주로 사용하는 백신 프로그램에서 웹쉘 탐지가 안 되므로 웹쉘을 찾기가 쉽지 않습니다. 관리자들이 해킹 피해를 인지하고 시스템을 재설치 하더라도 이전에 웹쉘이 업로드 되어 있는 소스 그대로 새롭게 설치한 시스템에 복사해 사용하기 때문에 지속적으로 웹쉘을 관리하는 공격자에게 피해를 입게 되는 것입니다.

그렇다면 이같은 웹쉘 공격은 어떻게 하면 막을 수 있을까요. 먼저 홈페이지 파일 업로드 취약점을 제거해야 합니다. 굳이 파일 업로드를 해야할 이유가 없는 게시판의 경우는 업로드의 기능을 완전히 제거하고 필요한 경우에는 파일의 확장자를 체크해야 합니다. 웹쉘 업로드를 제한하는 asp, cgi, php, jsp 등의 확장자를 막는 방법으로 구현하기보다는 허용하는 확장자 즉 txt, hwp, doc, pdf, gif 등의 업로드 가능한 파일 확장자만 올릴 수 있도록 체크하는 것이 바람직합니다. 특정 확장자만 막는 경우에는 우회해서 올릴 수 있는 방법들이 존재하기 때문입니다.

파일 업로드 폴더의 실행을 제한하는 것도 방법입니다. 웹서버의 파일 업로드 전용 폴더를 만들고 전용 폴더의 스크립트 파일 실행을 제한해 해당 폴더 내에 있는 파일이 실행되지 않도록 해야하는 것이지요.

SQL 인젝션을 방지하는 것도 웹쉘 공격을 막을 수 있는 방편이 됩니다. 웹쉘 공격은 파일 업로드 취약점뿐만 아니라 SQL 인젝션을 이용해서도 가능하므로 DB

쿼리와 관련된 특수 문자들을 걸러내 사용자의 입력 값에 포함돼 있을 경우 에러를 발생시켜 악의적인 쿼리가 실행되지 않도록 방지해야 합니다

최근 각 백신 업체나 전문 솔루션 업체들이 웹쉘 탐지가 가능한 전문제품을 잇달아 출시하고 있습니다. 윤광택 시만텍 이사는 "최근에는 웹셀의 공격을 차단하기 위해 이메일이나 파일 업로드가 되기 전 악성코드 유무를 미리 알아내 웹셀의 시스템 접근을 막는 방어기법이 사용되고 있다"고 설명했습니다.

강은성기자 esther@