KINEWS
Korea IT & Industry News

'국방융합기술.hwp' 파일...열지 마세요

안랩, "알려진 한글 취약점 악용한 악성코드 발견"

임지민 기자 승인 2012.06.27

안랩 보안대응센터(ASEC)는 지난 15일에 이어 27일 또다시 한글과컴퓨터에서 개발한 한글 소프트웨어에 존재하는 코드 실행 취약점을 악용한 악성코드 유포 사례가 발견됐다며 주의를 당부했다.

안랩은 "현재 해당 코드 실행 취약점에 대해서는 지난 22일 한컴이 공개한 보안 패치로 원천 차단이 가능하다."며 "해당 보안 패치를 설치해 악성코드 감염을 근본적으로 차단할 것"을 조언했다.

국내 특정 조직들을 대상으로 발송된 이메일의 첨부 파일 형태로 유포된 이 '한글파일'은 HncTextArt_hplg에 존재하는 스택(Stack)의 경계를 체크하지 않아 발생하는 버퍼 오버플로우(Buffer Overflow) 취약점이며, 해당 취약점은 2010년부터 지속적으로 악용돼 왔던 한글 소프트웨어 취약점들 중 하나다.

해당 취약점이 존재하는 한글 소프트웨어를 사용하는 시스템에서 금일 유포된 취약한 한글 파일을 열게 되면 사용자 계정의 임시 폴더에 scvhost.exe (138,752 바이트) 파일을 생성하게 된다.

c:\documents and settings\[사용자 계정명]\local settings\temp\scvhost.exe (138,752 바이트)

생성된 scvhost.exe (138,752 바이트) 파일이 실행되면 윈도 폴더(c:\windows)에 wdmaud.drv (78,848 바이트)와 wdmaud.dat (78,848 바이트)를 생성하게 된다.

wdmaud.dat (78,848 바이트)는 인코딩되어 있는 파일로 해당 파일을 디코딩하게 되면 실행 가능한 PE 파일이 wdmaud.drv (78,848 바이트)이 생성된다.

wdmaud.dat (78,848 바이트)의 디코딩 작업이 완료되어 wdmaud.drv (78,848 바이트)가 생성되면 해당 scvhost.exe (138,752 바이트)에 의해 해당 파일은 삭제된다.

그리고 생성된 wdmaud.drv (78,848 바이트)는 감염된 시스템에서 ▲하드웨어 정보 ▲윈도 운영체제 정보 ▲로그인 사용자 정보 ▲파일 업로드 및 다운로드 ▲감염된 시스템의 IP 주소 및 프록시(Proxy) 서버 주소 등의 정보들을 수집해 외부로 전송을 시도하게 되나, 분석 당시에는 정상적으로 접속이 되지 않았다고 안랩은 밝혔다.

임지민 기자 Ijm@ittoday.co.kr

인쇄하기