디지털타임스 뉴스인쇄

기사 주소: http://www.dt.co.kr/contents.html?article_no=2010012702010960739007

"국가·공공기관 대상 해킹 메일 알고보니… "

강진규 기자 kjk@dt.co.kr | 입력: 2010-01-26 21:02

어도비 리더 취약점 악용한 것

국가정보원 국가사이버안전센터가 지난 25일 저녁 `관심' 단계로 사이버위협 수준을 높인 후 경고한 국가·공공기관 대상 해킹메일이 어도비 리더와 PDF 취약점을 악용한 것으로 분석됐다. 1월 26일자 2면 참조

국정원은 26일 이번 해킹 메일이 주요 상용메일 포털사이트의 웹 서비스 취약점 중 하나인 크로스 사이트 스크립팅(XSS) 취약점과 지난해 12월 16일 발표된 어도비 리더와 애크로뱃 관련 보안 취약점을 악용한 것이라고 밝혔다.

국정원은 이 해킹 메일을 분석한 결과 클릭 시 로그인 화면이 표시되는데 동시에 아이디와 비밀번호 입력여부와 상관없이 iFrame 태그 등을 이용해 은밀히 악성 PDF파일을 다운로드하고 실행시켜 해당 PC에 자료를 유출하는 악성코드를 설치한다고 설명했다.

이에 따라 국정원은 어도비 PDF 리더 등이 설치된 PC는 최신 보안 패치를 설치해야 하며 PDF를 자동으로 열람하는 기능을 정지해 악성 PDF파일의 활동을 막아야 한다고 지적했다.

또 메일 수신시 익명으로 가입이 가능한 해외 메일계정으로 송신된 메일은 열람 시 주의하고 메일 열람 중 로그인 화면이 표시될 경우 전산담당자 등 보안 전문가들에게 신고할 것을 당부했다.

한편 방송통신위원회, 한국인터넷진흥원(KISA) 등과 보안업체들은 민간부문에서는 이와 관련된 피해가 보고되지 않았다고 밝혔다. 하지만 보안 전문가들은 이번 사건과 유사한 응용 소프트웨어(SW)의 취약점을 노린 해킹과 악성코드들이 나타날 수 있는 만큼 사용자들이 항상 보안 패치를 최신으로 유지하고 실시간으로 보안 SW를 사용할 것을 권고했다.

강진규기자 kjk@

출력시간: 2017-04-18 18:22:18