IT839로 u-KOREA 실현

정보통신부 보도자료

정책홍보관리실(750-2810)
www.mic.go.kr

정보통신부 mic

2006. 1. 5.(목)배포
문의 / 정보통신기반대응팀장 김동철팀장(750-1810) 연장길 사무관 (750-1811) jkyeon@mic.go.kr

수상한 사이트 · 이메일 · 메신저 사용 조심 !

- 정통부 사이버위협 모니터링 강화 -

정보통신부와 한국정보보호진흥원은 아직까지 공식 보안패치가 배포되지 않은 윈도우 이미지(WMF)관련 취약점을 이용한 악성코드가 국내·외에서 지속적으로 발견됨에 따라 컴퓨터 이용자 및 보안관리자들을 대상으로 주의를 당부했다.

※ WMF(Window Metafile) : 윈도우에서 사용되는 그래픽 파일로서 MS 오피스의 클립아트 등에 사용

특히 마이크로소프트사에서는 해당 악성코드 감염을 예방할 수 있는 정식 보안패치를 다음 주 수요일인 1월 11일(미국 현지 1월10일)에 배포할 예정이어서 컴퓨터 사용자들의 각별한 주의가 요구된다.

이번에 유포되고 있는 악성코드는 특정사이트 접속 시 해당 사이트를 통해 유포되거나, 이메일 또는 메신저 등의 첨부파일을 통해 전파되고 있으며, 감염되는 경우 공격자가 해당 컴퓨터의 사용자 권한을 획득하여 새로운 해킹 도구를 설치하거나, 키보드 입력정보 획득 등의 명령을 실행할 수 있어 다양한 피해가 발생 할 수 있다.

※ 해당 악성코드로는 Troj_WMFCRASH(win-trojan/Exploit-WMF, Trojan.WIN32.WMF-Exploit) Troj_NASCENE 등이 있으며 변종도 10여종 발견되고 있음

일반 컴퓨터 사용자의 경우 악성코드에 감염되는 것을 예방하기 위해서는 **불필요한 사이트의 접속을 피하고, 이미지 파일이 첨부된 수상한 메일이나 메신저는 내용을 읽지 말고 바로 삭제해야 하며, 백신 프로그램을 업데이트하여 사용하는 것이 바람직**하다.

그리고 무엇보다도 금번에 발견된 WMF취약점을 악용한 악성코드로부터 피해를 근본적으로 차단하기 위해서는 **1월11일(미국 현지 1월10일) 마이크로소프트사에서 배포(예정)하는 보안패치를 반드시 설치해야만** 한다.

또한 국내 일부사이트를 통해 악성코드가 유포가 발견됨에 따라 기업의 웹서버 관리자들은 해당 서버의 구성설정 및 패치현황 등 보안사항을 재점검하여 해당 웹사이트가 악성코드 유포사이트로 악용되지 않도록 각별히 주의해야 한다.

현재까지 국내에 직접적인 피해가 확인된 바는 없으나 국내·외 일부 사이트를 통해 해당 악성코드가 유포되는 것이 발견되어 한국정보보호진흥원은 ISP 등 사업자와 공동으로 관련 사이트 차단 및 복구조치를 취한 바 있으며, 국내·외 정보보호 관련기관과 협조하여 인터넷 위협 모니터링을 강화하고 있다.

금번 취약점 및 악성코드에 대한 더 **자세한 내용은 인터넷침해사고대응지원센터(전화 : 국번없이 118 , www.krcert.or.kr)나 보호나라(www.boho.or.kr)에서 확인**할 수 있다. 끝.