<붙임>

ActiveX 취약점 악용 방지 가이드

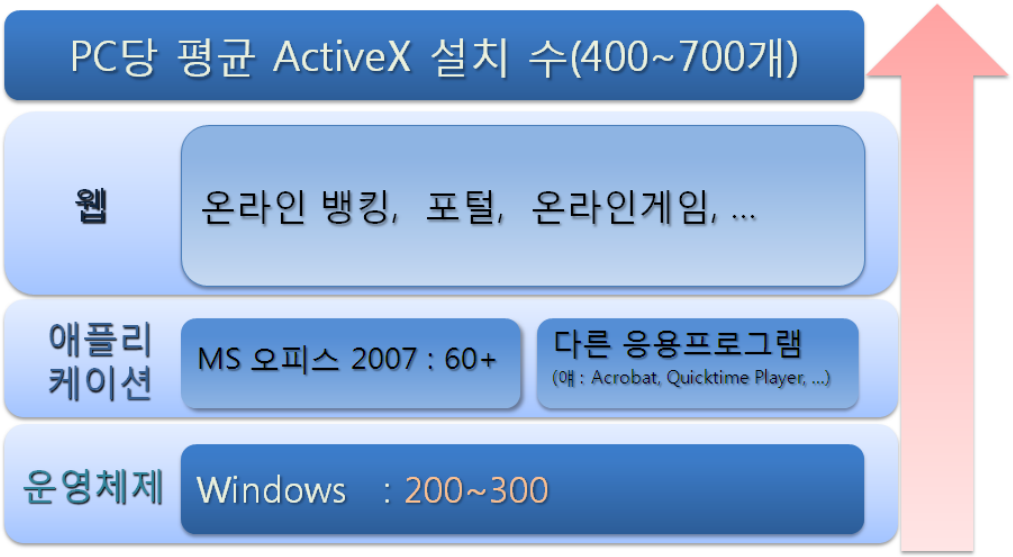
최근 ActiveX 취약점이 DDoS 공격용 좀비PC를 양산하는데 악용될 가능성이 있으니 본 가이드 활용, 적극 대처하시기 바랍니다.

Ⅰ. ActiveX 사용 현황

○ ActiveX는 텍스트와 그림으로만 구성된 웹문서를 멀티미디어 문서로 작성할 수 있게 하는 기술로 온라인 뱅킹·쇼핑몰 등 웹사이트에서 사용자 인증 등 다양한 목적으로 활용됩니다.

○ MS社 운영체제를 사용하는 PC에는 기본적으로 200~300개 ActiveX가 설치되고, 웹·애플리케이션을 위한 ActiveX 등을 포함하여 평균 400~700개 정도가 설치되어 있습니다.

○ 또한 ActiveX를 이용한 온라인 뱅킹 가입자가 6천만명(복수가입)이 넘어 ActiveX 취약점을 악용한 해킹 발생 가능성이 매우 높습니다.



Ⅱ. ActiveX 보안 위협

○ ActiveX는 관리자 권한으로 동작하기 때문에 ActiveX가 악용될 경우 파일 및 레지스트리를 읽기, 쓰기뿐만 아니라 실행도 가능합니다.

○ ActiveX 보안 위협은 사용중인 ActiveX의 취약점을 악용하는 경우와 악성코드가 있는 ActiveX를 고의적으로 유포하는 경우입니다.

√ 사용중인 ActiveX 취약점은 개발시 보안을 고려하지 않아 발생하는 것으로 웹플러그인 취약점의 80~90%를 차지합니다.

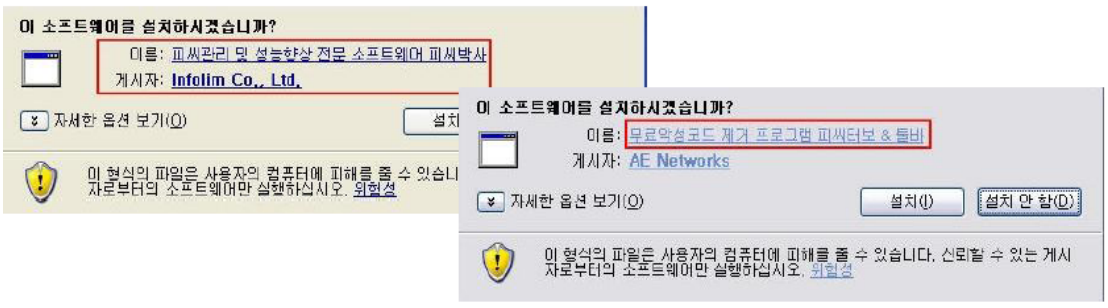
[ActiveX 취약점 종류]

취약점	심각성	설 명
파일/레지스트리 읽기	Medium	PC 파일 및 레지스트리 정보 유출
파일/레지스트리 쓰기	Critical	파일 및 레지스트리에 악성행위 코드 삽입
자동업데이트	Critical	자동업데이트시 서버로부터 악성 파일을 다운로드
프로세스 실행 취약점	Critical	프로세스 생성 후 악성행위 수행
버퍼오버플로우	Critical	긴 문자열에 의한 버퍼오버플로우 발생

√ 악성코드가 있는 ActiveX는 다음과 같습니다.

❶ ActiveX 형태로 유포되는 악성코드는 Rogueware, Backdoor /Trojan, Spyware, Adware 등입니다.

❷ 악성 ActiveX는 정상적인 절차로 위장하여 설치를 유도합니다.



Ⅲ. ActiveX 취약점 악용 방법

○ 온라인 뱅킹·게임·쇼핑몰, 전자정부(G4C) 등 접속자 수가 많은 홈페이지에서 사용하는 ActiveX 취약점을 악용할 경우에는 순식간에 좀비 PC 양산이 가능합니다.

○ 다음은 ActiveX 취약점을 악용하는 과정입니다.

Ⅳ. ActiveX 취약점 대처 방안

주체	대처 방법
개발자	국가사이버안전센터(NCSC) 홈페이지(www.ncsc.go.kr)에 게시된 보안권고문(228번) 'ActiveX 개발 보안가이드라인' 활용하여 개발
사용자	☞ 윈도우 보안업데이트 실시 ☞ PC 사용자 권한 최소화 ☞ 신뢰하는 사이트에서 배포하는 ActiveX만 설치 ☞ 서명된 ActiveX만 설치 ☞ 음란물 및 게임, 카페, 개인 블로그, 무료백신, 툴바 등 사이트에서 제공하는 ActiveX는 설치 금지 ☞ NCSC 홈페이지에 게시된 보안권고문(237번)의 ActiveX 삭제 도구(CleanAX)를 활용, 사용하지 않는 ActiveX 삭제

[사용자 대처 방법]

첫째, MS사에서 윈도우 보안업데이트를 발표되었을 시 즉시 적용한다.

둘째, PC를 최소의 권한으로 사용한다. 즉, ActiveX 취약점으로부터 자신의 PC를 보호하는 방법 중 하나는 권한이 없는 일반 사용자 계정으로 인터넷을 하는 것이다. 일반 사용자 계정을 생성하는 방법은 윈도우 제어판 선택 → 사용자계정 선택 → 사용자 추가 순이다. 이때 '제한된 계정'을 선택하도록 한다.

셋째, 신뢰할 수 있는 웹사이트에서 제공하는 ActiveX만 설치한다. 신뢰할 수 있는 웹사이트는 다음으로 확인할 수 있다.

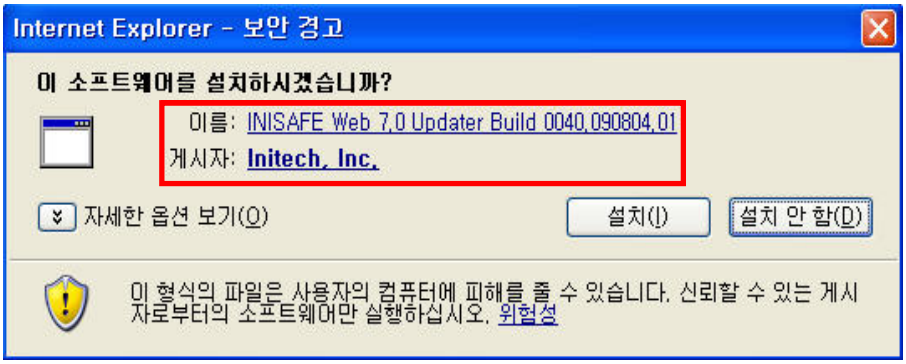
❶ BBBonline, TRUSTe 또는 WebTrust 등 개인정보 보호인증 로고 표시가 있는지 확인한다.

❷ 평소 신뢰하는 기관이나 업체인지 확인한다.

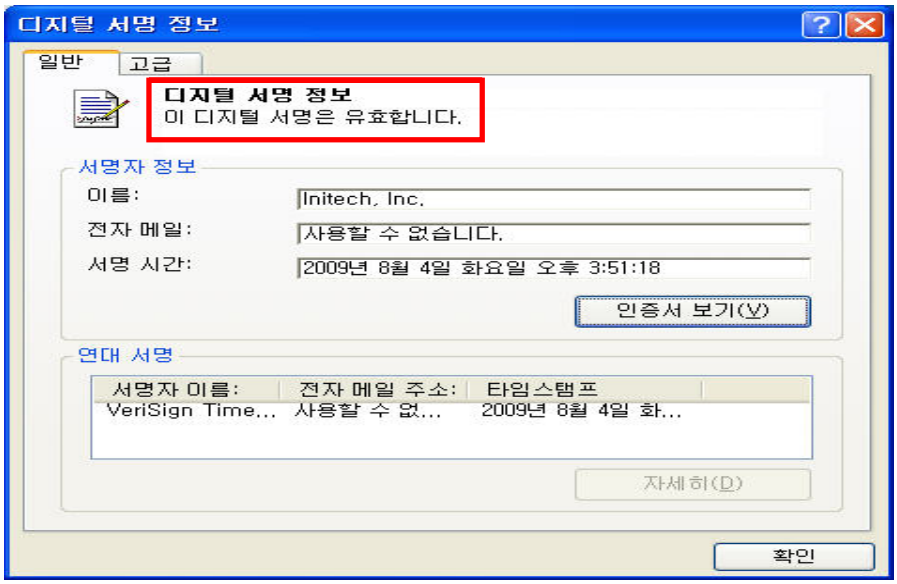
❸ 쇼핑몰 사이트인 경우 구입물품 반환정책이 있는지 확인한다.

❹ 주민번호, 신용카드번호, 은행정보 등 중요정보 요청시 암호화된다는 문구가 있는지 확인한다.

❺ 신뢰할 수 있는 ActiveX 확인 방법은 다음과 같다.

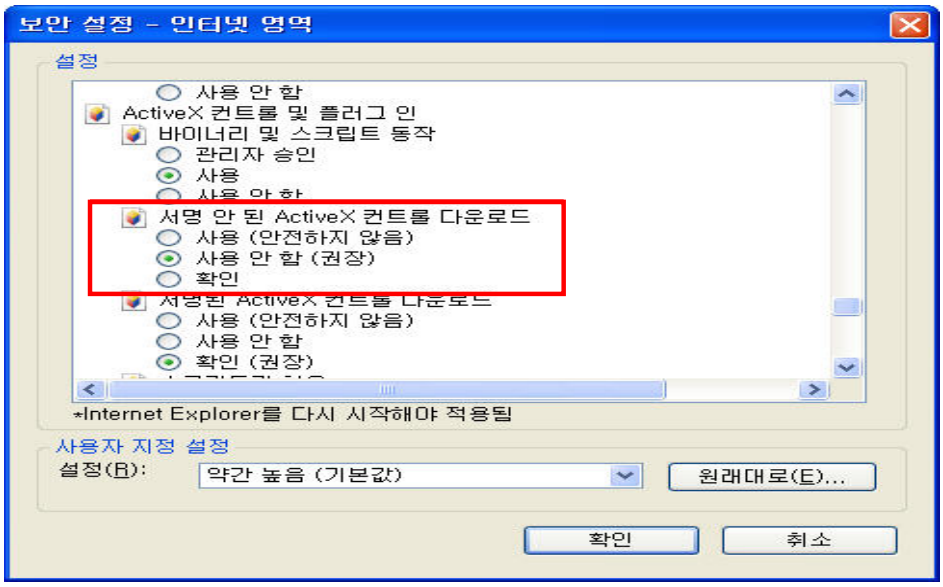


※ 이름/게시자 부분을 선택하여 신뢰할 수 있는지 확인



※ 디지털서명정보 존재 및 인증서 유효기간 확인

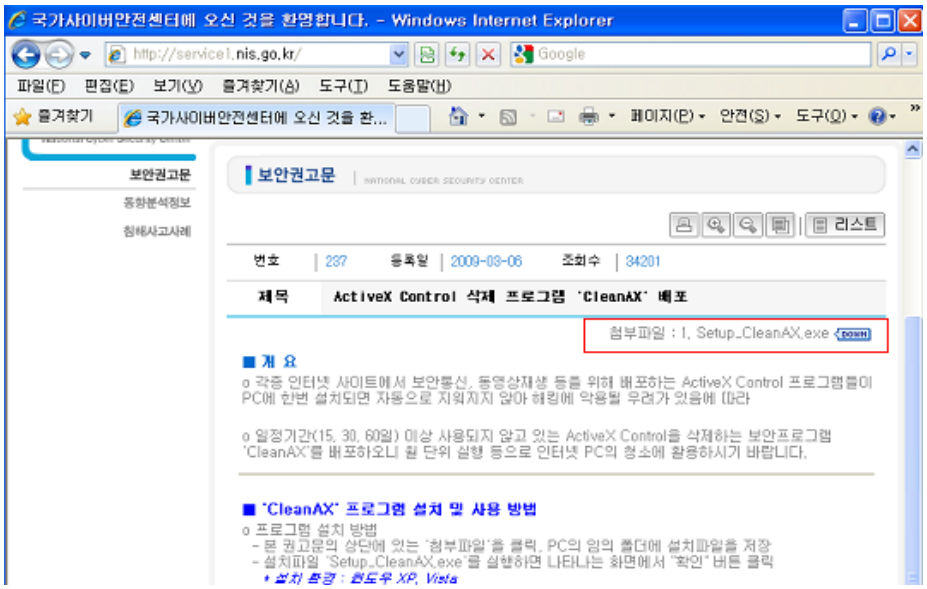
넷째, 윈도우 메뉴에서 도구 선택 → 인터넷 옵션 선택 → 보안 선택하여 ActiveX 보안설정 조건을 조정할 수 있다.



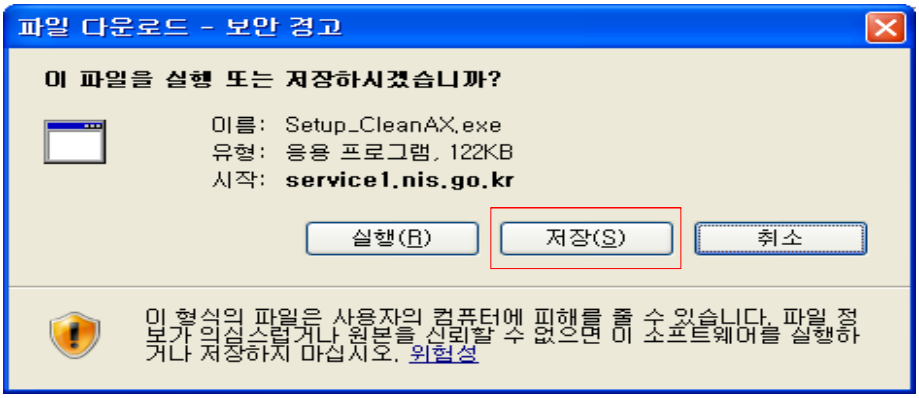
[ActiveX 삭제도구인 CleanAX 설치 및 활용법]

① NCSC 홈페이지(www.ncsc.go.kr) 접속한 후 센터자료실 선택

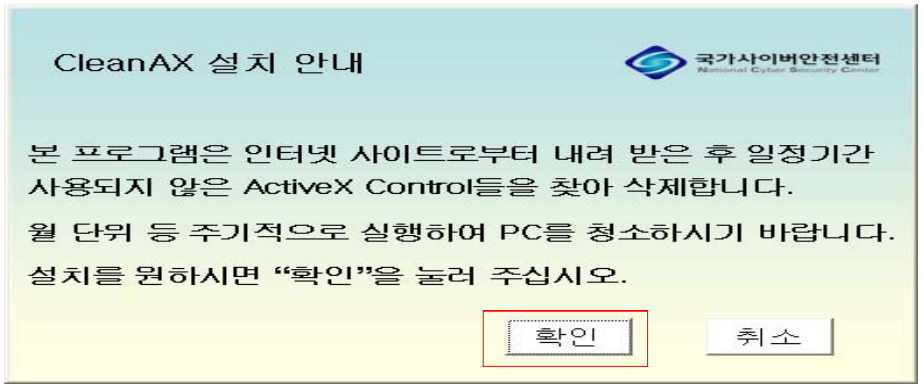
② 보안권고문 237번 선택→ setup.CleanAXexe 선태프로그램



③ 첨부파일을 바탕화면에 저장



④ 바탕화면에 저장된 첨부파일 실행



⑤ 프로그램실행 화면

⑥ ActiveX 선택하여 삭제

Ⅴ. 맺는 말

○ MS사의 인터넷 익스플로러(IE)를 기반에서 동작하는 ActiveX는 다양한 기능을 제공하지만 취약점으로 인해 웜/바이러스 유포 및 악성코드 설치 등에 악용되고 있습니다.

○ 그러나 ActiveX에 대한 취약점을 분석하기에는 고도의 전문성이 요구되기 때문에 일반 사용자들은 그 취약점 유무를 쉽게 확인할 수가 없습니다.

○ 이에, 본 가이드를 활용하여 사용하고 있는 PC가 좀비되지 않도록 CleanAX 도구를 이용하여 주기적으로 사용하지 않는 ActiveX를 삭제하여 주시기 바랍니다. 끝.