OUCH! | 2014 년 12월호

컴퓨터 사용자를 위한 월간 정보보호 인식 뉴스레터

OUCH!

이달 호 주제..

- 개요
- 안티바이러스 동작 방법
- 안티바이러스 팁

안티바이러스란 무엇인가?

개요

안티바이러스는 컴퓨터나 모바일 기기 등이 악성코드에 감염되는 것을 방지하기 위한 보안 프로그램이다. "악성코드"라는 용어는 바이러스, 웜, 트로이목마, 스파이웨어와 같은 악의적인 소프트웨어를 통칭하는 단어이다. 사실 악성코드라는 용어는 '악성'과 '코드(프로그램)' 단어를 합친 합성이다. 만약에 컴퓨터가 악성코드에 감염이 되면, 사이버공격자는 키보드 입력 값을 모두 캡쳐하고, 문서를 훔치고, 다른 사람을 공격할 때 그 컴퓨터를 사용할 수 있다. 일부 사람들이 생각하는 것과 달리 맥 OS X 및 리눅스 등 모든 운영체제가 악성코드에 감염될 수 있다.

객원 편집자

제이크 윌리엄스는 렌디션 인포섹(www.renditioninfosec.com) 설립자이며, SANS 공인강사 및 과정 저자이다. 제이크는 @MalwareJake 트위터에서 활동하고 있으며, malwarejake.blogspot.com 블로그를 운영하고 있다.

사람들은 독립적으로 안티바이러스 프로그램을 구매할 수도 있으며, 아니면 보안 패키지 안에 포함될 수도 있다. 문제는 안티바이러스는 사이버 공격자의 수준을 더 이상 따라갈 수 없다는 것이다. 사이버 공격자는 항상 새로운 종류의 악성코들 개발하고 있다. 안티바이러스 프로그램이 탐지할 수 없는 너무나 많은 새로운 악성코드가 매일 나오고 있다. 그래서 안티바이러스가 모든 종류의 악성코드를 탐지하고 방어하지는 못하지만, 이를 이용해서 컴퓨터를 보호하는 방법을 이해하는 것이 중요하다. 좀 더 잘 이해할 수 있도록, 대부분의 안티바이러스 프로그램이 동작하는 방법에 대해 살펴보자.

안티바이러스 동작 방법

일반적으로 안티바이러스가 악성코드를 식별하기 위해서는 시그너처 탐지와 행위 탐지 등 두 가지 방법이 있다. 시그너처 탐지는 사람의 면역시스템과 같이 동작한다. 즉 알려진 악성코드의 문자나 특징을 가지고 컴퓨터를 스캔한다. 이것은 알려진 악성코드 사전을 참고하는 것으로 컴퓨터에 어떤 것이 프로그램 사전과 일치하면 이것을 중성화 시킨다. 사람의 면역시스템과 같이 사전적 방법은 감기 주사와 같이 새로운 종류의 악성코드로부터 보호하기 위해 업데이트가 필요하다. 이러한 안티바이러스는 유해한 것으로 인식하고 있는 것만 보호할 수 있다. 문제는 사이버 공격자들이 너무 빨리 새로운 악성코드를 개발하고 있어 안티바이러스 개발회사들은 이를 따라갈 수 없다. 그 결과 안티바이러스를 업데이트 속도와 관계없이, 안티바이러스를 우회할 수 있는 새로운 악성코드 변종이 항상 존재한다.

안티바이러스란 무엇인가?

행위탐지 방법은 안티바이러스가 알려진 악성코드를 찾지 않고, 컴퓨터에 설치된 소프트웨어의 행위를 감시한다. 어떤 프로그램이 보호된 파일에 접근하고자 하거나 다른 프로그램을 수정하고자 하는 등의 의심스러운 행위가 있으면 행위기반의 안티바이러스는 의심스러운 활동을 찾아내고 경고문을 알린다. 이 방법은 사전에는 없는 새로운 행태의 악성코드에 대해서 보호할 수 있다. 이 방법의 문제점은 잘못된 경고를 생성할 수 있다는 것이다. 컴퓨터 사용자는 어떤 것을 허용하고 허용하지 말아야 할지 확신하지 못할 수 있으며, 그래서 경고가 자주 반복되면 이러한 경고에 무감각해 진다. 모든 경고를 "허용"할 수 있으며, 그래서 공격이나 감염될 수 있다. 또한 악성 행위가 탐지되면, 악성코드는 컴퓨터에 이미 실행되고 있었을 가능성이 크며, 안티바이러스가 탐지하기 전에는 악성코드가 전에 어떤 행위를 했는지 모른다는 것이다.

안티바이러스가 보안의 중요한 한 부분이지만, 모든 공격을 탐지하거나 차단할 수 없습니다. 최종적으로 기술이 아니라 사용자가 최선의 방어책입니다.

안티바이러스는 컴퓨터나 모바일 기기를 보호하는 중요한 부분이며, 가능하면 안티바이러스를 설치하고 사용할 것을 권고한다. 하지만 안티바이러스가 어떻게 동작을 하던 모든 종류의 악성코드로부터 보호할 수 없다는 점을 기억해야 한다. 최종적으로 기술이 아니라 사용자가 최근의 사이버 공격자들로부터 최고의 방어이다.

안티바이러스 팁

1. 유명하고 신뢰받는 회사의 안티바이러스 프로그램을 구매해야 한다. 일반적으로 사이버 공격자들이 악성코드가 포함된 가짜 안티바이러스 프로그램을 배포하고 있다.
2. 설치된 안티바이러스 제품은 최신의 버전으로 업데이트해야 한다. 즉 연간 유지보수 비용을 지불하고, 안티바이러스가 자동 업데이트하도록 설정해야 한다.
3. 안티바이러스가 USB와 같이 이동식 매체를 자동으로 스캔하도록 하고, 실시간 탐지 기능을 사용해야 한다.
4. 안티바이러스 가 생성하는 스크린에 뜨는 경고사항에 주의를 기울여야 한다.
5. 컴퓨터 속도가 느려지고, 웹사이트를 차단하고, 앱이나 프로그램을 설치하지 못하게 한다고 해서 안티바이러스 프로그램을 사용하지 않거나 삭제하면 안 된다. 안티바이러스를 사용하지 않으면 위험에 노출될 수 있으며, 심각한 보안사고가 발생할 수 있다. 만약에 회사의 컴퓨터에 문제가 계속 발생하면, 회사 지원부서로 연락하는 것이 좋다.

안티바이러스란 무엇인가?

만약에 개인용 컴퓨터에 문제가 계속 발생하면, 안티바이러스 개발회사로 연락하거나, 추가적인 정보를 얻기 위해 웹사이트에 방문하는 것이 좋다. 또는 다른 회사 제품으로 안티바이러스를 교체해야 한다.

6. 컴퓨터에 동시에 여러 개의 안티바이러스 프로그램을 설치하면 안 된다. 동시에 여러 개의 프로그램을 설치하는 경우, 충돌이 발생할 수 있으며 컴퓨터 보안성이 약화될 수 있다.
7. 안티바이러스 프로그램에서 나오는 경고문을 이해하도록 해야 한다. 사이버 공격자들은 악성 웹사이트를 구축하여 진짜와 같은 가짜 안티바이러스 경고문이 나오게 할 수 있다. 그리고 컴퓨터를 "수리"해야 한다고 제안한다. 이러한 웹사이트의 링크나 버튼을 클릭하면 컴퓨터가 감염될 수 있다.

자세히 알아 보기

http://www.securingthehuman.org를 방문해서 OUCH! 뉴스레터를 읽어 보시고, 월간 OUCH! 정보보호지식 뉴스레터를 구독하십시오. 그리고 SANS 정보보호지식 솔루션에 대해서 좀 더 알아보시기 바랍니다.

한글판

본 문서는 한국의 ITL(http://www.itlkorea.kr)에서 번역하였습니다. ITL 은 미국 SANS 연구소의 한국 파트너로서 IT 거버넌스 및 IT 보안 분야의 최신의 지식과, 양질의 교육과 세미나를 진행하는 교육기관입니다. 추가적인 사항은 itl@itlkorea.kr 로 문의해주시기 바랍니다.

참고자료

안티바이러스 제품 비교: http://www.av-test.org/en/
사회공학: http://www.securingthehuman.org/ouch/2014#november2014
이메일 피싱 공격: http://www.securingthehuman.org/ouch/2013#february2013
해킹당한 후 대응지침: http://www.securingthehuman.org/ouch/2014#may2014

편집위원회 : Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, 번역: 진수희(ITL Inc.)