전 국민대상 월간 정보보호 인식제고 뉴스레터

악성코드 차단

개요

사람들이 사이버보안에 관해 이야기 할 때, 바이러스, 트로이 목마, 랜섬웨어 또는 루트킷과 같은 용어에 대해 들어 봤을 것입니다. 이러한 것들은 사이버 범죄자가 컴퓨터 및 장비를 감염시키는 데 사용하는 다양한 악성 프로그램 즉 악성코드를 말합니다. 악성코드가 일단 설치되면, 범죄자들은 원하는 대로 할 수 있습니다. 이번 뉴스레터에서 악성코드가 무엇인지, 위험 요소가 무엇인지, 가장 중요한 우리 자신을 보호할 수 있는 방법을 알아보십시오.

악성코드란?

간단히 말해 악성코드는 컴퓨터 프로그램으로 악의적인 행위를 하는데 사용되는 소프트웨어입니다. 이 용어는 '악성'이라는 단어와 '프로그램(코드)'의 합성어입니다. 사이버 범죄자는 컴퓨터나 장비에 악성코드를 설치하여 해당 컴퓨터나 장비를 제어합니다. 이러한 악성코드가 설치되면, 범죄자가 이 악성코드를 통해 온라인 활동을 감시하거나 패스워드나 파일을 훔치거나, 감염된 시스템을 사용하여 다른 사람을 공격할 수 있습니다. 악성코드는 자신의 파일을 제어할 수도 있습니다. 몸 값을 지불해야 파일을 다시 가져올 수 있습니다. 많은 사람들은 악성코드가 윈도 컴퓨터에서만의 문제라고 생각합니다. 하지만 악성코드는 Mac 컴퓨터, 스마트폰, DVR 및 보안 카메라에 이르기까지 모든 장비를 감염시킬 수 있습니다. 사이버 범죄자가 컴퓨터와 장비를 더 많이 감염할수록 더 많은 돈을 벌 수 있습니다. 그러므로 우리 자신을 포함하여 모든 사람이 공격 대상이 됩니다.

보호조치 - 악성코드 차단

바이러스 백신 소프트웨어와 같은 보안 프로그램만 설치하면 감염되지 않고 안전하다고 생각할 수 있습니다. 하지만 안티 바이러스는 모든 악성코드를 차단할 수 없습니다. 사이버 범죄자는 탐지를 피할 수 있는 새롭고 보다 정교한 악성코드를 끊임없이 개발하고 있습니다. 반대로 바이러스 백신 공급 업체는 악성 프로그램을 탐지하는 새로운 기능으로 제품을 지속적으로 업데이트하고 있습니다. 여러 면에서 군비 경쟁과 같은 상황이 되고 있으며, 나쁜 사람들은 대개 한걸음 앞서 나가고 있습니다. 안티 바이러스만으로는 의존 할 수 없기 때문에 다음과 같은 방법으로 자신을 보호해야합니다:

사이버 범죄자는 소프트웨어의 취약점을 악용하여 컴퓨터나 장비를 감염시키는 경우가 많습니다. 소프트웨어가 최신 버전 일수록 시스템의 취약점이 줄어들고 사이버 범죄자가 시스템에 감염시키는 것이 어려워집니다. 운영 체제, 응용 프로그램, 브라우저 및 브라우저 플러그인 및 장비가 항상 최신 상태로 업데이트되었는지 확인하십시오. 이를 보장하는 가장 쉬운 방법은 가능하다면 자동 업데이트를 설정하여 사용하는 것입니다.

사이버 범죄자가 컴퓨터나 모바일 기기를 감염시키는 일반적인 방법은 가짜 컴퓨터 프로그램이나 모바일 응용 프로그램을 만들어 인터넷에 게시한 다음 다운로드하여 설치하는 것입니다. 신뢰할 수 있는 온라인 스토어에서만 프로그램이나 앱을 다운로드하여 설치하십시오. 또한 새롭고 긍정적인 리뷰가 거의 없고, 업데이트도 거의 되지 않았거나 소수의 사람들만 다운로드한 모바일 앱은 멀리 하셔야 합니다. 그리고 더 이상 컴퓨터 프로그램이나 모바일 앱을 사용하지 않는다면, 삭제하시기 바랍니다.

사이버 범죄자는 종종 사람을 속여 악성코드를 설치합니다. 예를 들어 합법적인 것처럼 보이는 첨부 파일이나 링크가 포함된 이메일을 보낼 수 있습니다. 이러한 이메일이 은행이나 친구에게서 온 것 같습니다. 그러나 첨부 된 파일을 열거나 링크를 클릭하면 시스템에 악성 코드를 설치하는 악성 코드가 활성화됩니다. 메시지 내용이 긴박하거나 사실이라고 생각하기에는 너무 좋아 보인다면, 그것은 공격 일 수 있습니다. 의심해보고, 상식적인 판단이 최선의 방어입니다.

시스템과 파일을 클라우드 기반 서비스에 정기적으로 백업하거나, 오프라인의 외부 저장매체와 같은 곳에 백업을 저장하십시오. 이렇게 하면 악성코드가 파일 암호화 또는 삭제를 시도할 경우에도 백업 데이터를 보호 할 수 있습니다. 백업은 매우 중요하며, 악성 코드 감염으로부터 복구할 수 있는 유일한 방법입니다.

궁극적으로 악성코드를 막을 수 있는 가장 좋은 방법은 가능한 모든 소프트웨어 및 장비를 최신 상태로 유지하고, 신뢰할 수 있는 바이러스 백신 소프트웨어를 설치하고, 우리 자신을 속여 시스템을 감염시키려는 사람에 대해서 의심해보고 경계하는 것입니다. 다른 모든 방법이 실패하면 정기적인 백업만이 데이터를 복구 할 수 있습니다.

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.

객원 편집자

레니 젤트서는 미네르바 연구소에서 엔드 포인트 보안 제품을 만들고 SANS 연구소에서 교육하여 악성코드와 싸우고 있습니다. 레니 젤트서는 트위터 @lennyzeltser에서 활동하고 있으며 zeltser.com 에 보안 블로그를 작성합니다.

참고자료

랜섬웨어: https://www.sans.org/u/EdI
백업: https://www.sans.org/u/EdN
피싱 차단: https://www.sans.org/u/EdS

 편집위원회: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | 번역: 진수희(ITL Inc.)