OUCH! | 2016 년 03 월호

컴퓨터 사용자를 위한 월간 정보보호 인식 뉴스레터

OUCH!

이달 호 주제..

- 악성코드란 무엇인가?
- 악성코드는 개발자
- 보호방안

악성코드란 무엇인가?

개요

아마 여러분들은 사이버 보안에 대해서 회의할 때 바이러스, 트로이목마, 랜섬웨어 또는 루트킷과 같은 용어를 들어보았을 것입니다. 이러한 용어는 동일한 것으로 컴퓨터 및 모바일 기기를 감염시키고 통제하기 위해 사이버 범죄자들이 사용하는 프로그램 종류입니다. 최근 이러한 다양한 용어들을 간단히 "악성코드"라고 부릅니다. 본 뉴스레터에서는, 악성코드가 무엇인지, 누가 왜 개발하는지 그리고 악성코드로부터 보호하기 위해 해야 할 일에 대해서 설명합니다.

객원 편집자

레니 젤트서는 NCR社에서 고객 IT 운영 보안을 담당하고 있으며, SANS 연구소에서 악성코드 분석에 대해서 강의합니다. 레니는 @lennyzeltser 트위터 및 blog.zeltser.com 보안 블로그를 운영하고 .있습니다.

악성코드는 무엇인가?

악성코드를 간단히 말하면, 악성 행위를 위해 개발된 컴퓨터 프로그램 즉 소프트웨어입니다. 사실 악성코드라는 용어는 악성과 소프트웨어의 합성어입니다. 사이버 범죄자들은 컴퓨터나 기기가 보유하고 있는 정보에 접근하고 제어하기 위해 컴퓨터나 모바일 기기에 악성코드를 설치합니다. 한 번 악성코드가 설치되면 공격자들은 악성코드를 이용해서 온라인 활동을 훔쳐보고, 패스워드나 파일을 훔치고, 다른 컴퓨터를 공격하는 데 사용합니다. 악성코드는 기기 소유자의 컴퓨터 파일에 접근하는 것을 차단할 수 있으며, 다시 접근 권한을 얻기 위해 몸 값을 지불하라는 요구도 합니다.

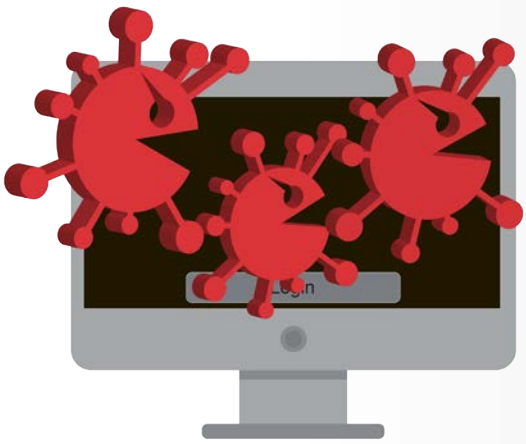
많은 사람들이 악성코드는 윈도우 컴퓨터에서만 가능한 것이라고 오해 하고 있습니다. 물론 윈도우가 가장 많이 사용되고 있어 주요 공격대상이지만 악성코드는 맥 OS, 스마트폰 및 태블릿과 같은 모든 컴퓨팅 기기를 감염시킬 수 있습니다. 사이버 범죄자들은 더 많은 컴퓨터와 모바일 기기를 감염시킬수록 더 많은 돈을 벌 수 있습니다. 즉 나를 포함해서 모든 사람이 공격대상입니다.

악성코드 개발자

악성코드는 더 이상 순진한 엔지니어나 아마추어 해커들이 만드는 것이 아니라, 구체적인 목표를 달성하기 위해 지능적인 사이버 범죄자들이 만듭니다. 그들의 목표는 감염된 컴퓨터 또는 기기로부터 돈을 버는 것입니다. 또한 훔친

악성코드란 무엇인가?

데이터를 판매하기도 하고, 스팸 이메일을 보내고, 디도스(DDoS) 공격을 하고, 금품을 강탈합니다. 악성코드를 제작, 배포하고 이익을 얻는 사람들은 범죄 조직원으로 활동하는 개인 또는 정부 기관 등 다양합니다. 오늘날 지능적인 악성코드를 제작하는 사람들은 이러한 목적을 가지고 있으며, 정규 직원으로 악성코드를 개발하고 있습니다. 또한 악성코드를 개발하면, 다른 개인이나 조직에게 판매도 하며 고객들에게 정기적인 업데이트 및 지원도 합니다.



악성코드로부터 방어할 수 있는 가장 좋은 방법은 컴퓨터 기기를 업데이트하고, 항상 최신의 안티 바이러스를 사용하고, 수상한 메시지에 대해서 .주의하는 것입니다.

보호 방안

일반적인 보호방법은 신뢰받는 기업의 안티 바이러스(AV)를 설치하는 것입니다. 안티 악성코드 소프트웨어라고도 불리는 이러한 도구는 악성코드를 탐지 및 차단합니다. 하지만 안티 바이러스는 모든 악성코드를 차단하거나 제거할 수 없습니다. 사이버 공격자들은 지속적으로 새롭고 더 지능적인 악성코드를 개발하여 안티 바이러스 프로그램을 우회할 수 있습니다. 그러면 안티 바이러스 업체에서는 제품에 새로운 악성코드를 탐지할 수 있는 기능을 지속적으로 업데이트합니다. 많은 경우 이것은 양측이 상대편을 앞서기 위해 군비 경쟁과 같이 됩니다. 안타깝지만 범죄자들이 한 발 앞서 있습니다. 그래서 단지 안티 바이러스만 믿을 수 없기 때문에 다음과 같은 추가적인 조치를 취해야 합니다.

- 사이버범죄자들은 소프트웨어의 취약점을 공격하여 컴퓨터나 기기를 감염시킵니다. 소프트웨어가 최신 버전일수록, 시스템 취약점이 줄어들며 감염을 막을 수 있습니다. 그래서 운영체제, 애플리케이션 및 기기들이 자동적으로 보안업데이트 되도록 설정해야 합니다.
- 사이버범죄자들이 모바일 기기를 감염시키는 일반적인 방법은 가짜 모바일 앱을 만들어서 인터넷에 올려놓고 사람들을 속여 다운로드하여 설치하도록 합니다. 이 경우 신뢰할 수 있는 온라인 스토어로부터 앱을 다운로드하고 설치하시기 바랍니다. 추가로 오랫동안 온라인에 게시된 모바일 앱만을 설치하고, 많은 사람들이 이용하고 긍정적인 평가가 많은 앱을 다운로드 하시기 바랍니다.
- 컴퓨터에서 “Administrator” 또는 “root”와 같은 특별한 권한보다 제한된 권한을 가지는 표준 계정을 사용하시기 바랍니다. 이렇게 하면 많은 종류의 악성코드가 설치되는 것을 막을 수 있습니다.
- 사이버 범죄자들은 사람들 속여서 악성코드를 설치합니다. 예를 들어 합법적인 것처럼 보이는 이메일을 보내거나, 첨부문서나 링크가 포함된 이메일을 보냅니다. 이러한 이메일은 은행이나 친구가 보낸 것처럼 보입니다. 하지만

악성코드란 무엇인가?

만약에 링크를 클릭하거나 첨부 문서를 열면, 악성코드가 실행되고 시스템에 악성프로그램이 설치됩니다. 만약에 본문에 긴급하다는 내용이 있거나 너무 좋은 조건이 있으면, 공격일 수 있습니다. 이러한 이메일은 먼저 의심을 하고, 상식적으로 판단하는 것은 가장 좋은 방어책입니다.

- 시스템 및 파일을 클라우드 서비스로 주기적으로 백업하거나, 외부저장매체에 저장해야 합니다. 이렇게 하면 악성코드가 데이터를 암호화하거나 삭제하는 경우에도 백업파일을 보호할 수 있습니다. 백업은 굉장히 중요하며, 악성코드 감염 시 데이터를 복구할 수 있는 유일한 방법입니다.

정리하면, 악성코드로부터 가장 좋은 방어방법은 최신의 소프트웨어를 유지하고, 신뢰할 수 있는 업체의 안티바이러스 소프트웨어를 설치하고, 시스템을 감염시키기 위해 속이는 이메일에 대해서 주의하는 것입니다.

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

피싱:	https://securingthehuman.sans.org/ouch/2015#december2015
소셜 엔지니어링:	https://securingthehuman.sans.org/ouch/2014#november2014
모바일 앱 안전하게 사용하기:	https://securingthehuman.sans.org/ouch/2015#january2015
태블릿 컴퓨터 보안:	https://securingthehuman.sans.org/ouch/2016#january2016
백업:	https://securingthehuman.sans.org/ouch/2015#august2015

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