OUCH! | 2016 년 08 월호

전 국민대상 월간 정보보호 인식제고 뉴스레터

OUCH!

이달 호 주제..

- 랜섬웨어란
- 몸 값을 지불해야 하는가?
- 파일 백업
- 추가 보호 조치

랜섬웨어

랜섬웨어란

랜섬웨어는 오늘날 인터넷을 통해 활발히 전파되는 특수한 악성코드입니다. 랜섬웨어는 피해자의 문자 및 파일 등을 파괴한다고 위협합니다. 악성코드는 소프트웨어 프로그램으로 악성행위를 수행하는 데 사용됩니다. 랜섬웨어는 여러 가지 종류의 악성코드 중 하나이지만, 범죄자들에게 수익이 되면서부터 일반화되었습니다. 일단 랜섬웨어가 컴퓨터를 감염하면, 컴퓨터 하드디스크 전체 또는 일부 파일을 암호화합니다. 그리고 컴퓨터 관리자는 시스템에 접근하지 못하거나, 문서, 사진 등 중요한 파일에 접근할 수 없게 됩니다. 악성코드는 그리고 파일을 복호화 하거나 컴퓨터를 복구할 수 있는 유일한 방법은 몸 값을 지불하는 것이라고 알려줍니다. 종종 몸 값은 비트코인과 같은 디지털 화폐로 지급되어야 합니다. 랜섬웨어는 다른 악성코드와 유사하게 전파합니다. 가장 일반적인 방법은 피해자에게 악성 이메일을 발송하는 것이며, 범죄자들은 수신자를 속여서 감염된 문서를 열게 하거나, 공격자의 웹사이트로 이동하게 하는 링크를 클릭하도록 합니다.

객원 편집자

레니 젤트서는 NCR社에서 고객 IT 운영보안 담당하고 있으며, SANS 연구소에서 악성코드 퇴치에 대해서 강의합니다. 레니는 트위터 @lennyzeltser 및 zeltser.com보안 블로그를 운영하고 있습니다.

몸 값을 지불해야 하는가?

이게 어려운 문제입니다. 문제는 컴퓨터가 감염되었을 때 범죄자에게 몸 값을 지불하는 사람이 많을수록 범죄자들은 더 많은 사람들을 감염시킵니다. 반면 파일을 복구할 수 없는 다른 방법이 없다면, 몸 값을 지불하더라고 파일을 복구할 수 있다는 보장은 없습니다. 범죄자와 협상을 하면, 범죄자들은 파일을 복구해주 지 않을 수 있습니다. 또는 몸 값을 지불하고 복호방법을 받더라도, 복호화 과정에서 잘못될 수도 있거나, 다른 악성코드에 감염될 수도 있습니다.

파일 백업

랜섬웨어 감염 시 몸 값을 지불하지 않고 복구할 수 있는 유일한 방법은 백업한 파일에서 복구하는 것입니다. 이 방법은 랜섬웨어에 감염되었다고 하더라도 컴퓨터를 새로 설치하여 파일을 복구할 수 있습니다. 만약에 백업파일이 감염된

랜섬웨어

시스템에서 접근된다면 랜섬웨어는 백업파일을 지우거나 암호화시킬 수 있습니다. 그러므로 백업파일을 유명한 클라우드 서비스에 저장하거나, 시스템과 연결되어 있지 않은 외부 저장매체에 저장해 놓는 것이 중요합니다. 추가로 많은 사람들이 백업을 만들 때 하는 실수가 파일이 실수 복구될 수 있는 지 시험하지 않는 것입니다. 백업파일은 제대로 복구가 되는 지 주기적으로 시험하고, 시스템이 랜섬웨어에 감염되었을 때 필요한 파일을 복구할 수 있는 확인하시기 바랍니다. 사고로 파일을 삭제하거나 하드 디스크가 고장 날 경우에도 백업을 통해 복구할 수 있기 때문에 백업은 굉장히 중요합니다.

랜섬웨어는 일단 컴퓨터를 감염시키면, 컴퓨터에 있는 모든 파일을 암호화하거나 접근을 할 수 없도록 하는 악성코드의 한 종류입니다.

추가 보호 조치

추가로 다른 종류의 악성코드 감염을 예방하는 방법과 동일하게 랜섬웨어 감염으로부터 보호할 수 있습니다. 최신의 유명한 회사의 안티바이러스 소프트웨어를 최신으로 유지하기 바랍니다. 안티 악성코드 소프트웨어라 불리는 이러한 도구는 악성코드를 탐지하고 중지시키는 기능을 합니다. 하지만 안티바이러스는 악성프로그램을 차단하거나 삭제할 수 없습니다. 사이버 범죄자들은 지속적으로 연구하여 탐지를 우회할 수 있는 새롭게 더 지능적인 악성코드 개발합니다. 마찬가지로 안티바이러스 회사들은 악성코드를 탐지할 수 있는 새로운 기능으로 업데이트합니다. 이것은 상대방을 앞서기 위해 양측이 군비 경쟁하는 것과 유사합니다. 불행히도 범죄자들이 한 발짝 앞서갑니다. 그러므로 파일을 백업하고, 아래의 조치를 적용해야 합니다.

- 사이버범죄자들은 소프트웨어 취약점을 공격하여 컴퓨터나 기기를 감염시킵니다. 소프트웨어 최신일수록 시스템의 취약점은 줄어들며 감염이 어렵게 됩니다. 그러므로 운영체제, 프로그램 및 기기들이 자동으로 업데이트하도록 설정해야 합니다.
- 컴퓨터에서 “Administrator” 또는 “root”와 같은 특별한 권한의 계정대신 권한이 제한된 일반 계정을 사용하십시요. 이 방법은 다른 악성코드를 예방하는 데에도 도움이 됩니다.
- 사이버범죄자들은 사람들을 속여서 악성코드를 설치합니다. 예를 들어 첨부 파일이나 링크와 같이 정상적인 것처럼 보이는 이메일을 발송합니다. 이메일은 은행이나 친구가 보낸 것처럼 보입니다. 하지만 첨부파일이나

랜섬웨어

링크를 클릭하면, 악성코드가 활성화되어 시스템에 악성프로그램이 설치됩니다. 이메일 내용이 긴급한 느낌이 있거나, 너무 좋은 내용이거나, 문법이 틀렸거나 하면 공격일 수 있습니다. 의심하고 상식적으로 판단하는 것이 가장 좋은 방어책입니다.

이메일 첨부문서 또는 링크를 클릭할 때 주의하고, 최신의 안타바이러스 소프트웨어를 사용하고, 주기적으로 파일을 백업 및 복구하여 랜섬웨어로부터 우리자신을 보호해야 합니다.

자세히 알아 보기

securingthehuman.sans.org/ouch/archives를 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
악성코드란:	https://securingthehuman.sans.org/ouch/2016#march2016
암호:	https://securingthehuman.sans.org/ouch/2016#june2016
백업:	https://securingthehuman.sans.org/ouch/2015#august2015
마이크로소프트 랜섬웨어:	https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx
SANS FOR610 : 악성코드 역공학 과정:	https://sans.org/for610

편집위원회 : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley, 번역:진수희(ITL Inc.)