OUCH! | 2016 년 04 월호

컴퓨터 사용자를 위한 월간 정보보호 인식 뉴스레터

OUCH!

이달 호 주제..

- 개요
- 해킹피해 단서
- 대응방법

해킹당한 후 대응지침

개요

모두들 자신의 컴퓨터와 모바일 기기를 보호하는 것에 신경을 쓰고 있으며, 보호조치에 대해서 잘 알고 있습니다. 하지만 아무리 안전하게 기술을 이용하더라도 언젠가는 해킹될 수 있습니다. 이번 달 뉴스레터에서는 자신의 컴퓨터 및 모바일 기기가 해킹되었는 지 알 수 있는 방법과, 해킹을 당했을 때 대응조치에 대해서 알려줍니다. 극단적으로 컴퓨터가 해킹되었는지 빨리 탐지하고 대응할수록, 공격자로 인해 발생하는 피해를 최소화할 수 있습니다.

객원 편집자

사만사 데이베슨(@sam_e_davison)은 전세계 350개 도시에서 우버사 직원을 교육하는 보안인식제고 교육프로그램 매니저이다.

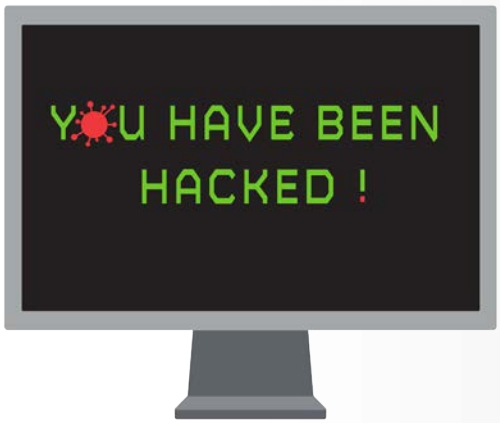
해킹피해 단서

해킹당했다는 것을 알 수 있는 확실한 방법은 없기 때문에 해킹 여부를 알아내기는 쉽지 않습니다. 대신 일반적으로 여러 개의 단서(지표)들을 남깁니다. 만약에 시스템에 아래와 같은 단서(증상)들이 나타난다면, 해킹되었을 가능성이 큽니다.

- 안티바이러스 프로그램에서 컴퓨터가 감염되었다고 알람을 띄운다. 특히 안티바이러스가 감염파일을 제거하거나 격리시킬 수 없다고 한다.
- 브라우저에서 홈페이지가 갑자기 바뀌거나 브라우저가 원하지 않는 웹사이트로 이동시킨다.
- 컴퓨터나 모바일 기기에 만든 적이 없는 새로운 계정 또는 설치한 적이 없는 프로그램이 동작하고 있다.
- 컴퓨터 또는 프로그램의 속도가 느려지고 계속 다운된다. 모르는 프로그램의 아이콘이 있고, 윈도에 팝업이 뜬다.
- 컴퓨터 관리자가 프로그램을 직접 설치하지 않거나 업데이트하지 않는데도, 컴퓨터에 있는 프로그램이 시스템을 변경하기 위해 승인을 요청한다.
- 패스워드가 정확한데도 시스템이나 온라인 계정에 로그인 시도 시 패스워드 오류가 난다.
- 친구들이 내가 보낸적도 없는 이메일 스팸이 오고 있다고 말한다.
- 모바일 기기에 프리미엄 SMS 번호로 요금 청구되고 있다.

해킹당한 후 대응지침

- 모바일 기기에 갑자기 데이터가 늘어나고 배터리 사용속도가 빠르다.



컴퓨터나 모바일 기기가 해킹된다면, 사고를 빨리 탐지하고 대응할수록 좋습니다.

대응방법

컴퓨터나 모바일 기기가 해킹되었다고 인지하면 빨리 대응할수록 좋습니다. 사용하는 컴퓨터나 모바일 기기가 회사 소유 또는 업무용이라면 직접 수리하지 말기를 바랍니다. 이 경우 더 큰 피해가 발생할 뿐만 아니라, 조사 시 사용될 수 있는 중요한 증거를 없앨 수가 있기 때문입니다. 대신 헬프 데스크, 보안 팀 또는 상사에게 연락해서 회사로 즉시 사고를 보고해야 합니다. 회사로 연락이 되지 않거나 지연이 될 것 같으면, 컴퓨터의 네트워크를 분리하고 비행모드로 설정해서 그대로 두는 것이 좋습니다. 해킹되었는 지 확신이 서지 않는다고 하더라도 보고하는 것이 좋습니다. 컴퓨터가 개인적인 용도로 사용되는 것이라면, 자체적으로 취해야 할 조치는 다음과 같습니다.

- **패스워드 변경**: 컴퓨터 및 모바일 기기의 패스워드뿐만 아니라 온라인 사이트의 패스워드도 변경해야 한다. 해킹된 컴퓨터에서 패스워드를 변경하면 안된다. 대신 안전한 컴퓨터나 모바일 기기를 이용해서 패스워드를 변경해야 한다.
- **안티바이러스**: 안티바이러스 프로그램에서 감염된 파일을 알려주면 권고하는 조치를 취해야 한다. 이 경우 주로 감염파일을 격리하고, 파일을 청소 또는 삭제한다. 대부분의 안티바이러스는 감염되었을 때 감염 정보를 알 수 있도록 안내하는 링크를 가지고 있다. 의심스러운 파일이 있으면 격리해야 한다. 이것이 불가능하면 삭제하는 것이 좋다.
- **재설치**: 감염된 시스템을 수리하지 못하거나, 완전한 복구를 원한다면 가장 안전한 방법은 재설치하는 것이다. 컴퓨터의 경우 먼저 컴퓨터 제조사의 지침을 따라야 한다. 대부분의 경우 빌트인된 유틸리티를 이용해서 운영체제를 새로 설치한다. 만약에 유틸리티가 없거나, 파괴되었거나 감염되었다면 제조사로 연락하거나 웹사이트를 방문해야 한다. 백업파일에서 운영체제를 재 설치하면 안된다. 백업파일을 이용하는 경우 기존의 해커들이 공격한 취약점이 있을 수 있다. 백업은 데이터를 복구할 때만 이용해야 한다. 모바일 기기의 경우 웹사이트에 나와 있는 기기 제조사 또는 서비스 회사의 지침을 따른다. 대부분의 경우 간단하게 공장 초기화로

해킹당한 후 대응지침

복구할 수 있다. 재설치 과정을 잘 모르겠으면 전문서비스 업체를 이용하는 것도 괜찮다. 또는 컴퓨터나 모바일 기기가 오래된 경우, 운영체제를 새로 설치하는 것보다 새로 구입하는 것이 더 낫다. 마지막으로 일단 컴퓨터나 모바일 기기를 재설치하거나 새로운 것을 구매하였으면, 항상 업데이트상태를 유지하고, 가능하면 자동 업데이트를 활성화하는 것이 좋다.

- **백업**: 백업에서 가장 중요한 조치는 미리 미리 정기적으로 백업하는 것이다. 자주 백업하는 것이 가장 좋다. 어떤 솔루션은 매 시간마다 자동으로 새로운 파일이나 변경된 파일을 백업한다. 어떤 백업 솔루션이던 주기적으로 파일을 복구할 수 있는 지를 확인해야 한다. 백업한 파일에서 데이터를 복구하는 것이 해킹당한 후 복구할 수 있는 유일한 방법이다.
- **경찰 신고**: 위협을 느낀다면, 사고를 지역 경찰로 신고해야 한다.

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

백업:	https://securingthehuman.sans.org/ouch/2015#august2015
패스워드:	https://securingthehuman.sans.org/ouch/2015#april2015
악성코드란 무엇인가?:	https://securingthehuman.sans.org/ouch/2016#march2016
태블릿 컴퓨터 보안:	https://securingthehuman.sans.org/ouch/2016#january2016

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