컴퓨터 사용자를 위한 월간 정보보호 인식 뉴스레터

OUCH!

이달 호 주제..

- 개요
- 해킹지표(IoC)
- 대응방법

해킹당한 후 대응지침

개요

컴퓨터와 정보를 보호하는 방법 및 이를 보호하는 단계에 대해서 모두들 걱정하고 있다. 하지만 자동차를 운전하는 것처럼 아무리 안전하게 운전을 한다고 해도 사고를 당할 수 있다. 이번 달 뉴스레터에서는 컴퓨터가 해킹되었는 지 알 수 있는 방법과, 해킹을 당했을 때 대응조치에 대해서 알려준다. 극단적으로 컴퓨터가 해킹되었는지 빨리 탐지하고, 빨리 대응할수록, 컴퓨터 및 조직에 피해를 최소화할 수 있다.

객원 편집자

제이크 윌리엄스(@MalwareJake; malwarejake.blogspot.com)는 CSR그룹 컴퓨터 보안 컨설턴트에서 수석과학자이다. 제이크는 메모리 포렌식(FOR526) 및 악성코드 역공학(FOR610) 과정의 공동 저자이다.

해킹 지표(IOC)

먼저 대부분의 경우 컴퓨터가 해킹되었는 지 정확하게 알 수 있는 왕도는 없다는 점을 알아야 한다. 대신 일반적으로 여러 개의 징후들이 있다. 만약에 다음의 징후들이 나타난다면, 해킹되었다는 뜻이다. 다음의 이러한 예이다.

- 컴퓨터가 감염되었다고 안티바이러스 프로그램이 알람을 띄운다. 특히 안티바이러스가 감염파일을 제거하거나 격리시킬 수 없다고 한다.
- 브라우저에서 홈페이지가 갑자기 바뀌거나 브라우저가 원하지 않는 웹사이트로 이동시킨다.
- 컴퓨터에 만들지 않은 새로운 계정이 있다.
- 설치하지 않은 새로운 프로그램이 실행되고 있다.
- 컴퓨터의 속도가 느려지고, 계속 다운된다.
- 컴퓨터 관리자가 직접 설치하지 않거나 업데이트하지 않는데도, 컴퓨터에 있는 프로그램이 시스템을 변경하기 위해 승인을 요청한다.
- 우리가 인식하지 않는 프로그램이 인터넷에 접속하도록 허가를 요청한다는 컴퓨터 방화벽에서 경고한다.

해킹당한 후 대응지침

대응 방법

컴퓨터가 해킹되었다면, 빨리 대응할수록 좋다. 사용하는 컴퓨터가 회사 것이거나 업무용이라면, 직접 수리하지 말고, 전원도 끄면 안 된다. 더 큰 피해가 발생할 뿐만 아니라, 조사 시 사용될 수 있는 중요한 증거를 없앨 수가 있기 때문이다. 대신 헬프 데스크, 보안 팀 또는 상사에게 연락해서 회사로 즉시 사고를 보고해야 한다. 회사로 연락이 되지 않거나 지연이 될 것 같으면, 컴퓨터의 네트워크를 분리하고 그대로 두는 것이 좋다. 해킹되었는 지 확신이 서지 않는다고 하더라도 보고하는 것이 좋다. 조직에서 이와 같은 상황을 처리하는 팀이나 프로세스가 있을 수 있다. 컴퓨터가 개인적인 용도로 사용되는 것이라면, 자체적으로 취해야 할 조치는 다음과 같다.

컴퓨터가 해킹된다면, 빨리 사고를 탐지하고 대응할수록 피해를 최소화할 수 있습니다.

- **백업**: 가장 중요한 조치는 자료를 백업하는 것이다. 특히 정기적으로 주기적으로 데이터를 백업하여 필요 시 백업 파일에서 복구할 수 있다. 컴퓨터가 해킹되었다면, 유일한 방법이 시스템과 하드디스크를 포맷하고 운영체제를 다시 설치하거나 새로운 컴퓨터를 구매하는 것이다. 어떤 방법이든 백업을 하면 개인적인 데이터를 복구할 수 있다.
- **패스워드 변경**: 모든 패스워드를 변경해야 한다. 컴퓨터 및 모바일 기기의 패스워드뿐만 아니라 온라인 사이트의 패스워드도 변경해야 한다. 온라인 사이트의 패스워드 전체를 변경하는 것만이 안전하다.
- **안티바이러스**: 안티바이러스 소프트웨어에서 감염 파일을 알려주면, 권고하는 조치를 취해야 한다. 이 경우 주로 감염파일을 격리하고, 파일을 청소 또는 삭제한다. 대부분의 안티바이러스 소프트웨어는 감염되었을 때 감염 정보를 알 수 있도록 안내하는 링크를 가지고 있다. 의심스러운 파일이 있으면 격리해야 한다. 이것이 불가능하면 삭제하는 것이 좋다.
- **재설치**: 안티바이러스로 컴퓨터를 청소하지 못한다면 가장 안전한 방법은 훼손된 컴퓨터를 재설치하는 것이다. 먼저 컴퓨터를 네트워크에서 분리하고, 컴퓨터 제조사의 지침을 따라야 한다. 대부분의 경우 운영체제를 새로 설치할 때 기존의 복구 파티션을 사용하는 것이다. 만약에 복구 파티션이 없거나, 파괴되었거나 감염되었다면 제조사로 연락해서 복구 DVD를 보내달라고 요청해야

해킹당한 후 대응지침

한다. 백업파일에서 운영체제를 재 설치하면 안된다. 백업파일을 이용하는 경우 기존의 해커들이 공격한 취약점이 있을 수 있다. 백업파일은 개인적인 데이터만 이용해야 한다. 또한 컴퓨터가 오래된 경우, 운영체제를 새로 설치하는 것보다 새로 구입하는 것이 더 낫다.

- **전문적인 도움**: 만약에 해킹된 것으로 의심되는데 직접 해결할 수 있는 지식이나 기술이 없다면, 전문가에게 컴퓨터를 맡기는 것이 좋다. 예를 들어 해킹 된 후 최근의 데이터가 백업이 되지 않았다는 것을 알았다 그래서 사진, 문서 또는 동영상을 감염된 컴퓨터에서 새로운 컴퓨터로 이동시키고 싶을 수가 있다. 하지만 이렇게 하는 경우 파일 뿐만 아니라 악성코드도 함께 새로운 컴퓨터로 복사 될 수 있다. 좀 더 안전한 방법은 감염 파일을 이동시키지 않고 파일을 안전하게 복구할 수 있는 자격을 갖춘 기술자에게 컴퓨터를 맡기는 것이다.

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

OUCH! 백업:	http://www.securingthehuman.org/ouch/2013#september2013
OUCH! 패스워드:	http://www.securingthehuman.org/ouch/2013#may2013
OUCH! 악성코드란 무엇인가?:	http://www.securingthehuman.org/ouch/2014#february2014
공격자 탐지 포스터:	https://digital-forensics.sans.org/media/poster_2014_find_evil.pdf

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