SANS SECURITY AWARENESS

전 국민대상 월간 정보보호 인식제고 뉴스레터

해킹당한 후 대응지침

개요

아무리 안전에 대해서 주의를 하더라도, 자동차 운전하는 것과 마찬가지고 사고를 당할 수 있습니다. 다음은 해킹 당했는지 알 수 있는 단서를 제공하며, 만약 그렇다면 무엇을 해야 하는지 알려줍니다. 극단적으로 컴퓨터 해킹여부를 빨리 인지할수록, 더 빨리 문제를 수정할 수 있습니다.

해킹단서

- 바이러스 백신 프로그램이 시스템이 감염되었다는 경고합니다. 이 경우 경고하는 바이러스 백신 소프트웨어가 자신의 백신소프트웨어라는 것을 확인해야 합니다. 웹 사이트에서 팝업 경고하는 경우, 전화를 걸도록 하거나 다른 것을 설치하도록 하는 것은 공격일 수 있습니다. 확실하지 않다면, 자신의 안티 바이러스 프로그램을 실행하십시오.
- 컴퓨터가 암호화되었다는 팝업 창이 뜨고, 파일을 되찾기 위해 몸값을 지불해야합니다.
- 브라우저에서 원하지 않는 이상한 웹 사이트로 이동합니다.
- 컴퓨터 또는 응용 프로그램이 계속 충돌합니다. 알 수 없는 응용 프로그램이나 이상한 창이 표시되는 아이콘이 있습니다.
- 패스워드가 맞는데도 패스워드가 맞지 않다고 나옵니다.
- 이메일을 보낸 적이 없는데 친구가 이메일 스팸을 보내는 이유를 묻습니다.
- 사용하지 않은 신용 카드에는 요금이 결제되었거나, 은행에서 돈이 인출되었습니다.

대응방법

해킹되었다고 인지하면 빨리 대응할수록 좋습니다. 사용하는 컴퓨터나 모바일 기기가 회사 소유 또는 업무용이라면 직접 수리하지 마시고 즉시 보고하시기 바랍니다. 개인 컴퓨터 또는 개인의 계정이 해킹되었다면, 자체적으로 취해야 할 조치는 다음과 같습니다.

패스워드 변경: 컴퓨터 및 모바일 기기의 패스워드뿐만 아니라, 온라인 사이트의 패스워드도 변경해야 한다. 해킹된 컴퓨터에서 패스워드를 변경하면 안됩니다. 대신 안전한 컴퓨터나 모바일 기기를 이용해서 패스워드를 변경해야 합니다. 계정이 많은 경우 먼저 가장 중요한 계정부터 시작하십시오. 모든 패스워드를 관리할 수 없다면 패스워드 관리프로그램을 사용하십시오.

금융: 신용 카드 또는 금융 계좌 관련 문제는 즉시 은행이나 신용 카드 회사에 문의하십시오. 신뢰할 수 있는 전화번호를 사용하여 은행 카드 뒷면, 재무 재표 또는 신뢰할 수 있는 컴퓨터에서 웹 사이트를 방문하여 전화하십시오. 또한 신용 카드 정지 또는 계좌 정지 등을 고려하십시오.

안티바이러스: 안티바이러스 프로그램에서 감염된 파일을 알려주면 권고하는 조치를 취해야 합니다. 대부분의 안티바이러스는 감염되었을 때 감염 정보를 알 수 있도록 안내하는 링크를 가지고 있습니다.

재설치: 감염된 시스템을 수리하지 못하거나, 완전한 복구를 원한다면 가장 안전한 방법은 재설치하는 것입니다. 백업파일에서 운영체제를 재 설치하면 안됩니다. 백업은 데이터를 복구할 때만 이용해야 합니다. 재설치 과정을 잘 모르겠으면 전문서비스 업체를 이용하는 것도 괜찮습니다. 또는 컴퓨터나 모바일 기기가 오래된 경우, 운영체제를 새로 설치하는 것보다 새로 구입하는 것이 더 낫습니다. 마지막으로 일단 컴퓨터나 모바일 기기를 재설치하거나 새로운 것을 구매하였으면, 항상 최신의 업데이트상태를 유지하고, 가능하면 자동 업데이트를 활성화하는 것이 좋습니다.

백업: 자신을 보호하기위한 핵심 단계는 정기적인 백업으로 사전 준비하는 것입니다. 많은 솔루션이 파일을 매일 또는 시간별로 자동 백업합니다. 어떤 솔루션을 정기적으로 사용하든 관계없이 해당 파일을 복원할 수 있는지 확인하십시오. 데이터 백업을 자주 복구하는 것이 해킹으로부터 복구할 수 있는 유일한 방법입니다.

경찰 신고: 위협을 느낀다면, 지역 경찰서로 사고를 신고해야 합니다. 귀하의 신분 이 도용되었다면, http://cyberbureau.police.go.kr/ 를 방문하십시오.

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

조하네스 울리치 박사(@johullrich)는 SANS 기술연구소의 SANS 인터넷스톰센터 이사이자 SANS 연구원입니다. 조하네스는 DShield 센서 네트워크를 만들고 인터넷스톰센터의 일일 네트워크 보안 뉴스 포드 캐스트를 방송합니다.

참고자료

백업: https://www.sans.org/u/JGP
패스워드: https://www.sans.org/u/JGU
패스워드 관리프로그램: https://www.sans.org/u/JGZ
악성코드란: https://www.sans.org/u/JH4
신용정지: https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/

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