OUCH! | 2018 년 9 월 호

SANS SECURITY AWARENESS

OUCH!

전 국민대상 월간 정보보호 인식제고 뉴스레터

CEO 사기/BEC

CEO 사기/BEC란?

사이버 공격자는 CEO 사기 또는 BEC(Business Email Compromise)라는 이메일 공격을 지속적으로 발전시키고 있습니다. 이것은 표적형 이메일 공격으로 피해자가 하지 말아야 하는 행동을 하도록 속이는 것입니다. 대부분의 경우 나쁜 사람은 돈을 쫓고 있습니다. 이러한 공격을 매우 위험하게 만드는 요인은 사이버 공격자가 공격을 시작하기 전에 범죄대상을 조사한다는 것입니다. 감염된 이메일 첨부 파일이나 탐지할 악성 링크가 없기 때문에 보안 기술로는 이러한 공격을 막는 것은 매우 어렵습니다. 공격 방법은 다음과 같습니다.

사이버 공격자는 인터넷을 사용하여 목표로 하는 범죄대상과 이들과 연락하는 사람들을 조사합니다. 예를 들어, 이들이 당신을 목표로 한다면, 당신의 상사가 누구인지 또는 사는 곳의 부동산 중개인을 조사하게 됩니다. 사이버 공격자는 이 사람들 중 하나인 것처럼 위장하여 이메일을 만들어서 사용자에게 보냅니다. 이메일은 긴급한 것이며, 청구서 처리, 지급 대상 변경, 중요한 문서를 송부하도록 하는 것과 같은 즉시 조치를 취하도록 요구합니다. 이메일을 통해 압박하여 이들이 원하는 것을 하도록 합니다. 다음은 이러한 공격이 동작하는 방식에 대한 두 가지 사례입니다.

계좌 이체: 사이버 범죄자가 돈이 목표입니다. 이들은 당신이 일하는 회사를 조사합니다. 예를 들어, 외상매입담당자가 누구인지, 예산지출 담당자를 찾아내는 것입니다. 그 범죄자들은 그 상사 또는 고위 간부로 위장하여 이들에게 이메일을 조작하여 보냅니다. 이메일은 긴급상황이라고 알려주고 즉시 새로운 은행계좌로 송금해야 한다고 합니다. 이메일을 통해 압박하여 실수를 유도해서, 실제로는 범죄자에 송금을 하게 합니다.

세금 사기: 사이버 범죄자는 세금 사기에 사용할 개인 정보를 찾고 있습니다. 이 것을 얻는 가장 빠른 방법 중 하나는 회사의 모든 직원의 정보를 훔치는 것입니다. 사이버 범죄자들은 인사부서에 누가 근무하는 지 연구하고 알아냅니다. 그런 다음 이들은 고위 간부 또는 법적으로 위장한 이들이 가짜 이메일을 보냅니다. 이메일은 모든 직원에 대한 세금 정보가 즉시 제출되어야 한다는 긴급한 내용이 포함되어 있습니다. 인사부 직원들은 민감한 문서를 고위 간부에게 보내는 것으로 생각하지만, 실제로는 사이버 범죄자에게 보내고 있는 것입니다.

보호방법

자신을 보호하기 위해 무엇을 할 수 있습니까? 상식이 최선의 방어입니다. 사기성 이메일을 알아낼 수 있는 가장 일반적인 단서는 다음과 같습니다.

- 이메일은 매우 짧고 (종종 문장이 두 개), 긴급하며, 모바일 기기에서 이메일이 발송되었다는 서명이 포함되어 있습니다.
- 긴박감이 있으며, 회사의 정책을 무시하거나 우회하도록 압력을 가합니다. 이메일이 상사 또는 CEO로부터 온 것으로 보이는 경우에도 항상 업무 관련 정책 및 절차를 따르십시오.
- 이메일은 업무와 관련되어 있지만 @naver.com 또는 @gmail.com 과 같은 개인 이메일 주소를 사용합니다.
- 이메일은 선임자, 동료 또는 업체에서 보낸 것처럼 보이지만, 메시지의 뉘앙스는 그렇게 보이지 않습니다.
- 지급 지침이 제공되지만, 이미 알고 있는 것과 다르며, 메시지에 다른 은행 계좌로 즉시 지불하도록 요구합니다.

만약에 자신이 직장에서 공격대상이 된 것으로 의심되면, 공격자와의 모든 상호 작용을 중지하고 상사에게 보고하십시오. 가정에서 공격을 받아 돈을 이체하였다면, 즉시 은행에 신고하고 그 다음 경찰에 신고하십시오.

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

돈 카벤더는 전직 FBI 특수 요원으로 디지털 포렌식 및 사이버 범죄 업무에 22년 이상의 경력을 가지고 있다. 돈은 최근 워싱턴 D.C. BEC 코디네이터로서 사이버범죄 기관 공격시험을 하였다. 돈은 디지털포렌식 및 사이버 조사, 연구 및 교육을 제공하고 있다. @don_cavender https://www.linkedin.com/in/donald-cavender 에서 돈을 만날 수 있다.

참고자료

사회공학: https://www.sans.org/u/HE3
피싱 차단: https://www.sans.org/u/HE8
악성코드 차단: https://www.sans.org/u/HEd
로그인 잠금: https://www.sans.org/u/HEi

OUCH!는 SANS Security Awareness 프로그램에 의해 발행되며 Creative Commons BY-NC-ND 4.0 라이센스로 배포됩니다 이 문서는 출처를 밝히고, 상업적 목적 또는 수정하지 않는다면 자유롭게 배포할 수 있습니다. 번역 및 추가 문의 사항이 있으시면 www.sans.org/security-awareness/ouch-newsletter 로 연락 주시기 바랍니다. 편집위원회: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | 번역:진수희(ITL Inc.)