전 국민대상 월간 정보보호 인식제고 뉴스레터

OUCH!

이달 호 주제..

- **사회공학이란**
- **사회공학 공격 탐지 및 차단**

사회공학

개요

사람들은 일반적으로 사이버공격자들은 첨단 해킹 도구와 기술을 이용해서 사람들의 컴퓨터, 계정 및 모바일 기기를 해킹한다고 오해하고 있습니다. 하지만 이것은 사실이 아닙니다. 사이버 공격자들이 정보를 훔치고 컴퓨터 및 계정을 해킹하는 가장 쉬운 방법 중 하나가, 사람들을 속여서 실수하도록 하는 것이라는 것을 알게 되었습니다. 이번 달호는 사회공학 공격이라는 불리는 공격의 방법 및 우리를 보호할 수 있는 방법에 대해서 배우게 됩니다.

객원 편집자

제임스 라인은 SANS 공인강사이며 (@jameslyne), 소포스의 글로벌 연구팀장이다. 제임스는 사이버공격자의 최신 공격을 분석한다. 제임스는 메타스플로잇(SEC580) 및 소셜 엔지니어링 (SEC567) 과정의 저자이다.

사회공학이란

사회공학은 공격자들이 사람들을 속여서, 해야 되지 않아야 할 뭔가를 하도록 하는 심리적 공격입니다. 사회공학은 수 천년 동안 존재해왔으며 사람을 속이는 생각은 새로운 것이 아닙니다. 사기꾼을 생각해보면 사이버사기도 비슷한 것입니다. 오늘날 최신 기술을 이용하면 사람들은 물리적으로 볼 수 없기 때문에, 더 효과적이며 이를 이용하여 전 세계 수 백만 명의 사람들을 대상으로 쉽게 신분을 위장 할 수 있습니다. 추가로 사회공학 공격은 보안 기술을 우회할 수 있습니다. 사회공학이 동작하는 방법을 가장 쉽게 이해할 수 있는 방법은 실제 세계의 사례를 보는 것이다.

우리가 컴퓨터 지원회사 또는 통신사, 마이크로소프트의 기술지원팀이라고 하는 사람들로부터 전화를 받습니다. 전화한 사람은 우리 컴퓨터가 인터넷을 스캐닝하는 등 이상한 행동을 보이며 감염된 것 같다고 하여 보안조치가 필요하다고 합니다. 이 사람들은 다양한 기술적인 용어를 사용해서 컴퓨터가 감염된 것이라고 믿도록 만듭니다. 예를 들어 이 사람들은 컴퓨터에 어떤 파일을 확인하도록 하고, 파일을 찾도록 합니다. 우리들이 그 파일을 찾으면, 이 사람들은 이 파일이 컴퓨터가 감염된 표시라고 믿게 합니다. 그런데 실제로는 이 파일은 모든 컴퓨터에 발견되는 일반적인 시스템 파일인 것입니다. 일단 이 사람들이 우리를 속여서 컴퓨터가 감염되었다고 믿게 만들면, 웹 사이트로 가서 보안

사회공학

소프트웨어를 구매하도록 유도하거나, 컴퓨터를 수리할 수 있도록 컴퓨터에 원격 접속을 할 수 있도록 해달라고 요청합니다. 하지만 판매하는 소프트웨어는 실제로는 악성 프로그램입니다. 만약에 이것을 실제 구매해서 설치하면, 실제로 컴퓨터를 감염시키고, 돈도 지불해야 합니다. 만약에 우리들이 컴퓨터 수리를 위해서 원격 접속을 허가하면, 실제로는 컴퓨터에 접속하여 데이터를 훔쳐서 팔기도 합니다.

사회공학 공격인 지를 알아내고 차단할 수 있는 가장 좋은 방법은 상식적으로 판단하는 것입니다.

다른 예로는, CEO사기라는 이메일 공격으로, 최근 직장에서 많이 발생합니다. 이 것은 공격자들이 온라인으로 공격 대상 조직을 연구하여 조직의 CEO 또는 동료의 이름을 찾아냅니다. 그리고 난 후 공격자들은 그 사람이 보낸 것과 같은 이메일을 만들어 보냅니다. 이메일에는 계좌이체 또는 민감한 직원 정보를 이메일로 보내달라고 하는 등의 급하게 뭔가를 하도록 요구합니다. 종종 이러한 이메일은 회사의 보안 절차를 우회하도록 긴급함을 강조합니다. 예를들어 굉장히 민감한 정보를 @naver.com 이나 @gmail.com 으로 보내달라는 것입니다. 이러한 표적형 공격이 위험한 이유는 공격자들이 사전에 연구를 한다는 점입니다. 추가로 안티바이러스 또는 방화벽과 같은 보안기술로는 이러한 사회공학공격을 탐지하거나 저지할 수 없습니다.

이와 같은 사회공학 공격은 전화 또는 이메일에 한정되어 있지 않으며, SMS, SNS메시지, 전화 등 다양한 기술로도 가능합니다. 핵심은 뭘 조심해야 하는 것인지를 아는 것이며, 우리가 최선의 방어책이라는 점입니다.

사회공학 공격 탐지 및 차단

이러한 공격을 저지하는 것은 생각하는 것보다 간단합니다. 상식적으로 판단하는 것이다. 의심스럽고, 적절한 것 같지 않으면 공격일 수 있다. 사회공학 공격의 일반적인 지표는 다음과 같습니다;

- 엄청나게 긴급한 일이라고 하는 사람이 우리를 속여서 실수를 하도록 합니다.
- 계좌번호와 같이 다른 사람이 접근할 수 없거나, 이미 알고 있는 정보를 요청하는 사람
- 패스워드를 요청하는 사람. 의심스러운 회사에서 요청할 수 있습니다.

사회공학

- 조직에서 따라야 하는 보안 절차를 무시하도록 압력을 가하는 사람
- 진짜라고 믿기에는 너무 좋은 것. 예를 들어 복권을 사지도 않았는데 우리가 복권에 당첨되었다는 것
- 친구나 동료가 사용하지 않는 단어가 포함된 것 같은데 그 사람들로부터 수상한 이메일을 수신. 사이버공격자들은 계정을 해킹하여 속이려고 하는 것일 수 있습니다. 이런 경우 전화나 직접 만나는 등 다른 통신수단을 통해 요청사항 확인이 필요합니다.

수상한 사람들이 우리를 속인다면, 더 이상 그 사람과 의사소통하면 안됩니다. 사회공학 공격이 업무와 관련된 것이라면, 회사의 정보보호팀에 보고해야 합니다. 상식적으로 판단하는 것이 가장 좋은 방어책이라는 것을 기억해야 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
CEO 사기:	https://securingthehuman.sans.org/ouch/2016#july2016
랜섬웨어:	https://securingthehuman.sans.org/ouch/2016#august2016
OUCH 뉴스레터:	https://securingthehuman.sans.org/ouch/archives

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