OUCH! | 2014 년4월호

컴퓨터 사용자를 위한 월간 정보보호 인식 뉴스레터

OUCH!

이달 호 주제..

- 개요
- 공격대상이 되는 이유
- 보호 방안

# 우리가 바로 공격대상입니다.

## 개요

많은 사람들이 오해하고 있는 점이 자신들은 사이버 범죄 대상이 되지 않을 것이라는 점입니다. 즉 우리가 가지고 있는 컴퓨터에는 가치있는 것이 없다고 생각하지만, 진실은 그렇지 않습니다. 컴퓨터, 모바일 기기, 온라인 계정, 이메일 주소, 신용카드 정보가 있거나 온라인 활동을 한다면, 우리는 사이버 범죄자들에게 금전적 가치가 있습니다. 이번 뉴스레터에서는 왜 우리들이 범죄대상이 되며, 공격 받는 방법 및 우리를 보호할 수 있는 방법에 대해서 다룹니다.

**객원 편집자**

에릭 콘래드는 백쇼어 통신社의 대표 및 CTO이며, CISSP 스터디 가이드 2판 및 11번째 시간 CISSP 2판의 선임 저자이다. 에릭은 SANS 연속 모니티링 및 보안 운영 (SEC511)의 공동저자이다.

## 공격대상이 되는 이유

사기, 신분 도용 및 금품 강탈과 같은 범죄는 문명의 역사만큼 오랫동안 존재하였으며 삶의 한 부분이었습니다. 범죄자들의 목적은 동일합니다. 최대한 쉽게, 최소한의 위험으로 가능한 많은 돈을 버는 것입니다. 전통적으로 범죄는 지역적 위치로 인해 제약을 받았고, 범죄대상과의 물리적인 상호작용 때문에 어려웠습니다. 이러한 이유로 범죄 대상도 제한되었고, 범죄가 큰 위험에 노출될 수 있었습니다. 하지만 인터넷 및 온라인 기술이 발전하면서 범죄도 엄청나게 변했습니다. 이제 사이버 범죄자는 쉽게 아주 적은 비용, 낮은 위험으로 전 세계 누구나 범죄대상으로 삼을 수 있습니다. 추가적으로 사이버 범죄자는 굉장히 조직화되고 있고 효율적이며, 과거보다 더욱더 효과적으로 발전하였습니다.

최종적으로 사이버 범죄자들은 신용카드 정보를 더 많이 훔치고 더 많은 은행 계좌번호를 해킹하고 더 많은 패스워드를 해킹할 수록 더 많은 돈을 벌게 됩니다. 사이버 범죄자들은 말 그대로 인터넷에 연결된 누구나 해킹할 수 있습니다. 전세계 수백만 명을 해킹하는 것은 어려운 일처럼 보이지만 자동화 도구를 이용하면 쉽게 할 수 있습니다. 예를 들어 범죄자들은 수백만 개의 이메일 주소 데이터베이스를 구축하고 자동화 도구를 이용해서 이메일 주소로 피싱 메일을 보냅니다. 이메일을 발송하는 비용은 거의 무료입니다. 사이버 범죄자들은 이메일 발송할 때는 해킹된 다른 컴퓨터를 사용합니다. 이 점은 다른 사람들을 해킹하는 데 있어서도 우리의 기기가 가치가 있다는 예가 될 수 있습니다. 결과적으로 이러한 범죄자들은 이메일

© The SANS Institute 2013

# 우리가 바로 공격대상입니다.

공격에서 누가 대상이 될지는 모르지만, 이메일을 더 많이 발송할수록 더 많은 사람들이 걸려든다는 것을 알고 있습니다. 또는 범죄자들은 말 그대로 인터넷에 있는 모든 컴퓨터를 스캐닝하고(스캐닝에는 해킹된 컴퓨터를 사용하는 등) 해킹할 수 있는 모든 컴퓨터 및 기기를 찾고 있습니다. 우리는 아주 특별하기 때문에 이러한 해킹 공격대상에서 제외되어 있지 않다는 점을 기억하시기 바랍니다. 사이버 범죄자들은 우리를 포함하여 가능한 모든 사람들을 공격 대상으로 삼고 있습니다.

우리가 알지 못할 수 있지만 컴퓨터 기기 및 정보는 전세계 사이버 범죄자들에게 엄청난 가치가 있습니다.

## 보호 방안

사이버 범죄자들이 전 세계 사람을 해킹하고자 할 때, 비교적 간단한 방법을 사용합니다. 간단한 단계를 따르기만 하면, 우리를 보호할 수 있습니다. 여기서 추천하는 단계는 다음과 같습니다.

- **우리자신**: 우리자신이 바로 사이버공격에 대한 첫번째 방어선입니다. 많은 공격 방법은 감염된 이메일 첨부 문서를 열게 하거나, 전화를 통해 패스워드를 보내도록 하는 등 먼저 우리를 속이려고 합니다. 상식적으로 접근 하십시오. 이상하거나, 수상한 점, 또는 너무 좋은 조건 등이 있으면 공격일 가능성이 있습니다.

- **업데이트**: 컴퓨터 또는 모바일 기기 등을 완전히 업데이트하고, 최신의 패치를 적용해야 합니다. 업데이트는 운영체제에만 중요한 것이 아니라 사용중인 모든 애플리케이션 및 플러그인에도 중요합니다. 시스템 및 애플리케이션을 최신의 상태로 유지하면 가장 일반적인 공격으로부터 보호받을 수 있습니다.

- **패스워드**: 각각의 계정별로 강력하고 유일한 패스워드를 사용해야 합니다. 이렇게 하면 사용중인 웹 사이트가 해킹되어 패스워드가 해킹되어도, 다른 사이트의 계정은 안전합니다. 모든 기기별로 강력하고, 유일한 패스워드, PIN 또는 다른 잠금 기능을 사용하여 보호되어야 합니다. 많은 계정의 서로 다른 패스워드를 안전하게 관리하기 위해 패스워드 관리 프로그램을 이용해 보시기 바랍니다.

- **신용카드**: 적어도 일주일에 한 번은 신용카드 결제 내역을 확인해보시기 바랍니다. 신용카드 결제내역에 사용하지 않은 거래가 있다면 즉시 카드 회사로 연락하시기 바랍니다. 은행에서 큰

© The SANS Institute 2013

## 우리가 바로 공격대상입니다.

금액 또는 이상한 거래에 대해서 이메일이나 문자 메시지 발송 서비스를 제공하면 이를 이용해서 의심스러운 활동에 대해서 빨리 통보 받으시기 바랍니다.

- **홈 네트워크**: 가정용 와이파이 AP에 강력한 관리자 패스워드를 설정하고, 다른 사람들이 접속할 수 없도록 패스워드를 설정하시기 바랍니다. 그리고 가정용 라우터에 어떤 기기가 접속하는 지 파악하고, 가정용 라우터의 업데이트 상태를 유지하시기 바랍니다.

- **SNS**: 온라인에 많은 정보를 게시할 수록, 위험에 노출될 확률이 높아집니다. 우리가 게시한 정보를 이용해서 사이버 범죄자들은 우리를 목표로 속일 수 있을 뿐만 아니라 실제로 우리를 가치 있는 공격대상으로 여길 수 있습니다.

### 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! 패스워드관리프로그램: | http://www.securingthehuman.org/ouch/2013#october2013 |
| OUCH! 홈 네트워크 보안: | http://www.securingthehuman.org/ouch/2014#january2014 |
| OUCH! 피싱 공격: | http://www.securingthehuman.org/ouch/2013#february2013 |
| 포스터: You Are A Target: | http://www.securingthehuman.org/resources/posters |

OUCH!는 SANS Securing The Human 프로그램에 의해 발행되며 Creative Commons BY-NC-ND 3.0 라이센스로 배포됩니다 이 문서는 출처를 밝히고, 상업적 목적 또는 수정하지 않는다면 자유롭게 배포할 수 있습니다. 번역 및 추가 문의 사항이 있으시면 ouch@securingthehuman.org 로 연락 주시기 바랍니다.

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