

안랩 온라인 보안 매거진

월간 安

2015. 11

Black Mine Operation



CONTENTS

3 EXPERT COLUMN

1989년 영화 ‘뺑 투 더 퓨처’ 속의 2015년은?

6 SPOTLIGHT

안랩, 글로벌 컨퍼런스 ‘VB 2015’에서 모바일 보안 기술 발표

7 SPECIAL REPORT

Black Mine Operation Analysis Report

안랩, ‘검은 광산 작전’의 비밀을 ‘캐내다’

13 PRODUCT ISSUE

‘여신전문금융업법’ 개정과 AhnLab EPS

새 POS 단말기만 설치하면 보안 걱정 끝?

16 THREAT ANALYSIS

겹겹이 위장한 PDF 파일, 기업 내부를 노린다

19 SECURITY VIEWPOINT

AhnLab ISF SQUARE 2015

안랩, 광주와 대전으로 ‘고객 만나러 갑니다’

22 IT & LIFE

일상 생활에서 무심코 지나치는 개인정보 노출

24 STATISTICS

2015년 9월 보안 통계 및 이슈

26 AHNLAB NEWS

안랩, ‘2015 지배구조 우수기업’ 최우수상 수상

V3 모바일, 진단율 및 CPU 사용률 ‘글로벌 최고 수준’

1989년 영화 ‘백 투 더 퓨처’ 속의 2015년은?

타임머신, 호버보드, 자동으로 신발끈을 매주는 나이키 운동화, 하늘을 나는 자동차.

이 단어들을 보고 떠오르는 것이 있다면? 바로 시간여행 영화의 고전 ‘백 투 더 퓨처(Back to the Future)’이다. 1980~1990년대를 기억하는 많은 이들이 가슴 속에 깊이 자리한 이 영화의 1편과 2편이 디지털 리마스터링 과정을 거쳐 10월 21일 재개봉했다. ‘백 투 더 퓨처’가 상상했던 2015년은 어땠을까? 영화의 재개봉과 함께 1989년에 상상한 2015년과 현재를 비교하며 이제는 고전이 된 영화 ‘백 투 더 퓨처’를 다시 보는 것은 색다른 즐거움이 될 것이다.

30년 전 추억 속의 영화가 갑자기 극장으로 돌아온 이유는 바로 1989년 개봉했던 ‘백 투 더 퓨처’ 2편에서 주인공 마티 맥플라이와 에메트 브라운 박사가 타임머신을 타고 간 미래가 바로 2015년 10월 21일이기 때문이다. 우리는 지금 그들이 그렇게 궁금해 했던 미래를 살고 있다.

1989년 백 투 더 퓨처의 두 번째 편이 개봉했을 당시 센세이션을 일으켰던 이유는 영화 속에 등장한 ‘미래’의 소품들 때문이라 해도 과언이 아니다. 그 중 어떤 것은 지금 우리가 흔하게 사용하는 것도 있고, 어떤 것은 여전히 연구 중에 있으며, 또 어떤 것은 2015년인 지금도 먼 미래의 것으로 보이기도 한다. 다시 보는 ‘백 투 더 퓨처’는 흥미로운 영화 내용과는 별개로 1989년에 상상한 2015년을 엿보는 재미가 아주 쏠쏠하다.

여기서 잠깐! 최근 재개봉한 이 영화의 한국 제목은 ‘백 투 더 퓨처’가 아니다. 1987년 개봉 당시의 제목 그대로 ‘백 투 더 퓨처’로 돌아온 것이다.



[그림 1] 타임머신을 타고 2015년으로 온 마티와 에메트 박사

하늘을 나는 ‘호버보드’는 시험 비행 중?

1편에서 능숙한 솜씨로 스케이트보드를 타던 주인공 마티는 2편에서 호버보드(Hoverboard)를 보고 놀라움을 감추지 못한다. 하늘을 나는 스케이트보드인 호버보드는 ‘뽀 투 더 퓨처’ 2편에서 빼놓을 수 없는 아이템이다. 2015년 현재, 하늘을 나는 스케이트보드는 다양한 방식으로 시도되고 있지만 영화에서처럼 상용화되기까지는 다소 시간이 걸릴 것으로 보인다. 하지만 그 다양한 도전은 충분히 살펴볼 만하다.

자동차 브랜드 렉서스는 브랜드 홍보의 일환으로 진행한 ‘Amazing in Motion’ 캠페인에서 호버보드를 만들어 소개했다. 렉서스의 호버보드는 액체질소를 냉각한 초전도체와 영구자석을 이용해 보드를 공중에 띄웠다. 이 호버보드는 자기장을 이용하기 때문에 금속판 위에서만 작동한다. 물 위에서만 동력을 잃을 뿐 그 외의 장소에서는 자유자재로 움직였던 영화 속의 호버보드보다는 제약이 많다.

미국 캘리포니아주의 신생업체 ‘헨도’가 개발한 호버보드는 미국 타임지가 선정한 2014년 최고의 발명품으로 선정되기도 했다. 이 호버보드는 자기장을 방출하는 엔진을 구동해 보드를 띄우는 방식을 사용하고 있으며 본격적인 양산을 준비 중이다.



[그림 2] 호버보드와 신발 끈 자동 조절 운동화

올해엔 나올까? 신발 끈 자동 조절 운동화!

주인공 마티가 미래에서 감탄하며 착용했던 신발 끈 자동 조절 운동화인 ‘나이키 매그(Nike MAG)’는 지난 2011년 한 차례 판매된 바 있다. 하지만 당시 제품은 외형적인 모습만 영화 속의 제품과 같았을 뿐 가장 중요한 기능인 자동 신발 끈 조절장치가 빠져있었다. 하지만 올해 안으로 나이키가 매그를 새롭게 출시할 거라는 소문도 있어서 이 제품의 현실화 여부는 좀 더 지켜봐야 할 것 같다.

하늘을 나는 자동차, 여전히 미래의 이야기

영화에서는 2015년쯤엔 자동차가 하늘을 날 거라고 상상했지만 자동차는 여전히 도로 위를 달리고 있다. 하지만 자동차를 공중에 띄우기 위한 노력 역시 현재 진행형이다. 현재 하늘을 나는 자동차에 가장 가까운 형태는 테라푸기아(Terrafugia)의 트랜지션(Transition)이 아닐까? MIT 졸업생들이 만든 이 회사는 2006년부터 비행자동차인 트랜지션을 연구하고 있다. 2009년 시제품 비행에 성공한 이후 양산을 위한 연구를 계속하고 있다.

일본의 자동차회사 도요타도 하늘을 나는 자동차를 개발하고 있다. 지난 9월 니혼게이지아신문은 도요타의 미국 자회사인 TEMA가 하늘을 나는 자동차를 위한 겹쳐놓는 날개를 미국에 특허출원했다고 전했다. 도요타가 개발하는 차도 하늘을 자유롭게 날 수 있는 건 아니고, 도로를 살짝 벗어나 마찰 없이 운행하는 정도인 것으로 알려졌다.



[그림 3] 하늘을 나는 자동차

‘조스’ 19편? 아쉽지만 4편 이후 나오지 않아

영화 ‘조스’는 당시 최고의 히트 시리즈 중 하나였다. 1975년 개봉한 스티븐 스필버그 감독의 이 영화는 1978년 2편, 1983년 3편, 1987년 4편을 마지막으로 2015년 현재까지 나오지 않고 있다. 하지만 ‘백 투 더 퓨처’ 2편에는 2015년 즈음엔 ‘조스’ 19편이 개봉하지 않을까 하는 상상이 담겨있다. 마티가 ‘조스’ 19편의 홀로그램 광고를 보고 놀라는 장면 또한 인상적이다. 홀로그램 광고 역시 시범적으로 선보인 바 있으나 아직 대중적으로 사용하는 광고 기법은 아니다. 한편, 유니버설 스튜디오는 흥미롭게도 ‘백 투 더 퓨처’ 재개봉에 즈음해 ‘조스’ 19의 예고편을 공개하기도 했다.

초 단위 일기예보, 현실화되면 얼마나 좋을까?

2015년 미래로 온 에메트 박사는 초 단위 일기예보 덕에 비가 언제 그칠지 정확히 알고 있다. 영화에서처럼 초 단위로 기상변화를 예측해주는 일기예보가 있다면 갑자기 내린 소나기에 옷이 젖는 일 따위는 없겠지만, 이 역시 여전히 미래의 이야기다. 일기예보의 정확성은 과거에 비해 훨씬 높아졌지만 갑작스런 변수 등은 여전히 정확한 예측이 어려운 모양이다.

강아지를 산책시키는 ‘드론’

무인비행기 드론(Drone)을 강아지 산책용으로 쓰고 있는 사람이 있을지는 모르겠지만, 드론은 상용화됐다고 봐도 무관할 것 같다. 군사용으로 사용되던 드론은 지난 2013년 미국 온라인 유통업체인 아마존이 물품 배송에 사용하면서 대중에게 알려졌다. 현재는 카메라를 달아 사용하는 등 다양한 영역에서 그 쓰임을 넓히고 있다. 국내에서도 취미용 드론의 인기가 높아지는 추세다.

현실화된 완전 평면 벽걸이 TV, 화상전화, 지문 인식 현관문

여러 채널을 동시에 시청할 수 있는 음성 인식 완전 평면 벽걸이 TV는 지금의 TV와 매우 흡사하다. 오히려 2015년의 TV는 음성인식 이상으로 스마트해졌다. TV로 인터넷을 할 수 있고, 쇼핑도 가능하다. 1980년대만 해도 TV는 TV장에 올려 놓고 쓰는 것이었는데, TV가 점점 얇아지면서 액자처럼 벽에도 걸 수 있게 됐다. 스크린을 이용한 화상전화도 현재 가능한 기술이다. 오히려 2015년엔 스크린 없이 전화기로도 아주 손쉽게 화상전화를 할 수 있다. [그림 4]에서 마티의 아들이 쓰고 있는 안경은 전화를 하는 용도로 보이는데, 겉으로 보기엔 흡사 구글 글래스를 닮았다. 하지만 구글 글래스의 기능은 당시의 상상을 훨씬 뛰어 넘는 수준이다. 지문으로 현관문을 여는 기술 또한 현재 상용화돼 있다.



[그림 4] 구글 글래스를 연상시키는 안경 형태의 전화기

미국의 천문학자 칼 세이건과 세계적인 미래학자이자 물리학자인 미치오 카쿠는 ‘백 투 더 퓨처’를 역사상 가장 훌륭한 타임머신 영화라고 극찬한 바 있다. 영화 속 아이템이 언제쯤 전부 현실화될 수 있을지는 모르지만, 이 영화의 상상력이 지금까지 영향을 미치고 있다는 점은 매우 놀랍다. ‘백 투 더 퓨처’의 상상력에 다시 한 번 박수를 보낸다.

* 이미지 제공: 안다미로



- 백 투 더 퓨처 (Back to the Future 1 & 2)**
- 감독: 로버트 저메키스(Robert Zemeckis)
 - 출연: 마이클 J. 폭스(Michael J. Fox), 크리스토퍼 로이드(Christopher Lloyd)
 - 장르: SF / 코미디
 - 개봉: 2015년 10월 21일
 - 상영시간: 백 투 더 퓨처 1편 - 120분 / 백 투 더 퓨처 2편 - 107분
 - 등급: 12세 이상 관람가

영화 ‘백 투 더 퓨처’는 1985년에 1편, 1989년에 2편, 1990년에 3편이 개봉해 전세계적으로 큰 인기를 끌었다. 이번 재개봉은 한국을 비롯해 미국, 영국, 프랑스, 독일 등 전세계에서 동시에 진행된다. 각 국 언어로 쓴 타이틀만 빼고 포스터 이미지도 모두 같다.

안랩 박준용 수석연구원, 안드로이드 악성 앱 분석 기술 'DEVIL' 소개

안랩, 글로벌 컨퍼런스 'VB 2015'에서 모바일 보안 기술 발표

안랩이 지난 9월 30일부터 10월 2일까지 3일 동안 체코 프라하에서 열린 글로벌 보안 컨퍼런스 'VB 2015'의 초청을 받아 전세계 보안 전문가에게 시각화 기반 안드로이드 악성 앱 분석 기술 'DEVIL(Dex Visualizer)'을 발표했다.



▲ 안랩 박준용 수석연구원

안랩은 올해 행사에서 국내 보안기업 중 유일하게 초청을 받아 발표를 진행했으며, 이는 글로벌 보안 평가기관이 안랩의 모바일 보안 기술의 우수성을 인정했다는 의미다.

이번 컨퍼런스에서 안랩 분석팀의 박준용 수석연구원은 'DARE DEVIL: beyond your senses with Dex Visualizer'라는 주제로 안랩이 개발한 안드로이드 악성 앱 분석 기술 'DEVIL'을 소개했다. 이번 발표에서 박 수석연구원은 DEVIL의 작동 원리와 앱 분석 사례발표를 소개해 참석자들의 호응을 얻었다.

DEVIL(DEX Visualizer)은 안랩이 독자적으로 개발한 시각화 기반의 악성 앱 분석 기술이다. 안드로이드 앱 소스코드 내의 다양한 구성요소(component)를 세부적으로 분석해 기능, 특징, 코드 흐름, 기존 코드들과의 유사점 등을 그래프 형태로 시각화한다.

일반적으로 악성코드 분석가들은 악성 앱의 방대한 소스코드를 분석하며 앱의 악성 행위를 유추해야 한다. 이 기술을 사용하면 새로 나온 변종 악성 앱을 분석하면 짧은 시간 내에 코드의 흐름, 악성 행위 정보, 기존 악성 앱 혹은 정상 앱과 유사점/차이점 등의 정보를 시각화된 보고서 형태로 한번에 볼 수 있어 보다 빠르고 정확한 분석이 가능하다.

안랩은 지난 5월에 독일에서 열린 글로벌 보안 컨퍼런스 'CARO 2015'에서도 초청 발표로 이 기술을 소개한 바 있다.

발표를 진행한 안랩 분석팀 박준용 수석연구원은 "안랩의 앞선 모바일 보안 기술 중 하나인 DEVIL을 전세계 보안전문가에게 소개할 수 있어서 영광이다"라며 "효과적인 스마트폰 보안을 위해서는 악성 앱 분석 기술은 필수"라고 강조했다.

올해 25회째를 맞는 VB 2015는 독립 보안 평가기관인 '바이러스 블러틴(Virus Bulletin, VB)'에서 주최하는 글로벌 보안 컨퍼런스다. 행사기간 동안 안랩을 비롯한 시만텍, 인텔시큐리티(맥아피), 카스퍼스키, 트렌드마이크로 등 글로벌 보안기업의 보안 전문가의 보안 기술 및 트렌드에 대한 발표와 솔루션 전시가 이루어졌다.

Black Mine Operation Analysis Report

안랩, ‘검은 광산 작전’의 비밀을 ‘캐내다’

심장이 빠르게 뛰기 시작한다. 드디어 녀석에게 한 발짝 다가선 느낌이다. 그 녀석을 본격적으로 쫓기 시작한 것은 지난 2014년 5월. 근래 몇 년 동안 발생한 대형 해킹 공격에 이용된 수 백 개의 악성코드를 분석하다가 이들이 비슷한 유형임을 알아냈다. 이 악성코드는 특정 그룹에 의해 국내 여러 기관과 기업의 공격에 이용되었다. 그렇게 몇 개월을 추적한 결과, 이제 이 악성코드들의 연결고리이자 숨겨진 진실을 열어 줄 ‘비밀의 열쇠’를 손에 쥐는 순간이다.

BM…… BM…… BM……

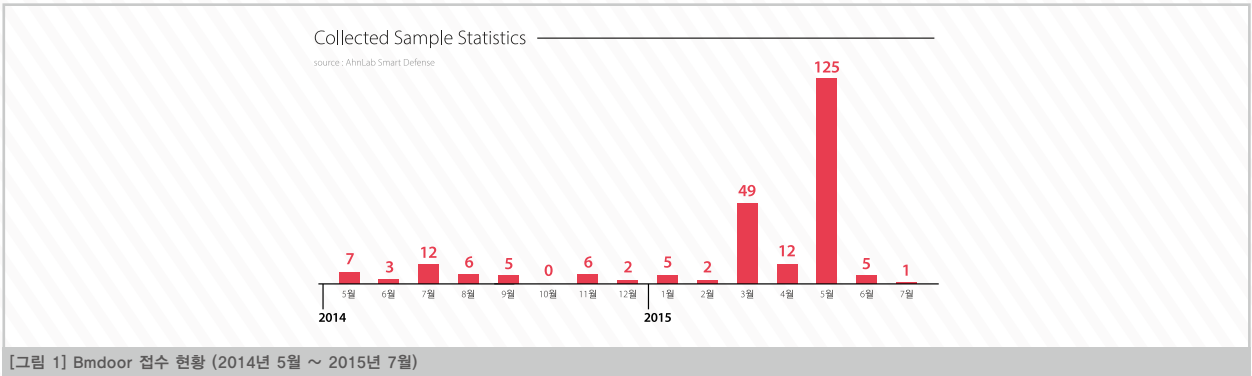
드디어 찾았다. 녀석은 정상 파일의 끝 부분, 암호화된 영역에 악성코드를 숨겨두었다. 그리고 그 영역은 특징적으로 ‘BM’ 문자열로 시작한다. 이제 악성코드 내부에 공통적으로 숨겨진 ‘BM’과 코드를 살펴보면 이 공격의 실체를 파악할 수 있게 된 것이다. 과연, 일부에서 주장하듯이 3.20 전산망 장애, 6.25 사이버 공격 등과 동일한 공격 세력일까? 또는 이들 그룹과 연관되어 있을까? 지금부터 ‘BM’ 문자열의 숨겨진 진실을 캐내기 위한 ‘검은 광산 작전(Black Mine Operation)’을 함께 추적해보자.

안랩에서는 2014년 5월부터 2015년 7월까지 1년여에 걸쳐 특정 그룹이 동일한 유형의 악성코드를 이용해 국내 여러 기관과 기업을 공격하고 있음을 파악했다. 악성코드 내부에서 공통적으로 볼 수 있는 ‘BM’과 코드를 자세히 살펴봐야 실제 기능을 파악할 수 있다는 의미에서 이 공격을 ‘검은 광산 작전(Black Mine Operation)’으로 명명했다.

이 문서에서는 검은 광산 작전의 공격 개요, 타임라인, 공격 방법 및 대상, 공격에 사용된 악성코드의 유형, 공격 추정 세력 등 5가지 항목으로 나누어 정리했다.

공격 개요

ASD(AhnLab Smart Defense) 시스템에 수집된 정보에 따르면 검은 광산 작전은 2014년 5월부터 시작되었다. 검은 광산 작전에서 기본이 되는 악성코드는 Bmdoor이며, 2014년 5월부터 2015년 7월까지 14개월 동안 총 240개 이상이 발견되었다. 특히, 2015년 3월과 2015년 5월에 많은 숫자의 Bmdoor 샘플이 수집된 것을 확인된 것으로 볼 때, 검은 광산 작전은 이 기간에 왕성한 활동을 한 것으로 유추할 수 있다.



공격자는 파워포인트 자료를 보여주는 실행 파일로 가장한 악성코드를 이용해 특정 대상을 공격한 것으로 보인다. 현재까지 안랩에서 파악한 공격 대상은 크게 한국의 에너지, 교통, 통신, 방송, IT 기업, 금융, 정치 분야 등으로 다양하다. 이외에도 공격자는 2014년 7월과 2015년 3월에는 국내 웹사이트를 해킹해 일반인을 상대로 악성코드를 퍼뜨리기도 했다.

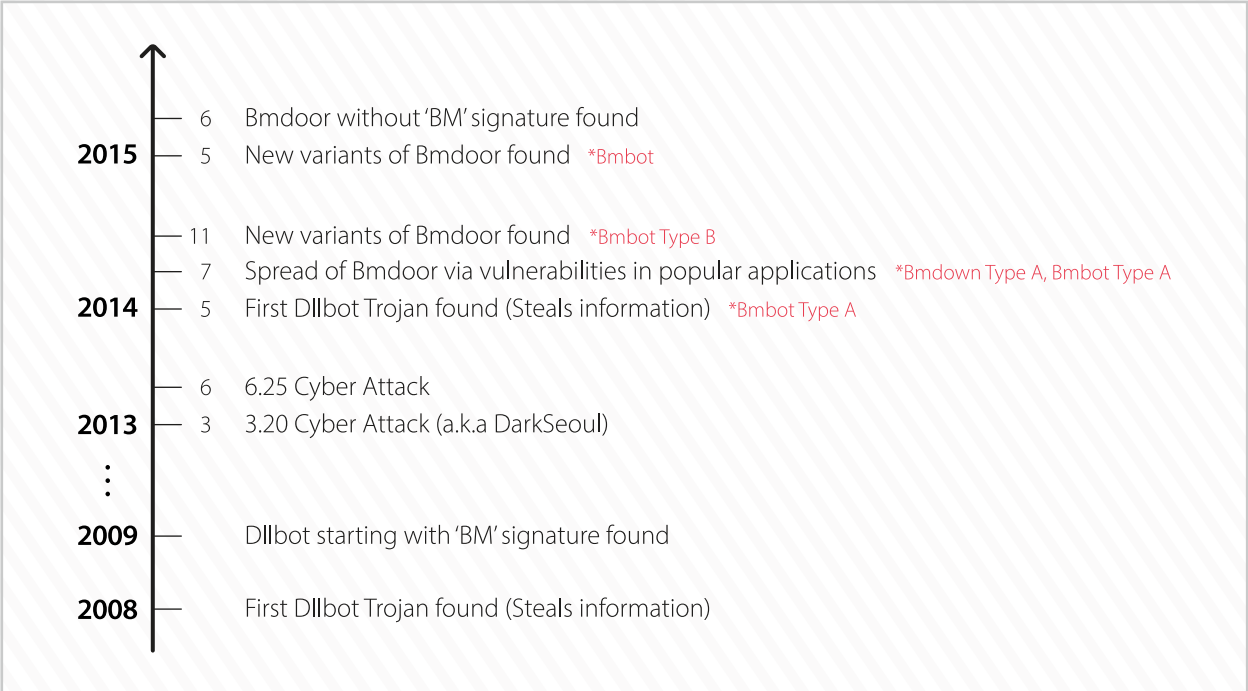
검은 광산 작전에는 다양한 악성코드가 이용되었다. 공격에 이용된 Bmdoor는 정상 실행 파일처럼 보이지만, 파일 끝부분에 암호화 되어 숨겨진 악성코드가 메모리에서 실행된다. 암호화된 영역이 ‘BM’ 문자열로 시작하는 것이 특징이며, 분석가와 자동분석 시스템을 우회하려는 기능을 포함한 경우가 많다.

Bmdoor는 공격에 사용되는 악성코드를 시스템 메모리에 올려주는 로더(Loader)로써 실행되면 암호화되어 있는 다른 악성코드를 실행시킨다. Bmdoor 내에는 공격자 서버에서 추가 악성코드 파일을 다운로드하는 다운로드더(Bmdown로 명명), 원격 제어로 정보 수집 등을 할 수 있는 봇(Bmbot으로 명명), 이미 알려진 원격 제어 툴을 이용한 형태로 크게 3가지 종류가 존재했다.

또한 지속적으로 발생하는 해당 공격에 대해 분석한 결과, 기존에 한국을 대상으로 한 대형 공격인 3.20 전산망 장애, 6.25 사이버 공격 등을 비교했을 때 검은 광산 작전을 주도한 공격 추정 세력과 이들 그룹과의 연관 가능성이 있음을 확인했다.

타임라인

Bmdoor 악성코드는 2014년 5월 최초로 발견되어 현재까지 지속적으로 그 변형이 확인되고 있다. ASD에서 2014년 5월부터 2015년 7월 까지 수집된 Bmdoor 변형은 총 240개로 아직 발견되지 않은 변형까지 고려하면 더 많은 수의 악성코드가 존재할 것으로 예상된다. 아래는 Bmdoor 악성코드와 관련 악성코드에 대한 주요 타임라인이다.



[그림 2] 검은 광산 작전 타임라인

2008년부터 특정 기관의 정보 수집을 목적으로 하는 Dllbot 악성코드가 발견된 후, 2009년에는 파일 시작이 MZ 대신 BM 시그니처로 시작하는 Dllbot이 발견되었다. 파일의 시작이 MZ가 아니면 실행되지 않지만 타 프로그램에 의해 실행될 때 MZ 시그니처로 변경되어 실행되는 것으로 확인된다.

2013년 3월 20일과 6월 25일에 각각 3.20 전산망 장애(일명 다크서울, DarkSeoul)와 6.25 정부기관 DDoS 공격이 있었다. 한국 정부 당국에서는 6.25 사이버 공격을 일으킨 그룹이 3.20 전산망 장애와 동일한 그룹이라고 추정하고 있다.

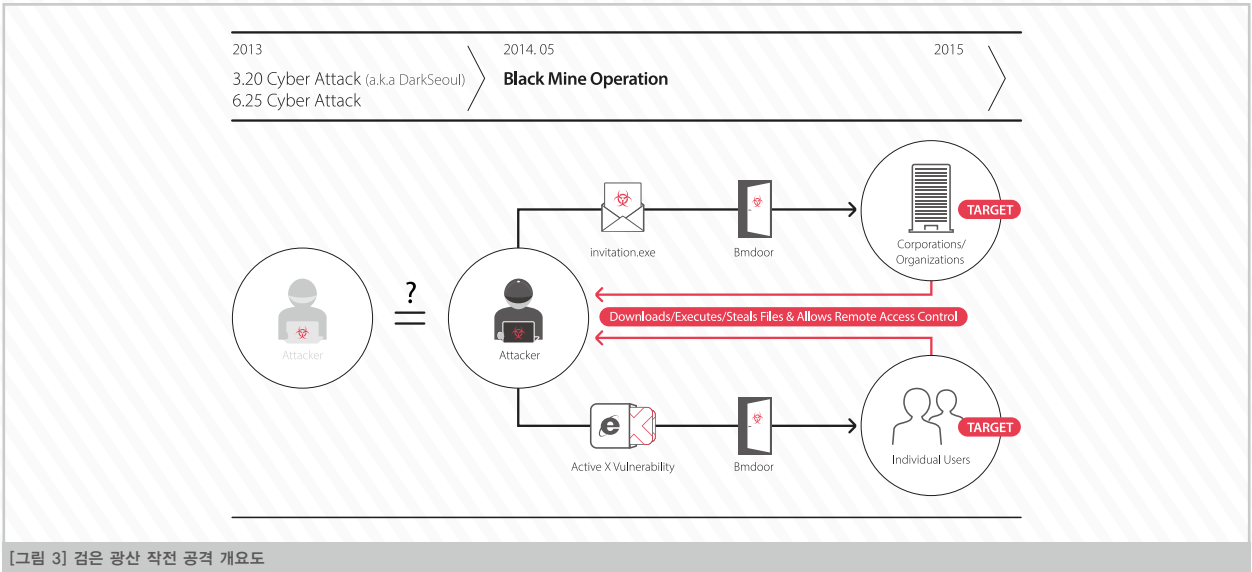
2014년 5월에는 Bmdoor로 분류하는 최초의 악성코드가 발견되었다. BM 시그니처로 시작하는 메모리 영역 내에 토르(TOR) 네트워크 상으로 통신하는 Bmbot A형 악성코드가 포함되어 있다.

2014년 7월에는 국내 주요 프로그램 및 어도비 플래시(Adobe Flash) 취약점을 이용한 Bmdoor 변형이 유포되었다. 이 기간 공격에 사용된 악성코드는 2013년 3.20 전산망 장애 때 공격에 사용된 악성코드와 유사성이 있었으며, 6.25 사이버 공격에 접속되었던 일부 IP와 동일한 점이 확인 되었다.

2014년 11월에는 주요 문자열이 암호화된 새로운 Bmbot B형이 발견되었고, 이 변형은 2015년 3월까지 공격에 이용되었다. 2015년 5월부터 새로운 Bmbot 변형이 발견되었고 2015년 6월 말 발견된 Bmdoor 변형에서는 BM 시그니처를 포함하지 않는 샘플이 확인되고 있다.

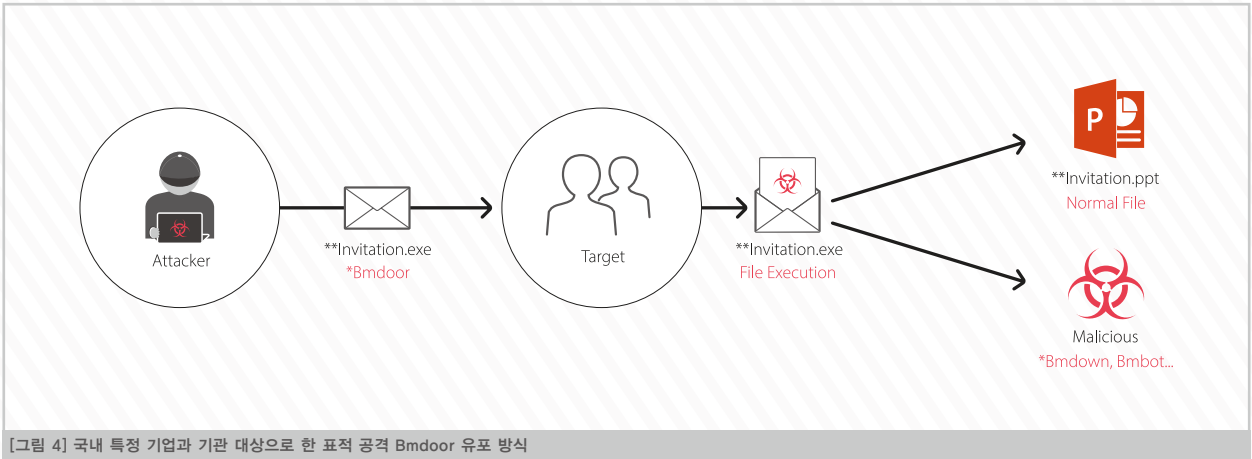
공격 방법 및 대상

공격자는 Bmdoor 악성코드를 이용하여 국내 특정 기업과 기관을 대상으로 하는 표적 공격, 그리고 일반 사용자 대상 공격을 시도하였다.



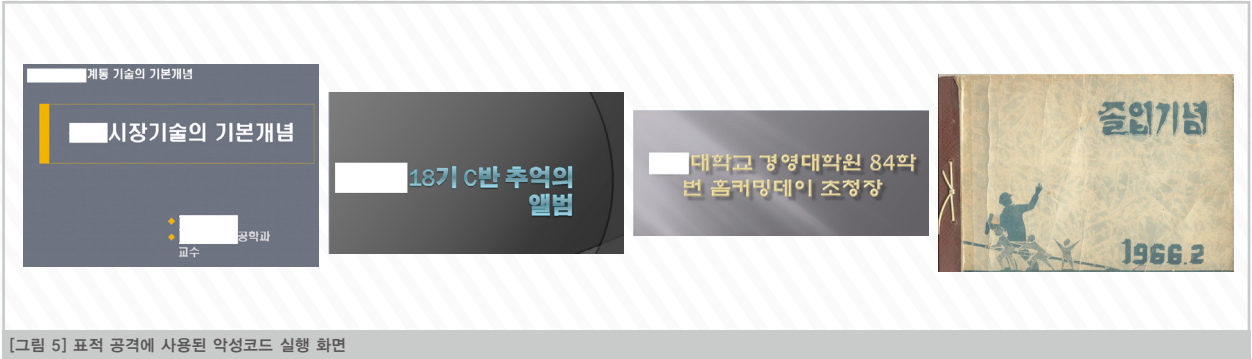
[그림 3] 검은 광산 작전 공격 개요도

먼저 기업과 기관을 대상으로 삼은 경우에는 Bmdoor 악성코드를 업무 관련 파일이나 공격 대상이 흥미롭게 생각하는 졸업 앨범, 동문회 초청장 등으로 위장하였다. Bmdoor 악성코드가 실행되면 정상적인 파워포인트 실행 화면이 나타난다. 이는 공격자가 미리 공격 대상이 열어볼 만한 주제의 파워포인트 자료를 준비한 후, 파워포인트 프로그램이 설치되지 않은 PC에서도 자료를 볼 수 있게 만들어주는 프로그램을 이용하여 만든 정상 실행 파일이다. 그리고 파워포인트 화면이 열림과 동시에 실제 악성 행위를 하는 악성코드(Bmdown, Bmbot 유형의 악성코드)도 내부에서 실행된다. 공격 대상은 아무 의심 없이 정상적으로 파워포인트 자료를 보게 되지만, 동시에 악성코드가 실행되는 것은 인지하지 못한다.



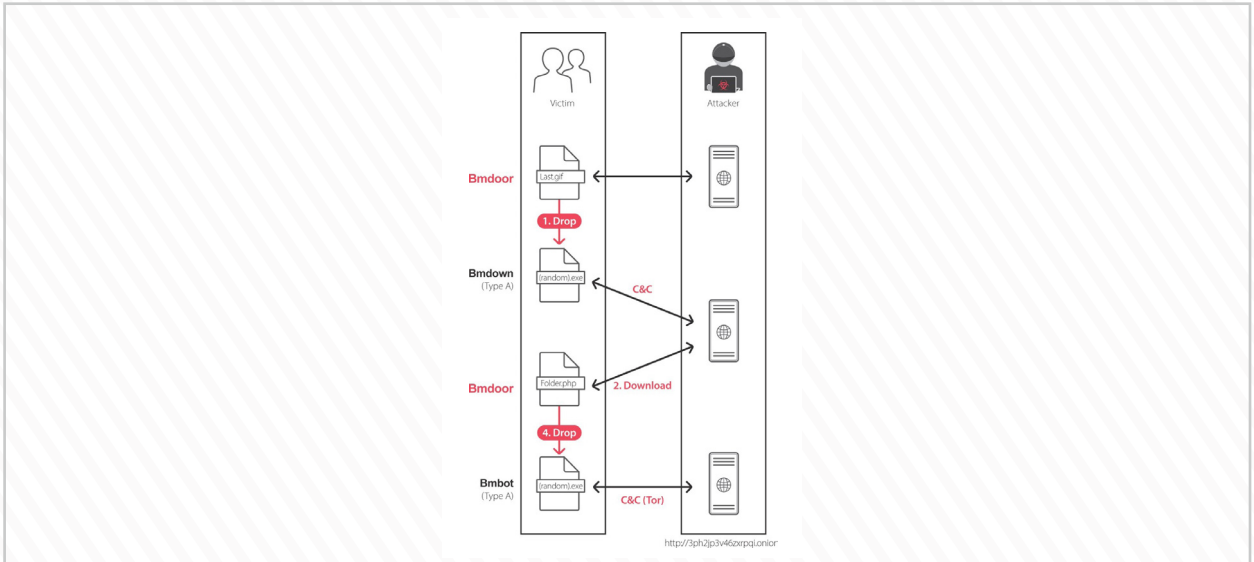
[그림 4] 국내 특정 기업과 기관 대상으로 한 표적 공격 Bmdoor 유포 방식

현재까지 감염 보고된 기관이나 기업은 에너지, 교통, 통신, 방송, IT, 금융, 정치 관련 기관 등이 있다. 아래는 표적공격으로 추정되는 Bmdoor 변형을 실행했을 때 나타나는 파워포인트 자료이다.



[그림 5] 표적 공격에 사용된 악성코드 실행 화면

반면, 국내의 일반 사용자를 대상으로 공격이 이루어진 경우에는 주로 유명 프로그램의 취약점을 통해 Bmdoor 악성코드가 유포되었다. 대표적인 예로 2014년 7월 7일 취약점을 이용하여 감염시킨 사례가 있다. 사용자가 사전에 해킹된 웹사이트에 접속 했을 때 국내에서 많이 사용되는 소프트웨어와 어도비 플래시 취약점(CVE - 2014 - 0515)을 이용해 감염시킨 것이다. 당시의 감염 방법은 [그림 6]과 같이 정리할 수 있다.



[그림 6] 취약점 이용 Bmdoor 유포 방식

사용자가 취약점을 통해 다운로드 된 Last.gif 파일을 실행되면 임의의 파일 이름을 가진 exe 파일(Bmdown A 형)이 생성된다. 이 파일은 공격자가 지정한 주소로 접속해 Folder.php를 다운로드 받아오고 이 파일은 임의의 파일 이름을 가진 실행 파일(Bmbot A 형)을 생성한 후 토르 (TOR)로 통신한다.

2015년 3월 20일에도 어도비 플래시(CVE - 2015 - 0313) 취약점을 이용해 Bmdoor 변형이 배포되었으며, 사용자 컴퓨터에 최종 감염되는 악성코드는 Bmbot B 형이다.

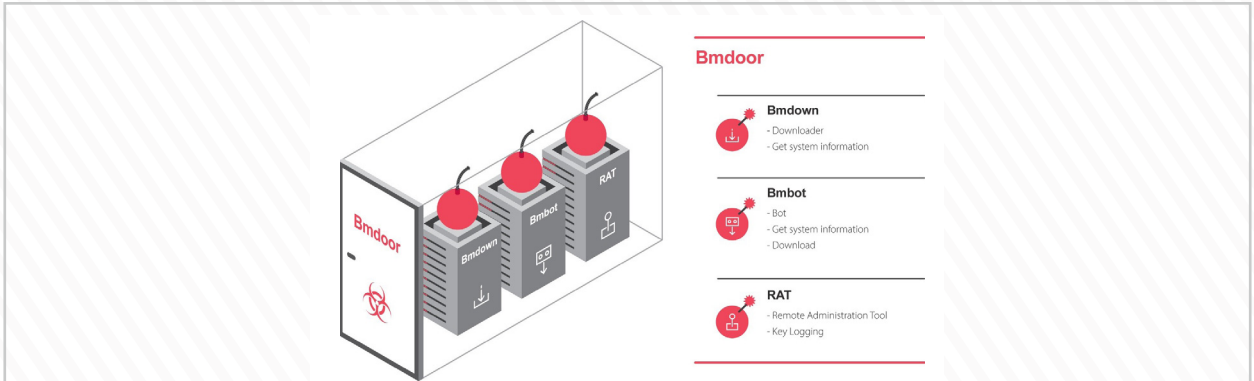
Bmdoor 악성코드 유형

Bmdoor 내에는 공격을 하기 위한 실질적인 악성 파일이 암호화 되어 숨겨져 있고, 그 종류는 크게 다음 3가지로 분류된다.

첫 번째 유형은 Bmdown이다. Bmdown에는 시스템 정보를 수집해 공격자 C&C 서버에 접속을 시도하고 수신된 명령에 따라 파일을 다운로드 하는 기능이 있다. 세부적으로 패킷의 문자열을 비교하는 Bmdown A형과 다운로드 받은 파일의 문자열을 비교하는 Bmdown B형 등으로 구분할 수 있다.

두 번째 유형은 Bmbot으로 C&C 서버와 통신을 하며 사용자 정보를 유출하는 기능이 있다. 또한 Bmdoor 내부에 가장 많이 포함되어 있다. Bmbot은 공격자와 실시간으로 통신을 하면서 실행/비실행 파일을 추가로 다운로드 받고, 내부 파일 및 PC 정보를 유출하는 핵심 악성 행위를 한다. Bmbot은 TOR 네트워크를 사용하여 암호화 된 내용을 전송하는 Bmbot A형과 내부 문자열이 최초 암호화 되어 있고 함수 진행이 될 때마다 문자열을 복구하여 파일을 실행하는 Bmbot B형이 있다.

세 번째는 RAT(Remote Administration Tool)이다. 외국에서 제작된 아리안(Aryan), 다크코멧(Darkcomet), 제나(Xena), 익스트림(Xtreme) 등의 원격 제어 도구를 이용한 유형이 있다.



[그림 7] 공격에 사용된 악성코드 종류

Bmdoor 내 악성코드를 정리하면 [표 1]과 같다.

종류	유형	특징	기능
Bmdown	Bmdown A형	패킷의 문자열 비교	지정된 서버에 접속해 추가 파일 다운로드
	Bmdown B형	다운로드 받은 파일의 문자열 비교	
Bmbot	Bmbot A형	TOR 네트워크로 사용하여 암호화된 내용 전송	추가 파일 다운로드
	Bmbot B형	내부 문자열이 최초 암호화되어 있고 함수 실행이 될 때마다 문자열을 복구하여 파일 실행	감염 시스템의 정보 유출 가능
기존 악성코드 활용	Aryan		시중에서 구할 수 있는 원격제어 프로그램 화면 캡처와 키로깅 기능이 존재하기도 함
	Darkcomet		
	Xena		
	Xtreme		

[표 1] Bmdoor 악성코드 유형

공격 추정 세력

안랩에서는 2014년 5월부터 현재까지 지속되고 있는 여러 공격에서 유사한 악성코드 찾았고 이들 악성코드가 1년 넘게 활동하고 있음을 확인 했다. 공격에 사용된 악성코드의 뚜렷한 공통점으로는 파일 후반부에 'BM'으로 시작하는 영역이 존재한다는 것이다. 그림 파일인 BMP 헤더의 시그니처와 비슷하게 보일 수도 있지만 이 영역에는 암호화된 악성코드가 저장되어 있으며 주로 내부 정보를 유출하는 백도어류 악성코드를 포함하고 있다.

안랩은 이들 공격을 검은 광산 작전으로 보았고, 과거 국내에서 발생한 대형 보안 사건을 일으킨 그룹에서 사용한 악성코드와 공격 기법 등을 비교하여, 검은 광산 작전의 공격 추정 세력과 이들 그룹과의 연관성을 검토했다.

그 결과 공격 추정 세력이 3.20 전산망 장애를 일으킨 그룹과 간접적인 연관 관계가 있을 가능성이 높다고 판단하였다. 3.20 전산망 장애를 일으킨 공격자들과 연관된 몇 가지 정황은 다음과 같다.

정황 1	BM 문자열을 포함한 여러 악성코드 발견
정황 2	Bmdoor 변형에서 2013년 3.20 전산망 장애 때 이용된 악성코드 변형 발견
정황 3	3.20 전산망 장애 그룹이 이용한 취약점 기법 유사
정황 4	Bmdoor 변형의 유포 주소와 통신 주소가 과거 악성코드의 유포 도메인과 접속 주소와 일부 동일

[표 2] 3.20 전산망 장애 발생 그룹과 관련 정황

첫째, BM 문자열을 포함한 여러 종의 3.20 전산망 장애 연관 악성코드가 발견되었다. 2009년 파일 시작 부분이 BM으로 시작하는 파일이 발견되었다. MZ로 시작하지 않아 파일은 정상 실행되지 않지만 MZ를 BM으로 변경하면 Dllbot 변형을 포함하고 있는 드롭퍼(Dropper) 파일이다. Dllbot은 2008년부터 대한민국 특정 기관의 정보를 수집하기 위해 이용된 악성코드인데, 계속 진화하여 3.20 전산망 장애 당시 사전 정보 수집용 악성코드와 Bmbot에 영향을 준 것으로 보고 있다. Dllbot과 Bmbot은 코드 관점에서는 동일한 유형이라 보기 어렵지만 둘 다 CreateFileMappingA, OpenFileMappingA API 함수를 이용해 악성코드 실행 여부 검사를 한다. 또한 C&C 서버 통신을 위해 보통 2개의 PHP 주소를 이용하며, "interval"과 "wakeup"과 같은 특정 명령어를 이용하여 C&C와 통신을 하는 것으로 보았을 때 Dllbot과 같은 범주로 볼 수 있다.

둘째, 2013년 3월 20일 발생한 3.20 전산망 장애 발생 때 공격 대상 업체에서 발견된 악성코드와 4 바이트만 다른 변형이 2014년 7월 발견된 Bmdoor 내에 포함되어 있었다. 해당 악성코드는 다른 곳에서 발견되지 않아서 제작자만 보유하고 있을 가능성이 높다. 동일 그룹이 아니라고 해도 3.20 전산망 장애 그룹과 적어도 교류하거나 협력 관계로 추정할 수 있는 근거가 된다.

셋째, 2014년 7월 7일 Bmdoor 변형을 배포할 때 이용한 취약점은 주로 국내 프로그램의 취약점으로 3.20 전산망 장애 때 이용된 취약점과 유사하다. 3.20 전산망 장애를 일으킨 악성코드는 2013년 3월 20일 전에 국내에서 널리 사용되는 프로그램의 취약점을 통해 감염된 것으로 알려졌다.

넷째, 2014년 7월 7일 배포된 Bmdoor 변형의 배포 주소와 통신 주소가 2013년 6월 25일 발생한 6.25 사이버공격에 이용된 악성코드의 배포 도메인과 접속 주소와 일부 동일했다.

결론

검은 광산 작전(Black Mine Operation)을 진행하고 있는 이들은 다양한 Bmdoor를 제작해 국내 여러 기관과 기업에 대한 공격을 일년 넘게 수행하고 있다. 게다가 분석가와 분석 시스템을 회피하려는 시도를 보면 앞으로 더 은밀하게 작전을 수행할 것으로 예상된다.

공격 방식과 악성코드를 분석했을 때 3.20 전산망 장애를 일으킨 그룹과의 명백한 관계를 증명할 수 없지만 적어도 간접적으로 연관 관계가 있을 가능성이 높다.

지난 10년 동안 대한민국의 주요 기관과 기업에 대한 공격을 지속적으로 공격하는 세력은 분명히 존재한다. 이런 공격에 대비하기 위해서 주요 기관과 기업은 내부로 유입되는 파일에 대한 분석 역량을 강화하고 보안업체와 유관 기관과 협력을 강화해야 할 것으로 보인다.

안랩의 MDS와 V3 제품군에서는 검은 광산 작전에 이용된 악성코드에 대해 진단하고 치료 기능을 제공하고 있다.

- 지능형 위협대응 솔루션 AhnLab MDS 진단명: Malware/MDP.Drop 등
 - 엔드포인트 보안 솔루션 AhnLab V3 진단명: Win-Trojan/Bmdoor.Gen, Trojan/Win32.Bmbot, Trojan/Win32.Bmdown 등

‘여신전문금융업법’ 개정안의 POS 단말기 보안과 AhnLab EPS

새 POS 단말기만 설치하면 보안 걱정 끝?

올해 1월 개정된 여신전문금융업법이 지난 7월 21일 시행되었다. ‘여신전문금융업법(이하 여전법)’이란 대출, 할부, 신용카드 등 여신 전문금융업을 관리·감독하기 위해 제정된 법률로, 1997년 제정 당시 다른 금융업에 대해서는 등록제로 운영하되 지급결제기능을 가진 신용카드업의 경우에만 신용질서의 유지를 위하여 ‘허가제’로 유지되었다. 올해 이 여전법이 개정, 시행되면서 ‘신용카드 단말기의 등록 제도’를 도입하고 신용정보보호 및 결제의 안전성이 담보되는 신용카드 단말기만 사용할 수 있게 되었다(제19조제3항 및 제27조의4 신설). 편의점에서 소액 결제 시에도 신용카드를 이용하는 요즘, 여전법의 개정이 경제 전반에 미칠 파장이 적지 않을 것으로 보인다. 이 글에서는 여전법 개정으로 영향을 받는 업체들은 어떤 업체들이며, 신용카드 결제와 관련해 이들 업체가 고려해야 할 것은 무엇인지 상세히 알아본다.

먼저 여전법이 개정된 배경을 살펴보자. 수년 전부터 마그네틱 신용카드의 정보를 탈취해 불법으로 신용카드를 복제 및 결제하는 사례가 잇따르자 각국 정부에서는 마그네틱 신용카드 대신 IC카드로의 전환을 서두르고 있다. 우리나라도 지난 2004년부터 장기적인 계획으로 IC카드 전환을 추진하였으며, 현재 약 98.9% 가량 IC카드 전환이 진행된 것으로 알려져 있다.

이처럼 대부분의 신용카드는 IC카드로 전환되었지만 정작 이를 이용한 IC 거래는 활성화되지 못하고 있다. IC카드 결제가 가능한 단말기, 즉 신규 POS 단말기 등 기반 인프라가 미처 갖춰지지 않았기 때문이다. 특히 관련 기술의 기준이 정립되지 않았다는 것이 가장 큰 걸림돌이었다. 이에 여신금융협회는 지난 4월 말 ‘신용카드 단말기 정보보호 기술기준’을 발표했다. 이어 7월에는 금융감독원(이하 금감원)이 ▲물리적 해킹 시도 시 POS 단말기 메모리 자동 파괴 ▲정보 유출 차단을 위한 엔드투엔드(END-TO-END) 방식의 전체 암호화 등을 골자로 하는 ‘POS단말기 보안표준 규격안’을 발표했다.

또한 금감원은 여신금융협회와 함께 여전법을 개정해 신용카드 결제 대행업체(VALUE ADDED NETWORK, 이하 VAN) 등록제를 도입했다. 이에 따라 지난 7월 21일부터 신규 가맹점 및 신규 POS 단말기 설치 시 보안표준에 따라 제작되어 인증에 통과한 단말기만 설치 및 사용해야 하며, 이를 어길 시 VAN사와 가맹점에 5천만원 이하의 과징금이 부과된다.

여신전문금융업법 개정안

〈제19조 제3항〉

- ③ 신용카드가맹점은 신용카드회원의 정보보호를 위하여 금융위원회에 등록된 신용카드 단말기를 설치·이용하여야 한다.

〈제27조의4 (신용카드 단말기의 등록)〉

- ① 부가통신업자는 자신이 전기통신서비스를 제공하는 신용카드 단말기를 금융위원회에 등록하여야 한다. 다만, 부가통신업자가 전기통신서비스를 제공하지 아니하는 신용카드 단말기의 경우에는 신용카드가맹점이 금융위원회에 등록하여야 한다.
- ② 등록하려는 신용카드 단말기는 신용카드회원의 정보보호를 위하여 금융위원회가 정하는 기술기준에 적합하여야 한다.

(중략)

- ④ 금융위원회는 제1항 및 제2항에 따른 신용카드 단말기의 등록 및 기술기준에 관한 업무를 여신전문금융업협회장에게 위탁한다.

비용 부담 등 신규 POS 단말기 교체 쉽지 않아

금감원이 여신금융협회에 신용카드 단말기, 즉 POS 단말기의 등록 및 기술 기준에 대한 업무를 위탁함에 따라 VAN사, 카드리더기 제조업체 등 POS 단말기 개발 및 운영 주체들은 단말기를 개발하여 여신금융협회에 시험 및 인증을 신청해야 한다. 여신금융협회는 테스트를 통과한 POS 단말기 및 업체에 대해 인증서를 발급하며 홈페이지에 등록정보를 공개한다(<https://www.crefia.or.kr/> → 가맹점 → 신용카드 단말기 등록정보). 여신금융협회 홈페이지에 따르면 2015년 9월 현재 149개의 단말기가 등록되어 있다.

순번	단말기종류	연속번호	단말기식별번호	개발사	모델명	버전	신형기준	인증일자	만료일자
149	POS	2015-107-P1	###N-512011001	###자금융주사..	###1201	1001	###	2015.09.16	2020.09.15
148	카드리더기	2015-105-R1	D633KALOTR01L101	###클리어	DA	###OTR01 L101	###	2015.09.15	2020.09.14
147	POS	2015-106-P1	LTSUPERPOS015550	###광명정보대우.. LT	###RPOS01 5550	###	###	2015.09.15	2020.09.14
146	CAT	2015-105-C1	###N-1300M1001	###북경정보통신	###300M	1001	###	2015.09.15	2020.09.14
145	CAT	2015-104-C1	###N-14011001	###정보통신	###401	1001	###	2015.09.15	2020.09.14
144	CAT	2015-103-C1	###N-CP-21001001	###이력사건..	###2100	1001	###	2015.09.14	2020.09.13
143	CAT	2015-102-C1	###N-21301001	###정보통신	###2130	1001	###	2015.09.10	2020.09.09
142	CAT	2015-101-C1	###N-MS-2330001	###정보통신	###233	0001	###	2015.09.09	2020.09.08
141	CAT	2015-100-C1	###N-KTC58001116	###	###5800	1116	###	2015.09.07	2020.09.06
140	CAT	2015-099-C1	###N-MS-2234001	###정보통신	###223	H001	###	2015.09.02	2020.09.01

[그림 1] 여신금융협회에 등록된 신용카드 단말기

문제는 여신금융협회에 등록된 신규 POS 단말기로 교체하기에는 POS를 사용하는 업체들, 즉 카드 가맹점들의 비용 부담이 만만치 않다는 점이다. 기존 가맹점들의 POS 단말기에 대해 3년의 유효기간을 두고 신규 단말기로 교체할 것을 유도하고 있기는 하지만 여신금융협회에 인증 받은 VAN사의 신규 단말기 공급 물량이 부족하다는 지적도 있다.

소매업, 숙박업, 음식점도 개정안 적용 대상

여전법에 영향을 받는 업체는 신용카드업, 시설대여업, 할부금융업 또는 신기술사업금융업 등 여신전문금융업체들로, 특히 이번 여전법 개정과 관련이 있는 부분은 ‘신용카드업’이다. 직접적으로는 신용카드사 등이 적용 대상이지만, 신용카드가맹점의 준수사항(제19조) 등이 포함되어 있어 신용카드결제 기능이 있는 POS 단말기 등을 사용하는 소매업, 숙박업, 음식점 및 주점 등의 업종에 속하는 사업자 역시 여전법의 적용 대상이다.

즉, 신용카드 결제를 위해 POS 기기를 사용하는 일반 소매업체나 숙박업체, 일반 음식점 및 주점에서는 여전법 개정 시행일인 2015년 7월 21일로부터 3년(유효기간) 내에 여신금융협회에 등록된 신규 POS 단말기를 도입하여 운영하면 된다. 단, 유효기간 내라도 POS 단말기를 신규로 추가 설치하거나 단말기의 고장 등 기타 사유로 인하여 POS 단말기를 교체해야 할 경우에는 등록된 단말기를 설치 및 이용해야 한다.

한편 일반적으로 POS 단말기를 등록해야 하는 의무는 VAN사에게 있지만 VAN사에서 제공 및 관리하는 단말기가 아니라면 카드 가맹점이 직접 여신금융협회를 통해 단말기를 등록해야만 한다.

〈제27조의4(신용카드 단말기의 등록)〉

- 부가통신업자가 전기통신서비스를 제공하지 아니하는 신용카드 단말기의 경우에는 신용카드가맹점이 금융위원회에 등록하여야 한다.

또한 등록된 신용카드 단말기를 설치·이용 의무 위반에 관하여 500만원 이하의 과태료를 부과(제72조)하는 것은 물론, “신용카드가맹점과 체결한 가맹점 계약을 해지하여야 한다(제6조의17)”고 정하고 있다. 카드 단말기가 사업의 존망에 심각한 영향을 가져올 수 있어 업종을 불문하고 사업주들의 카드 결제 단말기에 대한 대책 마련이 시급하다.

여전법 개정과 POS 교체, 우선 순위는?

그런데 과연 신규 POS 단말기로 교체만 하면 보안 문제가 해결될 수 있을까? 꼭 그렇지만은 않을 것으로 보인다.

우선 보호해야 할 ‘정보’의 관점에서 법의 적용 범위가 ‘신용카드(체크카드 및 선불카드 포함) 정보’로 한정되어 있다는 것에 주목할 필요가 있다. 실제 POS 단말기에는 지불 소프트웨어 프로그램에서 처리하는 신용카드 결제 정보 외에도 포인트 카드, 쿠폰, 판매 정보 등이 처리되며 그 처리 과정 중에 발생하는 로그 데이터 등과 같은 기타 정보들이 존재한다.

또한 환경적인 관점에서 살펴보면, 가맹점에서 사용하는 POS 단말기마다 운영체제의 버전이 다르거나 패치 적용 수준이 다르거나 실행되는 프로세스가 조금씩 다르게 운영되는 경우가 적지 않다. POS 단말기 운영 과정 중 발생하는 형상변경 등에 따른 보안 수준의 약화가 발생 역시 POS 보안과 관련해 반드시 고려해야 할 부분이다. 만일 다수의 단말기 중 보안 수준이 낮은 단말기가 한 대라도 있다면 이를 통해 보안 침해가 발생할 수 있다는 것을 유념해야 한다.

이처럼 법 개정에 따른 POS 단말기 교체로 단일 단말기의 보안 수준이 높아질 것은 분명하지만, 실제 운영 상에서 지속적으로 안전한 상태로 운영될 수 있도록 하는 ‘관리’ 문제가 여전히 고민으로 남게 된다. 즉, 신규 POS 단말기를 기반으로 한 운영 환경에 대한 관리 방안 마련이 필요한 시점이다.

AhnLab EPS, 악성코드 차단부터 통합 관리까지

안랩은 최근 증가하고 있는 POS 시스템 해킹 및 POS 악성코드 대응을 위해 화이트리스트 기반의 초경량 솔루션인 AhnLab EPS(Endpoint Protection System)를 제공하고 있다. AhnLab EPS는 안정적 운용에 대한 민감도가 높고 정해진 프로그램만 사용하는 POS 단말기에 최적화된 보안 솔루션으로, 강력한 악성코드 억제 및 보안 성능을 제공한다.

AhnLab EPS는 전문적인 보안 지식 없이도 운용이 가능하며, 쉽고 간편한 중앙 관리를 통해 가맹점의 운용 부담이 적다는 점이 장점이다. 대시보드를 통해 EPS 에이전트가 설치되지 않은 시스템을 확인하는 등 전체 POS 단말기를 쉽고 편리하게 통합 관리할 수 있다. 특히 ‘원격 제어’ 기능을 통해 즉각적으로 개별 POS 단말기에 대한 조치도 가능하다.



[그림 2] AhnLab EPS 대시보드

앞서 살펴본 바와 같이 일반 가맹점이 신규 POS 장비를 도입했다 하더라도 보안 관리 방안을 마련할 필요가 있다. 예를 들어 등록된 신규 단말기를 도입하더라도 신용카드 정보 외에 단말기에서 처리되는 다양한 정보의 기밀성·무결성을 보호하는 한편 POS 단말기 자체의 가용성도 보호해야 한다. 특히 관리적 요구사항 중에서 '초기 단말기 제공업체에서 기본 보안 설정을 구성하도록' 하고 있으나, 이후 실제 운영하는 동안 초기 구성이 유지될 수 있도록 관리 및 통제가 필요하다. 게다가 현재 관련 법규에서 지정한 보안 기준은 대부분 알려진 위협에 대응하기 위한 것으로, 최근 증가하고 있는 알려지지 않은 위협에 대한 대책 마련이 필요하다.

AhnLab EPS는 강력한 락다운(Lockdown) 기능으로 POS 시스템 운용에 필요 없는 애플리케이션 및 시스템 기능과 매체·네트워크 연

결 통제 기술을 통해 모든 POS 시스템이 외부의 공격과 알려지지 않은 위협으로부터 항상 안전하게 유지할 수 있게 해준다. 또한 독자적인 화이트리스트(Whitelist) 기술을 통해 단말기 상에서 POS 프로그램 외에 기타 불필요한 프로그램이 실행되는 것을 차단하고 네트워크 등을 통한 악성코드의 유입 및 확산을 억제한다.

AhnLab EPS는 비즈니스 운용에 영향 없이 악성코드 차단과 통제가 가능하며, 보안에 관한 전문적인 지식이 없더라도 편리하게 중앙 관리가 가능해 대형 리테일 업체부터 중소 규모의 가맹점까지 POS 단말기 보안 및 생산성 향상과 운용 비용 절감에 기여한다.

〈참고 문서〉

[1]국가법령정보센터, 「여신전문금융업법」 및 관련법령, 2015.1.20.
[2]여신금융협회, 「신용카드 단말기 정보보호 기술기준」, 2015.4.29.
[3]여신금융협회, 「신용카드 단말기 보안강화 방안 관련 Q&A」, 2015.5.13.

PDF 문서를 이용한 악성코드 유포 및 예방법

겹겹이 위장한 PDF 파일, 기업 내부를 노린다

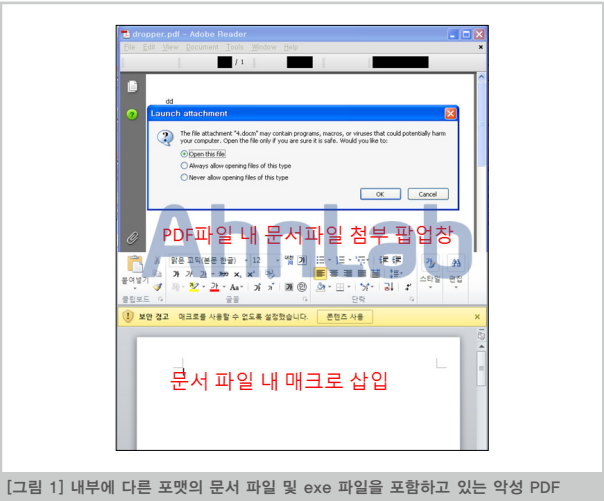
A씨는 거래처 영업대표로부터 이메일을 받았다. 메일 제목을 보니 이번 달 제품 단가에 대한 업데이트 문서를 첨부한 것 같다. 매달 비슷한 내용의 메일을 받기 때문에 별다른 의심 없이 메일에 첨부된 PDF 파일을 열었다. 그런데 PDF 문서 안에는 dd라는 두 글자만 쓰여 있을 뿐이고 다시 첨부 파일을 열라는 팝업창이 나타났다. '문서 포맷이 바뀐 건가?'라고 생각하며 팝업창의 OK 버튼을 눌렀다. 그러자 워드 파일이 열리며 문서가 표시되는데, 역시 아무 내용이 없다. 그리고는 문서 상단에 '매크로를 실행할 수 없다'는 표시가 나타났다. 무슨 문서를 이렇게 복잡하게도 만들었나 싶었지만 어쨌든 그 매크로란 것을 실행했다. 그런데 또다시 아무 내용도 안 보인다. 순간 짜증이 났지만 나중에 업체에 연락해야겠다고 생각하며 그 문서를 닫고 다른 업무를 처리했다.

그날 오후, 다른 거래처에 거래 대금을 송금하기 위해 A씨가 인터넷 뱅킹 사이트에 접속하자 보안카드 번호 전체를 입력하라는 팝업창이 나타났다. 뭔가 느낌이 좋지 않다.

최근 악성 PDF 파일을 이용한 공격 사례가 잇따르고 있다. 특히 업무 내용으로 위장한 이메일 첨부 파일 형태로 유포되고 있어 더욱 주의가 요구된다.

앞서 언급한 사례는 거래처 영업대표의 이메일 계정이 탈취되어 주소록에 포함된 사람들에게 악성 PDF 파일을 첨부한 이메일이 전송된 사례를 재구성한 것이다. 그나마 위의 사례에서는 의심 징후를 찾아볼 수 있다.

우선 PDF 문서에 아무 내용이 없었던 점도 이상하지만 ▲PDF 파일에 MS 워드 문서가 내장되어 있다는 점 ▲MS 워드 파일에도 아무 내용이 없고 매크로가 포함되어 있다는 점 등은 의심해볼 필요가 있다. 그러나 대다수의 공격에서는 위와 같은 징후를 알아차리기 쉽지 않다. 위의 사례를 중심으로 PDF 파일을 이용한 최신 공격 방식을 상세히 살펴보고 예방법은 없는지 알아본다.



[그림 1] 내부에 다른 포맷의 문서 파일 및 exe 파일을 포함하고 있는 악성 PDF

사용자가 많은 기업의 경우에는 ‘액티브 디렉터리’를 통해 다음과 같은 레지스트리 값을 배포하는 것도 방법이다.

[레지스트리 설정 가이드]

- 경로: HKLM\SOFTWARE\Policies\Adobe\<product name>\<version>\FeatureLockDown\cDefaultLaunchAttachmentPerms
- 레지스트리 명: tBuiltInPermList
- 레지스트리 값

```
version:1|.ade:3|.adp:3|.app:3|.arc:3|.arj:3|.asp:3|.bas:3|.bat:3|.bz:3|.bz2:3|.cab:3|.chm:3|.class:3|.cmd:3|.com:3|.command:3|.cpl:3|.crt:3|.csh:3|.desktop:3|.dll:3|.exe:3|.fxp:3|.gz:3|.hex:3|.http:3|.hqx:3|.hta:3|.inf:3|.ini:3|.ins:3|.isp:3|.its:3|.job:3|.js:3|.jse:3|.ksh:3|.lnk:3|.lzh:3|.mad:3|.maf:3|.mag:3|.mam:3|.maq:3|.mar:3|.mas:3|.mat:3|.mau:3|.mav:3|.maw:3|.mda:3|.mdb:3|.mde:3|.mdt:3|.mdw:3|.mdz:3|.msc:3|.msi:3|.msp:3|.mst:3|.ocx:3|.ops:3|.pcd:3|.pi:3|.pif:3|.prf:3|.prg:3|.pst:3|.rar:3|.reg:3|.scf:3|.scr:3|.sct:3|.sea:3|.shb:3|.shs:3|.sit:3|.tar:3|.taz:3|.tgz:3|.tmp:3|.url:3|.vb:3|.vbe:3|.vbs:3|.vsmacros:3|.vss:3|.vst:3|.vsw:3|.webloc:3|.ws:3|.wsc:3|.wsf:3|.wsh:3|.z:3|.zip:3|.zlo:3|.zoo:3|.pdf:2|.fdf:2|.jar:3|.pkg:3|.tool:3|.term:3
```



[그림 8] 레지스트리 설정

단, 어도비 리더의 메뉴를 통해 ‘첨부 파일을 외부 응용 프로그램으로 열기 허용’을 해제하면 생성되는 값이 많은 파일 유형을 포함하기 때문에 주의가 필요하다.

PDF 등 문서 파일 이용한 지능형 공격 증가 추세

위와 같은 방법을 통해 파일 내부에 다른 파일을 숨기고 있는 PDF 파일에 대해서는 대응이 가능하다. 문제는 공격자들이 이러한 악성 파일을 기업 내부로 침투시키기 위해 사회공학기법, 스피어피싱 등 교묘하고 다양한 공격 방법을 끊임없이 만들어낸다는 점이다. 앞서 언급한 사례처럼 업무와 관련된 내용 또는 업무 관계자의 계정으로 위장한 경우라면 아무리 보안 의식이 뛰어난 사람이라 해도 의심하기 어려운 것이 사실이다.

실제로 사회공학기법과 PDF, 워드 등 문서 파일을 이용해 기업 내부를 노리는 지능형 위협이 지속적으로 증가하는 추세다. 이에 추가 보안 솔루션 도입 등 지능형 위협 대응 방안을 마련하기 위해 고민하는 기업이 늘고 있다. 그러나 솔루션 도입에 앞서 조직원 하나하나가 기본 보안 수칙을 철저히 준수하고 의심스러운 파일이 열려봤을 경우 보안 관리자에 즉시 문의하게 하는 등 기업 내 보안 의식을 강화하는 것이 중요하다.

AhnLab ISF SQUARE 2015 in Gwangju and Daejeon

안랩, 광주와 대전으로 ‘고객 만나러 갑니다’

안랩은 ‘고객 주도형 보안(Customer driven Security)’ 전략의 일환으로 고객을 찾아가 특성과 요구를 듣고 이에 최적화된 해결책 (Resolution)을 고객과 함께 마련하는 AhnLab ISF(Integration Security Fair) SQUARE 2015를 진행하고 있다. 지난 6월 증권업계를 시작으로 은행, 건설업계 등 다양한 산업군의 고객을 만나는 자리를 가졌다. 뿐만 아니라 8월 전주를 시작으로 9월 부산에 이어 10월에는 광주와 대전 등의 지역 고객을 찾아가 다양한 환경에서 발생할 수 있는 보안 위협과 대응 방안을 제시했다.

지난 10월 20일과 21일, 광주와 대전 고객과 함께 한 ‘AhnLab ISF 스퀘어 2015’의 현장 모습을 소개한다.

안랩은 지난 10월 20일 광주에서 공공 및 교육기관의 정보보호 담당자를 대상으로 보안 세미나를 개최했다. 이 세미나에서는 ▲사례로 살펴본 악성코드 동향과 대응 방안 ▲진화하는 보안 위협에 대한 대응 방안 ▲보안 트렌드 변화에 따른 엔드포인트의 방향성 ▲Active X 제거 동향 및 대응 방안에 대한 안랩 보안 전문가들의 강연이 진행되었다.

특히, 안랩 글로벌기술지원팀 정광우 책임은 랜섬웨어 등 진화하는 보안 위협과 이에 대한 대응 기술을 소개하고, 고객사별 다양한 환경에서의 실제 구축 사례를 보여줌으로써 고객들의 큰 호응을 얻었다.



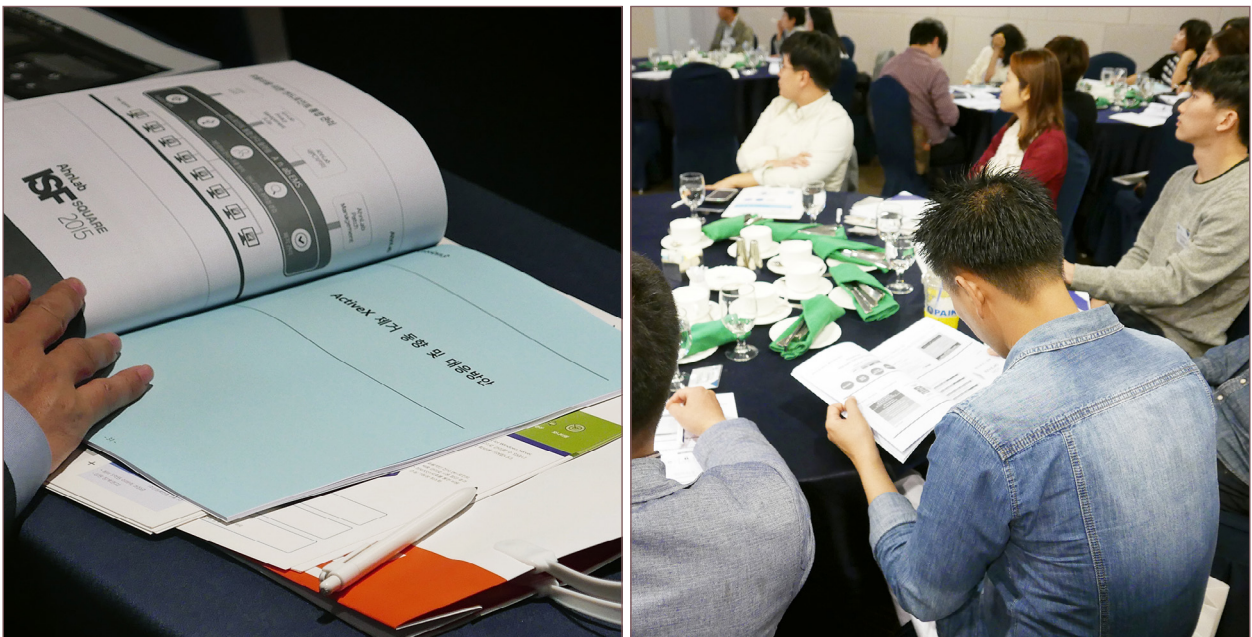
▲ ‘안랩 ISF 스퀘어 2015 광주’ 현장(좌)에서 진화하는 보안 위협에 대해 설명 중인 안랩 글로벌기술지원팀 정광우 책임(우)

안랩은 10월 21에는 대전 지역의 정보보호 책임자 및 담당자를 초청해 최신 보안 트렌드와 대응 방안을 소개하는 '안랩 ISF 스퀘어 2015 대전'을 개최했다. 이 행사에는 대전의 공공 및 교육, 의료기관 정보보호 담당자 50여 명이 참석했으며, 이들은 안랩 보안 담당자들과 IT 환경 변화에 따른 보안 위협과 대책은 무엇인지에 대해 의견을 나누는 자리를 가졌다.



▲ '안랩 ISF 스퀘어 2015 대전' 현장(좌)에서 엔드포인트 보안 전략을 발표 중인 안랩 제품기획팀 이건용 과장(우)

안랩 제품기획팀 이건용 과장은 “엔드포인트는 금전적·정치적인 목적으로 악용할 수 있는 유용한 정보가 가득하고 다양한 접근 경로가 존재하기 때문에 공격자에게 매력적인 먹잇감인 반면 방어자 측면에서는 많은 엔드포인트 보안 제품이 존재함에도 불구하고 여전히 보안 대책을 수립하기 어렵다”고 설명했다. 이어 그는 “엔드포인트 보안을 강화하기 위해서는 사용자 관점에서의 쉬운 보안, 보안 관리자 관점에서의 가시성을 확보할 수 있는 방안이 필요하다”고 강조했다.



▲ 안랩 ISF 스퀘어 2015 광주·대전 행사에 참석한 고객들은 최신 보안 트렌드와 대응 방안에 대해 함께 공유하는 자리를 가졌다.

안랩 ISF 스퀘어 2015는 다양한 지역과 산업군의 고객의 찾아가 '맞춤형 보안 전략과 솔루션'을 제공하는 방식으로 진행되고 있다. 특히, 서울에 비해 상대적으로 보안 관련 세미나를 접하기 쉽지 않은 지역 고객에게 사물인터넷과 핀테크, Active X 제거 동향, 랜섬웨어 대응 방안 등 다양한 최신 보안 트렌드를 소개하고, 안랩의 보안 전문가들의 이러한 궁금증의 해결할 수 있는 자리가 되고 있다.

이날 세미나에 참석한 한 고객은 “서울과 대전이 그리 먼 거리는 아니지만 세미나 참석을 위해 출장가야 하는 것에 부담이 있었다. 오전에 근무하고 오후에 세미나 참석하니 하루를 알차게 보낸 느낌”이라며 “대전에 자주 찾아와 달라”고 요청했다. 또 다른 고객은 개인 정보보호법 준수를 위한 보안 솔루션 소개가 없어 아쉬웠다고 다음 번에는 개인정보보호 관련된 내용을 포함해 달라고 당부하기도 했다.



▲ 안랩 ISF 스퀘어 2015 광주·대전 행사에 참석한 고객들은 현장에서 안랩의 제품과 보안 트렌드에 대한 궁금증을 해결했다.

이번 ‘안랩 ISF 스퀘어 2015 광주·대전’ 행사에서는 지능형 위협 대응 솔루션인 ‘안랩 MDS’, PC 취약점 점검 솔루션인 ‘안랩 내PC지킴이’ 등이 전시되어, 고객들이 이들 제품을 직접 경험할 수 있는 기회가 제공되었다. 특히 이번 행사는 안랩의 총판과 지역 파트너가 주최한 행사로, 고객 만족을 실현하기 위해 안랩과 파트너사가 협력한 사례로서 그 의미가 크다.

안랩은 앞으로도 보안에 있어서 진정한 해결책(Resolution)을 제공하기 위해 고객을 찾아가 다양한 목소리를 듣고 함께 논의하는 고객과의 소통을 지속할 계획이다.

일상 생활에서 무심코 지나치는 개인정보 노출

최근 몇 년 간 대규모 개인정보 유출 사건이 잇따라 발생하고 있다. “우리나라 국민 대다수는 개인정보 유출에 무감각해질 정도”라는 말도 과언이 아니다. 그런데 개인정보가 인터넷뿐만 아니라 우리의 일상 생활에서, 그것도 정작 우리 자신에 의해 노출되고 있다면? 우리가 미처 신경 쓰지 못하고 일상 생활 중에 노출하고 있는 개인정보는 어떤 것이 있는지 돌아보자.

우리가 인지하지 못하고 있을 뿐 우리의 개인정보는 일상생활 속에서, 그것도 우리 자신의 무관심 속에서 노출되고 있다. 업체의 관리 부주의로 인해 개인정보가 유출된 것이라면 남 탓이라도 할 수 있지만 내 스스로 지키지 못해 노출된 것이라면 누구를 탓할 수도 없는 노릇이다.

1. 택배 상자와 함께 버려지는 개인정보

인터넷을 통한 전자상거래가 활성화됨에 따라 택배 서비스 또한 급증했다. 택배에는 ‘송장’이라고 불리는 발송자와 수신자의 정보가 기록된 문서가 부착되어 있다. 이러한 송장에 기입되는 내용은 대개 이름(또는 업체명), 주소, 연락처, 발송 일자, 물건의 배달 경로 등이다.

많은 사람들이 택배로 상품을 받으면 택배 상자에 붙어있는 송장을 제거하지 않고 그대로 버리는 경우가 많다. 실제로 재활용쓰레기 수거장에서 이름과 전화번호 등 개인정보가 그대로 표시되어 있는 송장이 제거되지 않은 택배 상자들을 흔히 볼 수 있다. 송장에 기록된 정보들은 가장 최근까지 사용된, 즉 생생하게 살아있는 개인정보일 가능성이 높다. 게다가 송장에는 구매한 제품이 기입되어 있는 경우도 많다. 대수롭지 않은 부분일 수도 있지만 개인의 취향 등 사생활의 일부가 노출되는 것으로 볼 수도 있다.

전설적인 해커로 불리는 케빈 미트닉(Kevin Mitnick)은 자서전을 통해 가장 최근까지 사용된 개인정보를 획득하기 위해 쓰레기장을 뒤졌다고 밝혔다. 무심코 버려지는 개인정보들이 개인정보 유출의 또 다른 창구가 될 수 있음을 보여주는 사례다.

택배가 도착하면 기다리던 상품이 도착했다는 기쁨에 취해 택배 송장을 자세히 읽어보지 않고 박스부터 개봉하는 경우가 다반사다. 그러나 택배 송장을 조금만 살펴보면 “상품 수령 후 개인정보 보호를 위해 반드시 송장을 별도 분리하여 파기해주시기 바랍니다”라는 문구를 볼 수 있다. 번거롭더라도 택배 수령 시 택배 송장을 떼어내고 잘게 찢어서 별도로 버리는 습관을 갖는다면 재활용 쓰레기를 통해 개인정보가 함께 버려지는 불상사를 예방할 수 있다.

또는 상품 주문 시 배송 관련 옵션으로 “안심번호 사용”을 선택하는 것도 방법이다. 안심번호는 주문자의 진짜 전화번호 대신 가상의 전화번호를 부여하는 것으로, 배송이 완료되면 해당 번호는 없어지기 때문에 전화번호 노출을 예방할 수 있다. 이 경우에도 여전히 배송지 주소와 수신인 이름 등이 남아있는 만큼 택배 수령 시 송장을 별도로 분리 및 파기하는 것을 권장한다.

2. 자동차에 붙여 놓는 ‘연락처’

피치 못할 이유로 주차장이 아닌 곳에(중종 주차장에서도) 자동차를 주차해야 할 때 차량 앞 유리에 연락처를 남겨놓는 경우가 많다. 전화번호만 남겨두기 때문에 크게 문제되지 않을 것으로 생각하기 쉽지만 이를 이용한 범죄가 종종 발생하고 있다.

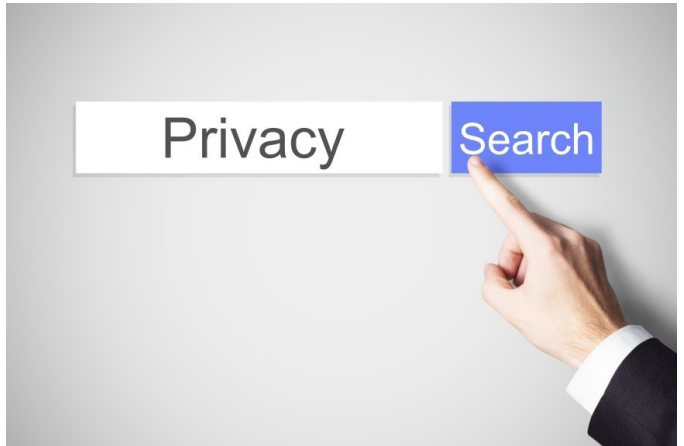
범죄가 아니더라도 이러한 정보를 수집해 광고에 이용하는 업체들도 적지 않다. 특히 차량 번호, 차종, 제조사와 같은 차량 정보는 바로 식별 가능하기 때문에 전화번호와 결합하여 부적절하게 이용할 수도 있다.

현재 일부 통신사에서는 개인을 위해 안심번호 서비스를 제공하고 있다. 한 번 신청해놓으면 사용자가 서비스를 해지하기 전까지 사용 가능하며, 중간에 교체도 가능하다. 부득이하게 전화번호를 노출해놔야 하는 상황이 우려된다면 이러한 안심번호 서비스를 이용하는 것도 방법이 될 수 있다.

3. 동창회 카페 등을 통해 노출되는 개인정보

동창회, 동문회, 친목회 등 모임 문화를 주관하다 보면 주소록을 최신으로 유지하고 관리하는 것이 중요하다. 개인정보 관련 법률에서는 이러한 주소록을 작성 시 반드시 당사자의 동의를 받아야 하며, 이를 입증할 수 있는 자료를 서면으로 보관하도록 하고 있다. 그러나 상당히 번거로운 작업이기 때문에 지켜지지 않는 경우가 대부분이며, 주소록을 작성하고 공유하는 과정에서 부주의로 인해 다수의 개인정보가 유출될 가능성이 크다.

따라서 부득이하게 주소록을 작성 또는 관리해야 하는 경우에는 반드시 문서 파일에 암호를 걸어서 저장하는 것이 좋다. 다른 사람에게 전달해야 하는 경우 암호를 걸어서 파일을 압축하여 전달하면 파일이 외부로 유출되더라도 개인 정보가 불필요하게 유출되는 것을 막을 수 있다.



특히 모임 사이트나 카페 등 인터넷 상에 무분별하게 업로드된 주소록이 수집하는 검색 사이트의 크롤링 봇에 의해 수집되는 경우가 있다. 실제로 현재 모 검색 사이트에서 “주소록”이라는 키워드로 검색하면 상당수의 개인정보를 어렵지 않게 수집할 수 있다. 문서를 올려놓은 당사자들은 의도하지 않은 것이겠지만 악의적인 사용자들은 이러한 방법으로 개인 정보를 탈취해가는 것이다. 심각한 경우 이렇게 노출되는 개인정보는 범죄에도 악용될 수 있으므로, 상당한 주의가 요구된다. 또한 업무에 필요한 문서에 부득이하게 연락처 정보 등을 기록해야 할 경우 반드시 암호를 설정하여 저장 및 보관하는 습관이 필요하다.

4. 휴대전화 교체 시 새어나가는 개인정보

우리나라는 다른 나라에 비해 휴대전화의 교체 주기가 짧은 편으로 알려져 있다. 휴대전화를 교체할 때 휴대전화에 저장되어 있는 개인정보를 삭제하지 않아 개인정보가 유출되는 사례가 적지 않다.

특히 기존에 저장된 전화번호를 옮기기 위해 판매업자의 컴퓨터를 통해 새로운 휴대전화로 옮기는 경우가 일반적이는데, 이때 판매자의 컴퓨터에 그 기록이 남을 수 있는 가능성이 있다. 따라서 휴대전화 교체 시 기존 휴대전화에 저장된 연락처나 중요한 개인정보는 다른 사람에게 맡기기 보다 본인이 직접 정리하는 것이 바람직하다. 번거롭더라도 기존에 사용하던 휴대전화에 저장되어 있는 연락처 정보는 백업한 후 직접 ‘공장초기화’할 것을 권장한다. 물론, 일반적으로 판매업자가 기존 휴대전화를 수거하면서 공장초기화를 해주지만 이것만 믿기 보다는 좀 더 능동적으로 자신의 직접 자신의 중요 정보를 관리하는 태도를 갖는 것이 바람직하다.

한편 안드로이드 스마트폰의 경우 구글 계정을 통해 연락처 동기화가 가능하다. 휴대전화에 직접 저장하지 않고 구글 계정을 통해 저장되기 때문에 별도의 연락처 백업이 필요하지 않다. 기존에 사용하던 기기에서 별도의 백업을 하지 않고 공장초기화를 하더라도 새 스마트폰에서 구글 계정을 동기화하면 구글 계정에 입력되어 있던 기존 연락처 정보도 함께 동기화된다.

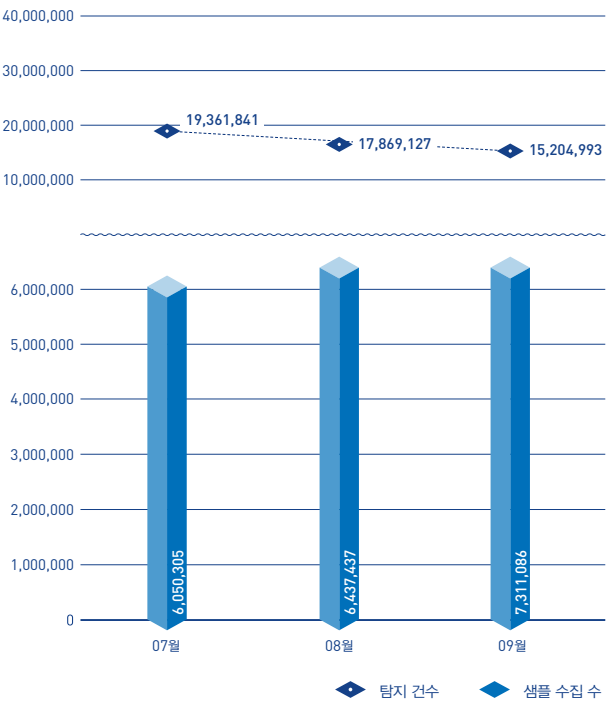
지금까지 우리가 무심코 지나칠 수 있는 일상 생활 속의 개인정보 노출 사례와 예방법에 대해 알아보았다. 상당히 번거롭고, 조금은 어려운 과정일 수도 있다. 그러나 진정한 스마트한 라이프 스타일을 유지하기 위해서는 우리 스스로 노출하는 개인정보를 최소화하기 위해 보다 많은 관심과 노력을 기울일 필요가 있다.

안랩, 9월 악성코드 통계 및 보안 이슈 발표

게임 이용자 노린 교묘한 악성코드 유포

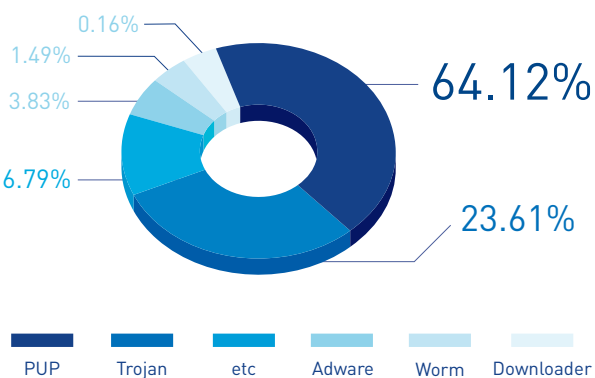
안랩 시큐리티대응센터(ASEC)는 ASEC Report Vol.68을 통해 지난 2015년 9월의 보안 통계 및 이슈를 전했다. 9월의 주요 보안 이슈를 살펴본다.

ASEC이 집계한 바에 따르면, 2015년 9월 한달 간 탐지된 악성코드 수는 1,520만 4993건으로 나타났다. 이는 전월 1,786만 9127건에 비해 266만 4134건 감소한 수치다. 한편 9월에 수집된 악성코드 샘플 수는 731만 1086건이다.



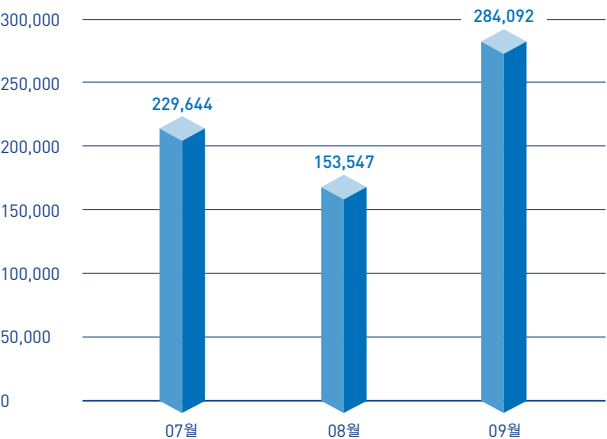
[그림 1] 악성코드 추이(2015년 7월 ~ 2015년 9월)

[그림 2]는 2015년 9월 한 달간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 64.12%로 가장 높은 비중을 차지했고, 트로이목마 (Trojan) 계열의 악성코드가 23.61%, 애드웨어(Adware)가 3.83%의 비율로 그 뒤를 이었다.



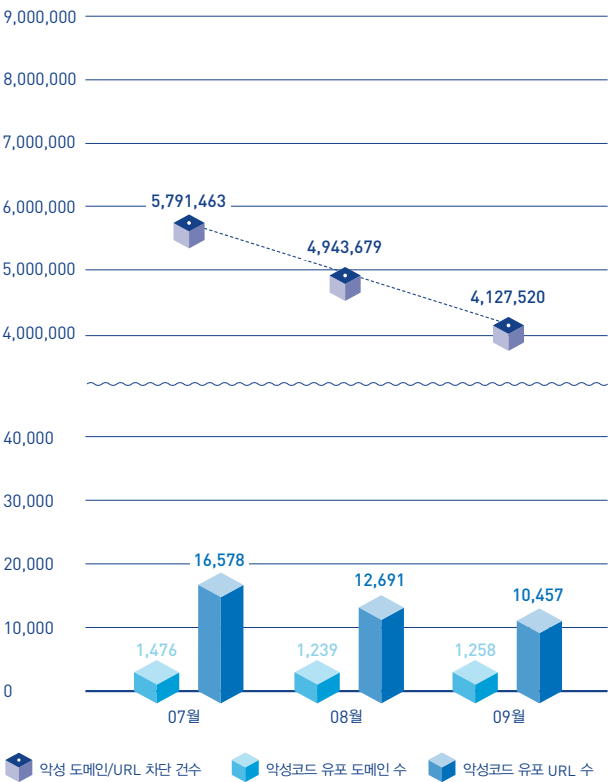
[그림 2] 2015년 9월 주요 악성코드 유형

지난 9월 한 달간 탐지된 모바일 악성코드는 28만 4,092건으로 집계 됐다.



[그림 3] 모바일 악성코드 추이(2015년 7월 ~ 2015년 9월)

또한 지난 9월 악성코드 유포지로 악용된 도메인은 1,258개, URL은 1만 457개로 집계됐다. 9월의 악성 도메인 및 URL 차단 건수는 총 412만 7,520건이다.



[그림 4] 악성코드 유포 도메인/URL 탐지 및 차단 건수(2015년 7월 ~ 2015년 9월)

게임 관련 프로그램으로 위장한 교묘한 악성코드

최근 게임 관련 프로그램으로 위장한 악성코드가 유포돼 게임 이용자들의 주의가 요구된다.

[그림 5]는 모 인기 게임과 관련된 불법 프로그램이다. 게임 이용자들은 종종 유리한 게임 상황을 만들기 위해 게임해킹(gamehack)이나 치트 키(cheat key), 매크로, 트레이너 프로그램 등의 불법 프로그램을 이용한다. 이러한 프로그램은 인터넷, 파일공유 사이트를 통해 쉽게 구할 수 있는데, 악성코드 제작자는 이 점을 이용해 게임 관련 불법 프로그램으로 위장한 악성 파일을 제작 및 유포했다.



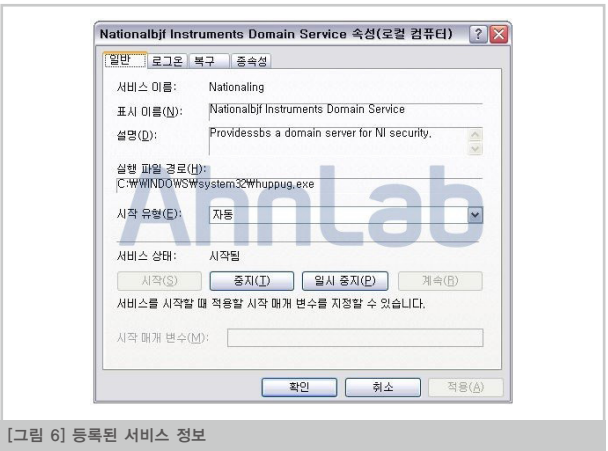
[그림 5] 게임 불법 프로그램으로 위장한 악성 파일

사용자가 이 악성 파일을 다운로드하여 실행하면 실제로 게임 관련 불법 프로그램이 생성 및 실행되어 사용자가 의심하지 않다. 그러나 아래와 같이 0.exe, 1.exe 파일을 생성하고 레지스트리 값 수정, 네트워크 연결 등을 시도한다.

```
[악성 파일이 생성하는 파일 및 경로]
C:\Documents and Settings\Administrator\Application Data\0.exe
C:\Documents and Settings\Administrator\Application Data\1.exe
C:\WINDOWS\system32\hupug(랜덤명).exe
```

위와 같이 생성된 파일 중 0.exe는 자가 복제하여 %system32% 경로에 악성 파일을 생성한다. 1.exe는 게임해킹 프로그램이다.

0.exe 파일에 의해 생성된 악성 파일은 시스템을 다시 시작할 경우에도 반복적으로 실행될 수 있도록 레지스트리 값을 수정하여 'Nationaling'이라는 이름의 서비스를 등록한다.



[그림 6] 등록된 서비스 정보

해당 악성코드는 특정 IP와 연결을 시도한다. 이 사이트와의 연결을 통해 추가적인 악성 파일 다운로드, 개인정보 탈취 등의 악성 행위가 이루어 질 것으로 추측되나, 분석 당시에는 해당 사이트로의 연결이 이루어지지 않았다.

문화체육관광부와 한국콘텐츠진흥원의 조사에 따르면 한국인 10명 중 7명이 게임을 이용한 적이 있는 것으로 나타났다. 공격자들은 공격의 성공률을 높이기 위해서라도 많은 사람들이 이용하는 인기 프로그램이나 인기 사이트를 노린다. 실제로 최근 게임 관련 프로그램뿐만 아니라 정품 소프트웨어의 인증을 우회하는 불법 소프트웨어인 크랙이나 제품번호 생성 프로그램으로 위장하여 악성 파일을 유포하는 사례도 부쩍 증가하고 있다. 특히 이런 사례처럼 사용자가 이용하려던 정상 파일과 함께 악성 파일이 실행되도록 교묘하게 제작되기 때문에 사용자로서는 자신이 다운로드한 파일이 악성 파일이라는 사실을 인지하기 어렵다. 따라서 교묘한 악성코드에 의한 피해를 방지하기 위해서는 불법 콘텐츠 및 불법 다운로드 이용을 자제하는 것이 바람직하다.

한편 V3 제품에서는 해당 악성코드를 아래와 같은 진단명으로 탐지한다.

<V3 제품군의 진단명>

- Win-Trojan/Malpacked5.Gen (2015.09.19.00)
- Dropper/Win32.Agent (2015.09.24.09)

안랩, '2015 지배구조 우수기업' 최우수상 수상

안랩이 최근 한국거래소에서 열린 '2015 지배구조 우수기업' 시상식에서 '최우수상'을 수상했다. 안랩은 지난해 우수상 수상에 이어 올해는 최우수상을 받았으며, 2008년 첫 수상 이래 7회째 수상해 모범 기업으로서의 명성을 재확인했다.



▲ 권치중 안랩 대표(오른쪽)가 최경수 한국거래소 이사장(왼쪽)과 함께 '2015 지배구조 우수기업' 최우수상 수상 기념 촬영을 하고 있다.

안랩은 '지배구조' 부문에서 2005년 CEO와 이사회역의 역할을 분리해 견제와 균형이 가능한 지배구조를 갖췄으며 이사회 내에 감사위원회와 평가보상위원회를 설치하고, 두 위원회를 모두 사외이사로 구성하는 등 선진 지배구조를 유지 및 운영하고 있다는 평가를 받았다. 또한 '사회책임경영'과 관련해 창립 당시부터 개인용 백신(V3 Lite)의 무료 배포와 2009년 7·7 DDoS 공격, 2011년 3·4 DDoS 공격 등 국가적 사이버 재난 시 솔선수범해 위기를 돌파하는 등 사회적 역할에 다양한 노력을 기울이고 있는 점이 높은 평가를 받았다. 안랩은 기업의 사회적 책임을 다하기 위해 청소년 무료 IT 교육 'V스쿨', 여러 대학과 산학협력 등 적극적인 지식 기부로 미래 보안 전문가를 양성하는 데 기여하고 있다. 또한 지역기반 기업 사회공헌연합 '판교CSR얼라이언스' 회원사로 참여해 지역 사회의 다양한 문제 해결에도 나서고 있다.

안랩 권치중 대표는 "안랩은 이번 수상을 계기로 앞으로도 투명경영 및 지배구조 모범 기업의 위상을 이어갈 수 있도록 노력하겠다"고 소감을 전했다.

V3 모바일, 진단율 및 CPU 사용률 '글로벌 최고 수준'

안랩의 안드로이드 스마트폰 보안제품 'V3 모바일 시큐리티(V3 Mobile Security, 이하 V3 모바일)'가 글로벌 테스트 기관인 AV-TEST의 9월 모바일 테스트에서 종합점수 만점과 독보적인 스마트폰 CPU 사용률을 기록하며 인증을 획득했다.

안랩은 최근 4주 내 발견된 악성코드 샘플과 실시간 악성코드 진단 테스트에서 모두 100% 진단율을 기록해 '진단율(Protection)'에서 만점을 받았다. 또한 오진 여부 및 단말기에 미치는 영향을 평가하는 '사용성(Usability)'에서도 만점을, 도난 방지나 스팸 방지 등 추가 기능을 평가하는 '부가기능(Features)'에서도 추가 점수를 받아 종합점수 만점으로 인증을 획득했다.

이번 테스트에서는 진단 테스트에서 상위권 성적을 기록한 제품들이 상세 CPU 사용률에서는 큰 차이를 보였다. V3 모바일은 보안 검

사 시 2.38%(업체 평균: 22.86%)의 스마트폰 CPU 사용률을 기록해 AV-TEST의 9월 테스트에 참가한 25개의 보안제품 중 1위를 차지했다. CPU 사용률이 높으면 스마트폰 배터리 소모량과 스마트폰 성능에 영향을 줄 수 있다.

V3 모바일은 AV-TEST가 모바일 백신 분야에 대한 테스트를 시작한 2013년부터 매회 참가해 17회 연속 인증을 획득했으며, 이번 9월 테스트를 포함해 올해 실시한 5회의 테스트 중 4회에서 악성코드 진단율 100%를 기록했다

안랩 권치중 대표는 "V3 모바일은 높은 보안성은 물론 사용성 면에서도 글로벌 기술력을 인정받고 있다"며 "IoT시대의 첨병인 스마트폰 등 모바일 환경에서 보안성과 사용성을 모두 충족하기 위해 노력할 것"이라고 말했다.

발행인 : 권치중

발행처 : 주식회사 안랩

경기도 성남시 분당구 판교역로 220

T. 031-722-8000 F. 031-722-8901

편집인 : 안랩 콘텐츠기획팀

디자인 : 안랩 디자인팀

© 2015 AhnLab, Inc. All rights reserved.

본 간행물의 어떤 부분도 안랩의 서면 동의 없이 복제, 복사, 검색 시스템으로 저장 또는 전송될 수 없습니다. 안랩, 안랩 로고는 안랩의 등록상표입니다. 그 외 다른 제품 또는 회사 이름은 해당 소유자의 상표 또는 등록상표일 수 있습니다. 본 문서에 수록된 정보는 고지없이 변경될 수 있습니다.



<http://www.ahnlab.com>

<http://blog.ahnlab.com>

http://twitter.com/ahnlab_man



AhnLab

경기도 성남시 분당구 판교역로 220

T. 031-722-8000 F. 031-722-8901

© 2015 AhnLab, Inc. All rights reserved.

