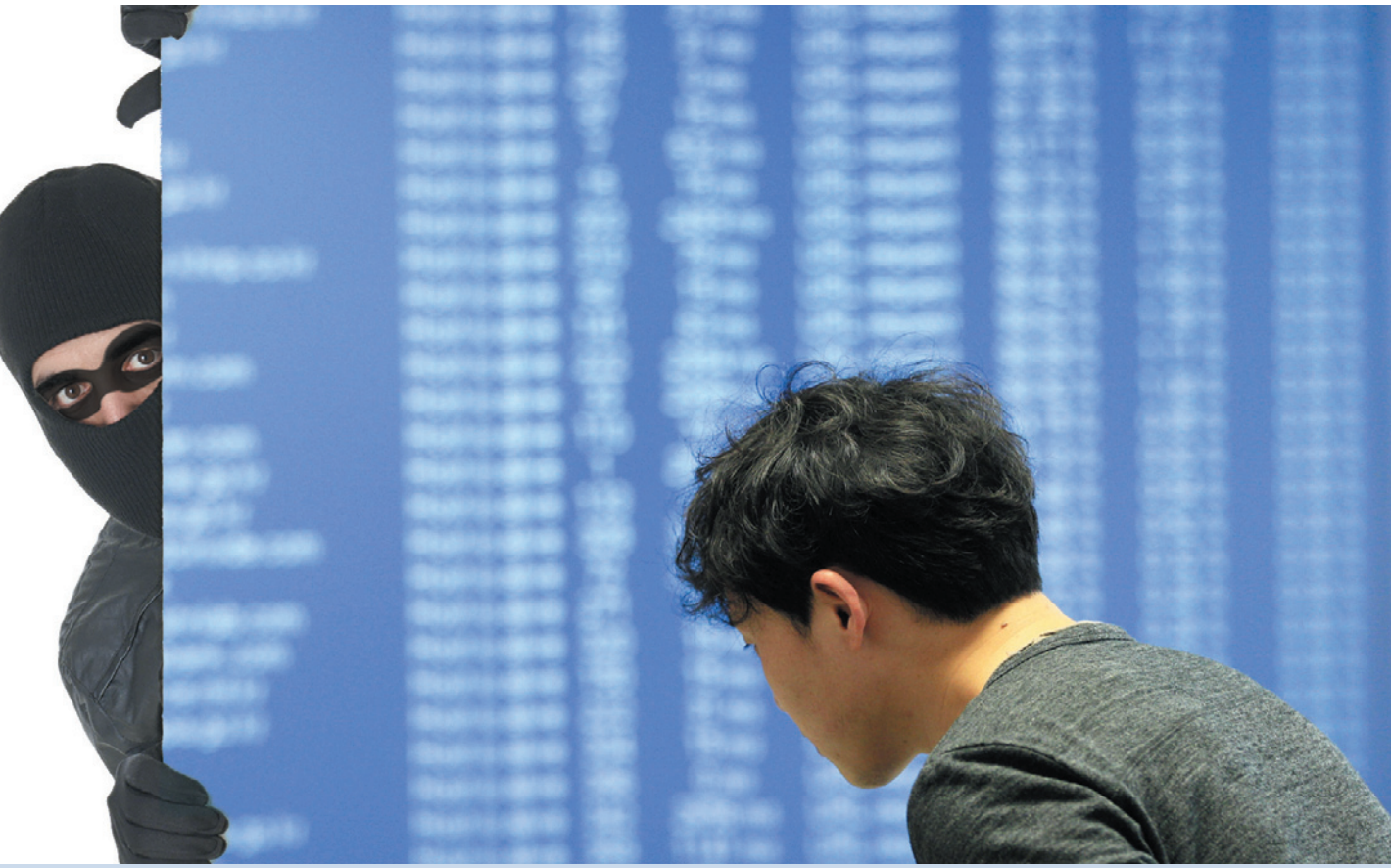

주로 운영체제를 겨냥하던 해커들의 표적이 소프트웨어로 옮아가고 있다. 운영체제나 웹브라우저 등에 비해 보안이 소홀하다는 약점을 노린 것이다. AP_ **연합뉴스**

보안 위협, 알고 대처하자

개인정보 노린 스마트폰 해킹 급증

2011년은 굵직한 보안 사고가 끊이지 않은 한 해였다. 농협과 넥슨, 현대캐피탈, SK커뮤니케이션즈 등의 해킹 사태로 고객들이 큰 불편을 겪었다. 아직까지 국내에서 구체적인 피해 사례가 발생하지는 않았으나 스마트폰도 안전지대라고 장담하기 어렵다. 그렇다고 인터넷을 안 쓸 수는 없는 일. 점점 지능화하는 해커들의 공격에서 소중한 개인정보를 지키려면 최신 보안 문제를 숙지하고 그에 걸맞은 대처 방안을 마련하는 수밖에 없다.

해커들, SNS를 노린다

요즈음 가장 주목되는 보안 위협은 무엇인가? 바로 소셜 네트워크 서비스(SNS)다. 정보 확산 속도와 범위가 빠르고 무엇보다 공격자를 감추기가 쉬워 해킹 급증이 우려된다. SNS를 통해 이메일을 수집한 뒤 신뢰할 만한 사람으로 위장해 악성코드가 포함된 문서를 발송하거나, 주소가 전부 드러나지 않는 단축 주소를 악용해 악성코드 유포 사이트나 피싱 사이트로 유인할 수도 있다.

지난해 연이어 터진 대형 보안 사고들은 예방이 가장 효과적인 대책이라는 사실을 새삼 일깨웠다. 올해에도 해커들은 더욱 정교하고 치명적인 공격을 가하려고 진화를 거듭할 것이 틀림없다. 보안의 중요성이 갈수록 더 커지는 이유다.

해커들의 표적이 운영체제(OS)에서 일반 소프트웨어(SW)로 옮아가는 것도 눈여겨 볼 만하다. 일반 SW는 OS나 웹브라우저 등에 비해 보안이 소홀하다는 점을 노린 것이다. 국내만 해도 작년 말 아래아한글(HWP)의 취약점을 공격한 사례가 발견됐고 이용자가 많은 동영상 재생 SW와 개인 간 파일 공유 SW(P2P), 웹하드 등의 업데이트 파일로 위장한 사례들도 적발됐다.

어디서나 자료를 올리고 내려받을 수 있는 클라우드 서비스가 본격화하면서 수비 범위도 넓어졌다. 실제로 지난해 금융 정보를 탈취하려는 '스파이아이' 악성코드가 처음으로 아마존 클라우드 서비스를 통해 유포되기도 했다. 컴퓨터(PC)나 스마트폰만 공격 대상은 아니다. 스마트TV 등 인터넷에 연결되는 가전도 해커들에게는 훌륭한 먹잇감이다. 가전은 PC 등에 비해 교체주기가 길고 보안에 무심한 편이어서 장기간 공격에 노출되기 쉽다. 일본에서는 이미 DVD 녹화기를 이용한 해킹 사례가 보고되기도 했다.

해커들은 심리전에도 능하다. 악성코드가 담긴 파일에 사람들이 궁금해 하는 사건이 수록된 것처럼 위장하는 식이다. 지난해에는 일본 대지진과 함께 오사마 빈 라덴, 스티브 잡스, 김정일 등 유명인의 사망 사건을 애용했고 올해에는 한국은 물론이고 미국과 러시아 등 세계 각국의 대선, 총선 관련 내용으로 사람들을 현혹하려 들 것으로 예상된다.

내 스마트폰이 '좀비 스마트폰'?

지난해 정보기술(IT) 분야의 최고 관심사는 단연 스마트폰이었다. 신제품이 쉴 새 없이 쏟아지면서 사용자가 폭발적으로 늘어났다. 모바일 애플리케이션(앱)시장이 2010년 52억 달러에서 지난해 150억 달러로 3배 가까이 늘어났고 2014년에는 580억 달러에 이를 전망이고 보면 삼성, 애플, 구글 등이 '특허 전쟁'에 명운을 걸 만도 하다.

모바일 악성코드도 덩달아 급증했다. 시장점유율 1위인 안드로이드를 겨냥한 것이 가장 많고 그중에서도 과금형 악성코드가 대표적이다. 통화나 문자 전송을 할 때 송신자에게 추가 요금을 물리는 '프리미엄 콜/SMS'이 새로운 수익 모델로 등장하자 재빨리 악용한 것이다. 악성코드에 감염시킨 뒤 몰래 특정 번호로 문자를 보내 부당한 요금을 편취하는 식으로 안드로이드 악성코드의 약 45%가 여기에 해당한다.

구글서치, 앵그리버드, 스카이프 등 유명 앱으로 위장한 악성코드도 발견됐다. 안드로이드마켓이나 티스토어 등 정식 앱시장이 아니라 사설 앱시장(써드파티마켓)에서 주로 배포되며 모양이나 이름이 진짜와 똑같아 구분이 안 된다. 정상적으로 동작하면서 몰래 악성코드를 삽입시키는 '리패키징'은 식별하기가 정말 힘들다. 좀비 PC처럼 '좀비 스마트폰'이 생겨날 가능성도 있다. 피해는 크지 않았지만 중국의 사설 앱시장을 통해 좀비 스마트폰의 본부 격인 '봇넷(botnet)'을 구축하려는 시도가 있었다.

대개 스마트폰에는 기존의 휴대전화 보다 개인정보를 더 많이 저장하므로 정보 유출에 따른 피해도 더 크기 마련이다. '니키'로 명명된 악성코드는 사용자의 위치 정보나 송수신 목록은 물론이고 음성 녹음 기능을 활용해 통화 내용까지 고스란히 훔쳐 간다. 개인정보를 빼내는 주목적은 역시 돈이다. 인터넷 뱅킹 정보 탈취로 유명한 악성코드 '제우스'는 심비안과 블랙베리를 거쳐 안드로이드로도 영역을 넓혔다. 해외 인터넷 뱅킹 보안업체의 제품으로 위장한 안드로이드용 제우스는 문자 수신 내역까지 해킹해 일회용 비밀번호(OTP)와 문자 인증의 이중 보안을 뚫을 정도로 정교하다.

안철수연구소 이호웅 시큐리티대응센터장은 "국내에서는 아직 피해가 발생하지 않았지만 스마트폰 악성코드가 안드로이드를 중심으로 폭발적으로 늘고 있다"고 경고하고 "OS 개조나 사설 앱시장 이용 등을 자제하고 앱을 내려받을 때에는 평판 정보를 반드시 확인하는 한편 V3모바일 같은 스마트폰 전용 백신을 최신 버전으로 유지해야 한다"고 조언했다.

정승희 기자 qqutti@hanmail.net