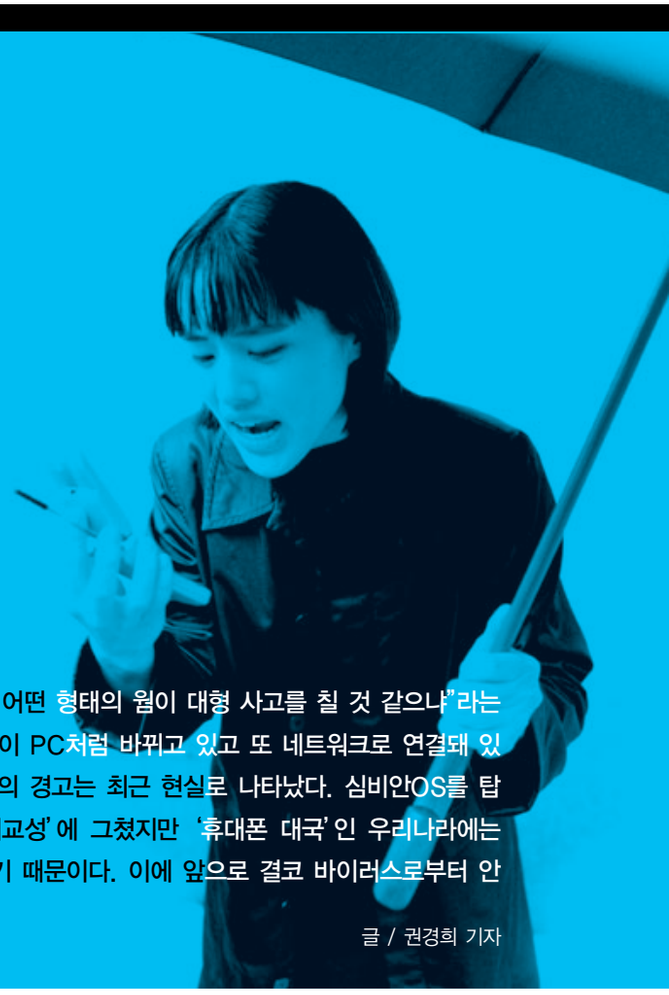
휴대폰 바이러스 안전지대 아니다



세계적인 바이러스 백신업체 트렌드마이크로의 스티브창 CEO는 올해 초 "앞으로 어떤 형태의 웜이 대형 사고를 칠 것 같으냐"라는 질문에 "모바일 분야에서 대형 사고가 있을 것이다"고 말한 바 있다. 그는 "휴대폰이 PC처럼 바뀌고 있고 또 네트워크로 연결돼 있기 때문에 이곳을 겨냥한 웜이 등장할 가능성은 매우 높다"고 경고했다. 스티브창의 경고는 최근 현실로 나타났다. 심비안OS를 탑재한 휴대폰을 노린 '카비르' 웜이 모습을 드러낸 것이다. 다행히 이번 웜은 '애교성'에 그쳤지만 '휴대폰 대국'인 우리나라에는 '적색경보'로 다가온다. 앞으로 좀더 '강한 놈'의 등장은 이제 시간문제로 부상했기 때문이다. 이에 앞으로 결코 바이러스로부터 안전하지 못한 휴대폰을 방어하기 위해 각계가 안전대책 현황을 점검한다.

글 / 권경희 기자

휴대폰이 PC처럼 운용체계(OS)를 탑재하고 인터넷에 접속하면서 바이러스 침투가 현실화되고 있다.

최근 심비안 OS를 탑재한 휴대폰에서 처음으로 바이러스가 발견돼 관련업계가 바이러스 비상에 걸렸다. GSM방식 휴대전화에 '카비르' 웜이 모습을 드러낸 것. 식인 물고기인 피라냐를 뜻하는 '카비르'라고 명명된 이 웜에 감염되면 휴대전화를 켤 때마다 액정화면에 '카비르'라는 글이 나타난다. 현재 '카비르'는 휴대폰 기능 자체에는 큰 피해를 주지는 않지만, 미래에는 심각한 피해를 줄 수도 있는 바이러스가 나타날 수 있다는 것을 피부로 느끼게 한 사건이다.

유사한 피해 사례 이미 나타나

이번에 처음으로 바이러스에 감염된 스마트폰은 휴대전화 기능에 개인휴대단말기(PDA)의 장점을 통합시켜 인터넷 접속과 이메일 전송, 소프트웨어 다운로드 등 컴퓨터의 기능을 수행할 수 있다.

보안전문가들은 앞으로 스마트폰이 악성 바이러스에 공격당할 경우 예상되는 피해는 통화상태가 나빠지거나 저장된 전화번호나 일정관리가 삭제되는 것 등이라고 경고했다.

바이러스 예방 소프트웨어업체인 시만텍사의 스티븐 트릴링 연구소장은 "이젠 휴대전화를 인터넷상 또 다른 컴퓨터 세트로 봐야 한다"면서 "휴대전화가 인터넷에 연결되면 컴퓨터와 마찬가지로 바이러스의 공격대상"이라고 강조했다.

이와 유사한 피해를 이미 일본과 유럽의 휴대폰 사용자들은 경험했다. 일본에서는 인터넷에 링크된 휴대폰들에게 이상한 이메일 메시지가 와서, 그 메시지 요청대로 클릭하면 119와 같은 번호로 계속해서 전화가 걸려졌다. 그래서 버그가 제거될 때까지 휴대폰 사용자들은 모든 긴급구제전화 이용을 자제해야 했다.

유럽에서는 짧은 수동 메시지 서비스(SMS) 기능에 바이러스가 침투해서 두개의 코드가 메시지에 굉음을 내도록 해 사용자는 배터리를 빼내어 다시 부팅해야 하는 불편을 겪었다. 더 악질적인 새 버전은 메시지가 완전히 지워질 때까지 굉음이 계속 울렸다는 것이다.

전화 해킹도 전혀 새로운 것은 아니다. 1970년대에는 소위 전화공격광(phone phreakers)들이 공짜 전화도 걸고 수화기에 휘파람을 불러 댐으로써 전화의 주요 간선을 교란시키기도 했었다.

캘리포니아에 살고 있는 컴퓨터 안전관리 소프트웨어 설계자 존 드레이퍼(John Draper)는 현재 58세인데, 그는 한때 콘플레이크 상자에 들어있는 플라스틱 호루라기를 사용해서 전화 네트워크의 해킹을 개척한 캡틴 크런치(Captain Crunch)로 더 잘 알려져 있다. 그런 장난을 치기는 아주 쉬워서 누구든지 하려고 마음만 먹는다면 네트워크를 완전히 통제할 수가 있고 관리자가 할 수 있는 모든 것을 할 수 있다.

국내에서도 연구소 단계에서 모 업체의 OS를 탑재한 개인휴대 단말기(PDA)에서 글자가 깨지는 바이러스가 발견되기도 했다. 하지만 아직 공식적으로 휴대폰 바이러스가 발견된 적은 없다. 그렇다고 국내에서도 안심할 수만은 없다는 분위기다.

무엇보다 그동안 나타난 바이러스는 '버그' 일 뿐. '카비르' 처럼 '웜' 이 등장한 것은 이번이 처음이다. '카비르' 웜은 휴대폰에 주로 탑재되는 '심비안' 운영체제(OS)와 블루투스를 탑재한 휴대폰을 공격 목표로 설정했다.

심비안은 전세계 스마트폰 OS 시장의 70% 이상을 점유하고 있으며 삼성전자, 노키아, 에릭슨 등 세계적인 휴대폰 제조업체들이 라이선스를 취득, 스마트폰 OS로 사용하고 있다.

하지만 심비안 OS는 대부분 GSM 단말기에 사용된다. 우리나라의 경우 CDMA 방식의 휴대폰이 널리 보급돼 있어 '카비르' 가 활동하기는 힘들다는 분석이다. '카비르' 는 국내서는 약발이 안 먹힌다는 것.

안철수연구소 시큐리티대응센터 조기흠 센터장은 "카비르 바이러스는 심비안을 OS로 사용하는 휴대전화가 근거리 무선통신망인 블루투스에 연결될 경우에만 전파되는데 국내 이동통신 업체의 경우 단말기 플랫폼이 다른데다 블루투스도 내장돼 있지 않아 아직은 걱정하지 않아도 된다"고 말했다. 그렇다고 안심할 문제는 아니다.

문제는 '카비르' 웜의 확산 우려보다, '카비르' 의 등장이 웜의 급증을 알리는 신호탄일 수 있다는 것이다. 이제부터 휴대폰업계와 바이러스와의 전쟁이 시작된 것이나 다름없다는 분석이다.

또 현재 모바일 환경은 PC로 치자면 80년대 말과 90년대 초 PC통신과 유사하기 때문에 각종 콘텐츠를 다운로드받는 과정을 노린 웜이나 바이러스가 등장할 것으로 예상하고 있다. 조기흠 센터장은 "현재와 같은 모바일 환경에서는 위협적이고 확산속도가 빠른 웜이 나올 가능성은 적지만, 트로이목마 형태의 악성코드는 충분히 등장할 수 있다"고 경고했다.

우리나라 모바일 바이러스 확산 최상 조건

세계에서 가장 발달한 휴대폰 시장과 무선인터넷 콘텐츠를 보유하고 있는 우리나라는 모바일 바이러스 확산의 최상의 조건을 갖추고 있다. 최근에는 정부의 보조금 허용으로 PDA와 스마트폰의 판매가 늘어나고 있어, 바이러스 발생 가능성이 더 높아졌다.

무엇보다 최근 모바일게임이 인기를 끌면서 사용료를 지불하지 않고 휴대폰으로 게임을 옮기는 속칭 '불법 모바일 게임 전송 프로그램' 이 등장해 관련업계를 긴장시키고 있다.

어느 프로그램 개발자가 만들어낸 것으로 알려진 '모바일 게임 PC 전송 프로그램' 을 이용하면 휴대폰으로 다운받은 유료 콘텐츠를 다시 컴퓨터로 다운받을 수 있는데, 이때 '마법사 전송 프로그램' 을 사용하면 확장자를 'ebm' 으로 한 파일을 휴대폰 전송케이블을 통해 다른 휴대폰으로 전송할 수 있다는 것이다.

현재 이러한 불법행위가 포털사이트의 자료실 및 휴대폰 동호회 사이트 등을 통해 급속하게 전파되고 있다. 이러한 상황은 결국 휴대폰에도 바이러스나 웜의 출현 및 확산을 예상케 하고 있다.

지금까지는 모바일 환경에서 네트워크를 특정 회사(주로 통신사업자)가 주로 통제를 했지만 이렇게 모바일 기기용 불법 복제 프로그램이 나돌고, 모바일용 와레즈 사이트 등이 여기저기 생기면 분명히 게임 등을 가장한 트로이목마나 웜이 발생할 수 있다는 것이 전문가들의 예상이다.

이밖에 전문가들이 추정하는 예상 시나리오 중 하나는 '웹투폰' 메일 서비스로 인한 웜 · 바이러스의 발생이다. 유무선 환경이 연동되면 휴대폰 등을 통해 웹에서 메일을 다운로드 받을 수 있다. 웹에서 메일을 다운로드받아 휴대폰으로 저장할 때 바이너리(콘텐츠)가 첨부되는 서비스를 통해서 유선에서 웜을 배포하고, '폰투폰' 을 통해서 웜이 전파되는(자기자신을 복제해 전송하는) 시나리오도 가능하다는 것이다.

안철수연구소는 "앞으로 모바일 시장이 확대되고 모바일 기기의 성능이 향상되면 유선 인터넷에 존재하던 컴퓨터 바이러스가 변형 또는 신규 제작돼 전파될 것"이라며 "휴대폰, PDA, 스마트폰 등 개인용 기기는 물론 모바일 기기를 통제하는 서버에도 광범위하게 나타날 것"으로 내다봤다.

국내 이통사 대책마련 '부심'

'카비르' 의 등장에 누구보다 긴장하고 있는 곳은 '당연지사' 국내 이동전화업계다. 특히 휴대폰이 생활필수품이 되어버린 우리나라의 경우 '카비르' 는 등장 자체만으로도, 조만간 대형사고가 터질 수 있다는 두려움으로 다가왔다.

삼성전자 관계자는 "누군가 악의적인 의도를 가지고 휴대폰에서 작동하는 바이러스를 유포한다면 속수무책으로 당할 수밖에 없다"며 "백신업체들과의 협력을 통해 바이러스 출현으로 인한 피해를 최소할 것"이라고 말했다.

보안업체들 역시 국내 모바일 인프라는 인터넷에서나 볼 수 있는 웜이나 바이러스가 등장, 휘젓고 다닐 가능성이 크다는 경고에 나섰다. 이런 이유로 모바일 인프라 보안을 슬로건으로 내건 업체들도 속속 등장하고 있다.

세계 최대 휴대폰 제조업체이자 네트워크 보안업체인 노키아도 그중의 하나다. 노키아는 최근 엔터프라이즈솔루션 사업부를 통해 7.5 기가비트급 보안 솔루션을 출시한 것은 물론 휴대폰 사업부문과의 공조도 강화, 모바일 비즈니스를 지켜주는 보안업체로

도약을 노리고 있다.

무엇보다 대책 마련에 부심한 곳은 이동통신 서비스 업체들. PC에 이어 휴대전화 단말기에도 바이러스가 발생, 소비자 피해가 우려되면서 이동통신 서비스 업체들이 백신 개발 전문업체들과 관련 프로그램을 개발하는 등 대책 마련에 본격 착수했다.

SK텔레콤 · KTF · LG텔레콤 등 이동통신 서비스 3사는 '위피(WIPI)'의 경우 개방형 무선인터넷 통합 플랫폼이고 무선 망 개방으로 콘텐츠에 대한 통제가 더욱 더 어려워 질 것으로 예상하고 바이러스 확산 방지를 위한 근본적인 대책 마련에 힘쓴다는 전략이다.

SK텔레콤은 안랩유비웨어, 안철수연구소와 공동으로 한국형 무선인터넷 플랫폼인 위피 기반의 휴대폰용 백신 'V3모바일'을 최근 개발했다. 이번 'V3모바일'은 SK텔레콤이 무선통신플랫폼 위피 기술 부문을, 안랩유비웨어가 무선 보안기술 부문을, 안철수연구소가 모바일 백신엔진 기술 부문을 각각 담당해 개발했다.

SK텔레콤은 단말기 제조업체와 협력해 최근 출시된 모든 위피폰에 V3모바일을 탑재했고 기존에 출시된 위피폰은 소프트웨어 다운로드를 통해 서비스를 제공할 예정이다.

V3모바일은 ▲사용자의 요구에 의한 바이러스 수동검사 ▲다운로드 및 실행되는 파일의 실시간 검사 ▲백신엔진 업데이트 ▲검사기록 관리 등 기존 PC에서 제공하는 기본적인 백신 ▲바이러스로 의심되는 파일의 분석을 사용자가 직접 요청할 수 있는 바이러스 신고 기능 등을 제공하고 있다.

SK텔레콤은 무선망 개방 등의 무선인터넷 환경에서 안전하고 지속적인 서비스 기반을 구축할 수 있게 됐고, 안철수연구소와 안랩유비웨어는 모바일 기기에 대한 백신기술과 무선보안 기술 및 응용기술을 확보함으로써 글로벌 모바일 보안시장을 선점할 수 있게 됐다고 설명했다.

KTF는 모든 위피 콘텐츠를 보안성이 뛰어난 자바 언어로만 개발하고, 단말기에서 단말기로 전파되는 바이러스 경로를 사전에 차단해 콘텐츠 확산 전 단계에서 사전에 검증, 모바일 바이러스의 가능성을 원천 봉쇄할 계획이라고 밝혔다.

KTF는 또 향후 외장메모리 · 망개방 등 콘텐츠에 대한 통제가 불가능해지는 환경을 고려해 하우리 등 국내 컴퓨터 바이러스 업체를 대상으로 바이러스 백신 개발업체 선정을 추진하고 있다.

기고/휴대폰 악성코드 현황과 전망

'Cabir 웜' 휴대폰을 겨냥한 악성 코드 첫 포문 열다

글 / 이성근 안철수연구소 전략제품개발팀 주임연구원

얼마 전 컴퓨터뿐 아니라 휴대폰에도 웜이 등장했다고 해서 화제가 됐다. 차세대 휴대폰으로서 심비안(Symbian™) 운영체제(OS)를 탑재한 스마트폰에 감염되는 '카비르(Cabir)'라는 웜이 등장한 것이다. 지금까지 휴대폰의 오작동을 유발하는 버그가 발견된 적은 있지만, 휴대폰에서 실제로 작동하는 웜이 발견된 것은 처음 있는 일이다.

이제까지 휴대폰의 오작동이 발생한 사례로는 2000년 1월 노르웨이에서는 특정 SMS 메시지가 노키아(Nokia) 휴대폰으로 전달될 경우 휴대폰 작동을 정지시켜 배터리를 탈착한 후 재장착해야 정상적인 이용이 가능한 경우가 있었다. 2001년 6월 일본에서는 I-Mode 어플리케이션 내의 악성 코드들이 일본 내 수백 대의 휴대폰에 경찰 응급 전화 번호로 전화를 걸도록 만들게 한 피해가 발생했다.

그나마 다행인 것은 카비르 웜이 단말기에 심비안 6.1 이상의 OS로 탑재하지 않았다면 대부분의 휴대폰 이용자들은 모바일 웜으로부터 안전하다는 것이다. 그리고 심비안을 OS로 탑재한 단말기일지라도 블루투스가 없다면 공격의 대상을 찾을 수가 없기 때문에 전파의 위험은 없다는 것이다.

이번에 발견된 카비르 웜이 침투하는 것으로 알려진 심비안 OS는 영국의 심비안사가 소유권을 가지고 있는 Date-Enabled 2G, 2.5G, 그리고 3G용 스마트폰 OS이다. 현재 심비안은 전세계 스마트폰 OS 시장의 70% 이상을 점유하고 있으며, 세계 유수의 휴대폰 제조회사(노키아, 삼성, 에릭슨 등)들이 자사 스마트폰의 OS로 사용하고 있다. 이번에 발견된 Cabir 웜은 블루투스를 이용해 자기 자신을 복제한다. 블루투스의 통신거리가 통상 10m 이내임을 감안하면 실제로 웜이 전파되기는 어렵다.

게다가 국내는 Cabir 웜이 퍼질 수 있는 환경 자체가 조성돼 있지 않다. 우선 국내 이동통신사의 무선 단말기 플랫폼이 다르고, 이동통신사 서비스의 전달 루트도 상이하며, 국내 무선 단말기의 대부분은 블루투스가 내장돼 있지 않기 때문에 유입 및 전파의 위험이 적다. 또한 Symbian 6.1을 탑재한 단말기에서 동작하므로, 기존의 데스크탑 OS를 사용하는 윈도우 사용자나 리눅스 사용자는 아무런 영향이 없다.

하지만 최초의 휴대폰용 웜이 전파력이 약하다고 해서 안심할 수는 없다. 첫 포문이 열렸기 때문에 악성 코드 제작 기술을 계속 발전할 것이기 때문이다. 남녀노소 할 것 없이 전국민의 필수품이 된 휴대폰과 곧 도래할 유비쿼터스 네트워크 환경에서의 보안 문제는 이제 먼 미래의 이야기가 아니다. 다음의 가상 시나리오는 멀지 않은 미래에 충분히 벌어질 수 있는 일이다.

화창한 일요일. 친구에게 전화를 걸려고 저장된 번호를 검색한 K씨는 깜짝 놀라고 말았다. 휴대폰에 저장된 지인들의 번호가 다 삭제되고 없는 것이다. 비밀번호가 걸려 있어 자신 외에는 다른 사람이 임의로 삭제할 수도 없는 일. K씨는 지인들의 전화번호를 일일이 다시 물어보고 입력하느라 엄청난 시간을 낭비해야 했다.

모 홍보에이전시에 근무하는 B씨. 어느 날 중요 고객으로부터 '왜 자꾸 알 수 없는 이상한 문자를 보내느냐'는 항의를 받았다. '자신은 문자를 보낸 적조차 없다'고 아무리 설명을 해도 고객은 B씨의 번호가 분명히 찍혀 있는데 무슨 소리냐며 더 화를 낸다. 답답해 하고 있는 B씨. 이번에는 친구, 가족, 동료 등 그의 휴대폰에 번호가 저장돼 있는 사람들로부터 같은 항의가 쏟아지기 시작했다.

긴급사항에 대비하여 24시간 대비를 하고 있는 119 구조대. 어느날 갑자기 응급 전화 번호로 수백 대의 휴대폰에서 전화가 폭주했다. 전 대원이 서둘러 출동했지만 번번히 헛탕. 알고 보니 악성 코

LG텔레콤 역시 바이러스 감염성이 있는 위피에 대해 바이러스가 플랫폼에서 애플리케이션으로 확산되지 않도록 플랫폼 단계에서 원천적으로 차단할 수 있는 방안을 모색키로 했다. LG텔레콤은 또 위피 플랫폼이 활성화하는 시점에서 바이러스 전문업체와 협력해 백신 프로그램을 개발해 적용할 계획이다.

전문가들 '휴대폰 바이러스 방심은 금물'

휴대폰 바이러스 대책 마련을 위해 보안업계와 함께 이동통신 서비스 업체들이 분주한 반면 휴대폰 제조사들은 아직까지 바이러스 대비에 적극적인 모습을 보이지 않고 있다. 대비책이 소홀할 경우 '상상할 수 없는' 재앙도 피할 수 없다는 점은 제조사들은 어느 정도 인지하고 있지만 심각하게 받아들이고 있지 않는 분위기다.

휴대폰업계는 바이러스 출현은 분명하지만, 초기에는 큰 문제를 일으키지 않을 것으로 보고 있다. 또 새로운 서비스와 신제품 개발에도 인력과 자원이 모자란다는 반응이다.

LG전자 관계자는 "PC는 바이러스라는 개념이 나온 지 10여년 후에 바이러스가 활동하기 시작했다"며 "80~90% 휴대폰은 OS를 탑재하고 있지 않아, 바이러스로 인한 피해가 현실화되기는 상당한 시일이 걸릴 것"으로 예상했다. 팬택&큐리텔 관계자는 "휴대폰 바이러스는 보안업체와 이동전화서비스업체가 해결할 문제"라며 "개발된 백신을 휴대폰에 탑재만 하면 된다"고 말했다.

그러나 보안 업계 관계자는 "러시아의 휴대폰 바이러스 출현은 시작에 불과하다"며 "3세대 휴대폰이나 PDA 등 휴대폰이 PC로 진화한 만큼 이동통신 서비스업체는 물론 휴대폰업체들도 바이러스 대책을 마련해야 한다"고 강조했다.

언제 도래할지 모르는 '무선인터넷 대란'과 같은 최악의 시나리오를 막기 위해서는 모바일 보안에 대한 사용자의 인식부터 바꿔야 한다는 게 전문가들의 조언이다. 핸드폰이나 PDA와 같은 무선 단말기들이 우리의 삶을 예전과 비교할 수 없을 만큼 편리하게 만들어주지만 이와 함께 위험성도 간과하지 못하게 됐다.

전문가들은 이런 위험성을 피하기 위해서는 절대로 불법 콘텐츠의 다운로드는 피하는 것이 중요하다고 조언했다. 한 순간 작은 유혹에 못 이겨 불법 콘텐츠를 사용하는 순간 우리 사회는 커다란 위협에 직면하게 될지도 모른다는 것이 이들의 우려다.

드에 감염된 한 대의 전화기로 시작된 모두 근거 없는 전화로 밝혀졌다.

여름 휴가를 맞아 친구들과 피서를 떠난 A씨. 집에 남아있는 가족들에게 연락하려고 휴대폰을 꺼내 들었지만 전화는 계속 불통. 기지국이 멀리 있어 그런가 싶어 근처 시내로 나가 봤지만 별 소용이 없다. 하지만 다른 사람은 전화가 잘만 터지는데….

알고 보니 모바일 게임을 다운받다가 감염된 바이러스로 인해 A씨의 단말기가 송수신 콜 신호를 거부하거나 조작해 기지국이 단말기의 위치를 파악하지 못해 전화기 본래의 기능을 수행하지 못하게 했던 것. A씨는 새삼 휴대폰의 무선 네트워킹 기능이 두려워지기 시작했다.

그런가하면 최근 모바일게임이 인기를 끌면서 사용료를 지불하지 않고 휴대폰으로 게임을 옮기는 속칭 '불법 모바일 게임 전송 프로그램'이 등장했다. 이 프로그램을 이용하면 휴대폰으로 다운받은 유료 콘텐츠를 다시 컴퓨터로 다운받을 수 있는데, 이를 '마법사 전송 프로그램'을 사용하면 확장자를 'ebm'으로 해 휴대폰 전송케이블을 통해 다른 휴대폰으로 전송할 수 있다. 현재 이러한 불법 행위가 포털 사이트 자료실 및 휴대폰 동호회 사이트 등을 통해 급속하게 전파되고 있다. 이 경우 어떤 위험이 도사리고 있을까.

지금까지는 모바일 환경에서 네트워크를 특정 회사(주로 통신사업자)가 주로 통제를 했지만 이렇게 모바일 기기용 불법 복제 프로그램이 나돌고, 모바일용 와레즈 사이트 등이 여기 저기 생기면 분명히 게임 등으로 가장한 트로이목마, 웜이 발생할 수 있다.

현재의 상황은 PC로 치면 80년대 말과 90년대 초반의 PC 통신과 유사한 환경이 만들어질 수 있다. 이 당시 바이러스의 주요 유포 경로는 PC 통신망이었다. 이들 통신망에 올려진 각종 프로그램들을 보안에 대한 개념이 부족한 PC 이용자들이 무차별 다운로드하는 과정에서 바이러스에 감염되는 사례가 속출했던 것이다.

이외에도 전문가들이 추정하는 예상 시나리오 중 하나는 웹투폰 메일 서비스로 인한 웜/바이러스의 발생이다. 즉 유무선 환경이 연동되면 모바일폰 등을 통해 웹에서 메일을 다운로드받을 수 있다. 웹에서 메일을 다운로드받아 모바일폰으로 저장할 때 바이너리(콘텐츠)가 첨부되는 서비스를 통해서 유선에서 웜을 배포하고, 폰투폰을 통해서 웜이 전파되는(자기자신을 복제해 전송하는) 시나리오도 가능하다는 것이다. 이는 물론 웹to폰, 폰투폰 서비스가 가능해야 가능하다.

이와 관련, 안철수연구소는 지난해 4월 휴대폰용 백신 개발 이전부터 IT기반의 디지털 생활혁명으로 인해 모바일 기기상에서의 보안문제가 심각한 이슈로 떠오를 것으로 예상하고 이에 대한 사전 대비책으로 모바일용 백신 개발에 나섰다. 그리고 지난 2001년 12월 PDA용 백신인 V3 Mobile for Palm 1.0을 국내 처음 개발한 것을 비롯, 2003년 4월에는 SK텔레콤 등과 함께 휴대폰용 백신을 세계 최초로 선보인 바 있다.

안철수연구소는 앞으로 모바일 시장이 확대되고, 모바일 기기의 성능의 향상으로 인해 유선 인터넷 상의 존재하던 컴퓨터 바이러스가 변형 또는 신규 제작돼 전파될 수 있을 것으로 예상하고 있으며, 향후 무선 환경에 발달에 따라 휴대폰, PDA, 스마트폰 등 개인용 기기는 물론 모바일 기기를 통제하는 서버에도 광범위하게 나타날 것으로 전망하고 있다.

즉 모바일 웜의 첫 발견은 사실상 예상 시나리오에서만 존재하던 모바일 환경에서의 보안위협이 이젠 충분히 실현 가능한 상황으로 전환됐음을 전하는 신호탄인 것이다.