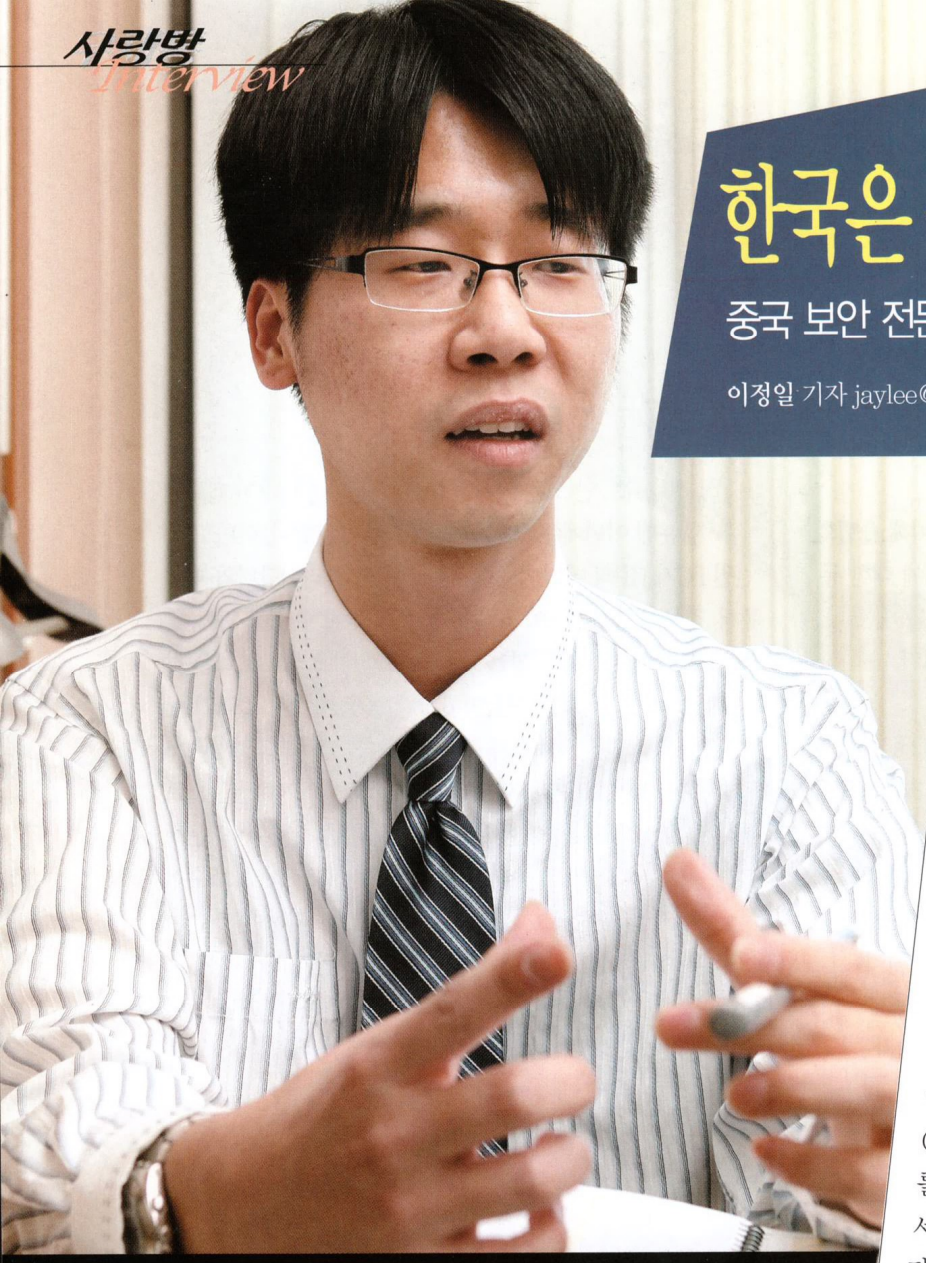

한국은 중국 해커들의 샌드백?

중국 보안 전문 회사 'CN시큐리티' 류승우 대표

이정일 기자 jaylee@ilovepc.co.kr

> "국내 해킹 사고 70%는 '중국'이 주범… 한국 초고속망이 중국 해커들 유혹해"

"한국 사이트를 공격하는 동영상이 버젓이 커뮤니티에 올라와 있는 곳이 중국입니다. 돈만 주면 한국인들의 개인정보를 얼마든지 살 수도 있습니다." '중국발 해킹'이 위험 수위를 넘어섰다. 중국 해킹 정보를 전문으로 다루는 'CN시큐리티'(www.cnsec.co.kr)의 류승우 대표는 "한국은 중국 해커들의 놀이터"라고 잘라 말했다. 그는 "국내 해킹 사고의 70% 이상이 중국 해커들에 의한 것"이라며 '중국 경계령'을 소리 높여 외쳤다.

중국발 해킹 사고 급증 중국발 해킹이 사회 문제로 떠오른 것은 3년 전. 2004년 7월 해양경찰청 77대, 국회 69대, 원자력연구소 50대, 한국 국방연구원 9대 등 10개 정부기관 211대의 PC가 중국 해커에게 공격당하면서 한바탕 소란이 벌어졌다. 2005년 12월에는 전북의 한 은행 서버가 뚫리면서 '보안이 잘 갖춰졌다'는 금융권마저 안심할 수 없다는 우려를 낳았다. 작년 3월에는 국내 지방 일간지 웹 서버를 중국 해커 3명이 침투한 사실도 있었다.

중국발 해킹은 작년 초 리니지 명의도용 파문이 일면서 정부 차원의 관리를 받기 시작했지만, 기세가 수그러들기는커녕 오히려 피해가 늘고 있다. 한국정보보호진흥원(KISA) 자료에 따르면, 2006년 중국발 해킹 피해는 5천 건을 넘어섰고 피해액은 2천 억원 규모에 이른다.

CN시큐리티의 류승우 대표는 "중국 커뮤니티에는 한국 사이트를 공격하는 방법이 동영상으로 아주 친절하게 올라와 있다"면서 "공격 툴도 많아 해커가 아니라도 누구나 쉽게 공격할 수 있다"고 경고했다. 실제로 '화학흑객연맹'(www.77169.com)나 '소호178닷컴'(www.soho178.com) 등의 해킹 커뮤니티에는 국내 기업이나 게임회사, 정부기관을 해킹하는 동영상이 수두룩하다.

바이두닷컴(www.baidu.com)과 같은 일반 포털에서는 한국인들의 개인정보를 쉽사리 구할 수 있다. 한국의 대기업 사이트가 해킹되면 그 정보는 신문광고를 통해 버젓이 거래되고, 국내 게임 사이트에서 해킹된 계정은 이른바 '작업장'을 만들어 게임 아이템 장사를 하는 이들에게 비싼 값에 팔려 나간다. 류 대표는 "중국 돈 200위안(한화 2만5천원)이면 한국 정보를 훔치는 해킹 툴을 손에 넣을 수 있다"고 귀띔했다.

중국 해커들은 P2P 파일에 악성 코드를 심어놓고 먹잇감이 걸려들기를 기다리기도 한다. 최근 국내의 굴지 기업에서 한 직원이 P2P에서 파일을 내려 받았다가 회사 내부망이 완전히 뚫린 사고는 P2P에 대한 경각심을 일깨운다.

해킹 수법도 가지가지 중국 해커들의 공격은 더욱 대담해져가고 있다. 얼마 전 국내 모 홈쇼핑 사이트는 중국 해커들의 집중적인 공격을 받아 정상적인 영업을 하지 못하고 큰 손해를 봐야 했다. "영업을 방해하겠다"면서 수백만 원을 달라는 중국 해커들의 요구를 들어주지 않은 보복이었다. 손해가 커지자 회사는 어쩔 수 없이 돈을 줘

야 했지만 이후에도 그들은 더 큰 액수를 요구하며 끈질기게 물고 늘어지고 있다.

그러나 중국발 해킹은 단순히 중국에서 들어오는 트래픽을 차단한다고 해결되지 않는다. 한국 서버나 PC를 '좀비'(또는 '숙주')로 이용하기 때문에 트래픽 차단은 사실상 아무 소용이 없다. '좀비 PC'는 해킹 툴에 감염돼 원격지에 있는 해커에 의해 다른 시스템이나 사이트를 공격하는 데 악용되는 시스템을 가리킨다. '직접 공격'의 부담을 덜어주는 좀비 PC가 한국에 어느 정도 있는지 파악조차 되지 않는 것도, 이 좀비 PC 리스트가 중국 해커들에게 인기가 많다는 것도 경계해야 할 대목이다.

그렇다면 한국이 중국 해커들의 주요 타깃이 되는 이유는 무엇일까? 첫 번째 배경은 한국의 인터넷 인프라가 너무 잘 갖춰져 있어서다. 류 대표는 "모뎀을 쓰는 곳을 공격해봤자 무슨 재미가 있겠느냐"면서 "전국적으로 초고속망이 깔린 한국은 중국 해커들에게는 더없이 좋은 놀이터"라고 분석했다.

한국이 '윈도 천국'이라는 점도 공격의 불씨를 제공한다. 정치적으로 반미성향이 강한 중국 해커들은 리눅스보다는 윈도를 공격하는 툴을 더 많이 만들고, 이 때문에 윈도 점유율이 높은 우리나라가 큰 피해를 입는다는 분석이다.

지리적으로 가까운 것도 한 이유다. 류 대표는 "법적인 규제가 강한 우리나라에서는 개인정보나 해킹 툴을 구하기 어렵고 돈도 많이 들기 때문에 가까운 중국 해킹 시장에서 불법 자료를 사는 한국인들이 적지 않다"고 털어놨다.

물론 중국에 해킹을 규제하는 법이 없는 것은 아니다. '중국인민대표상무위원회의 인터넷보안에 관한 결정'에 따르면 인터넷에서 누군가를 감시하는 행위와 해킹 프로그램을 만들어 파는 행위는 '위법'이다. 고의로 컴퓨터 바이러스 등 악성 프로그램을 만들어 퍼트리거나 다른 사람의 시스템을 공격하면 법률 규정에 따라 행사 책임을 받는다. 하지만 이런 규제는 아직 초보적인 데다 인터넷 인구가 1억3천명을 넘어선 것을 감안하면 단속이 쉽지 않은 게 현실이다.

중국 해커 500만 명으로 추정

500만 명의 해커가 활동하는 중국은 '해킹 = 범죄'라는 인식이 아직 뿌리 내리지 않았다. 법적인 제재가 마련된 것은 해킹을 분명 '범죄'로 규정하기 때문이지만, 다른 한편에서는 해킹 잡지들이 서점에서 불티나게 팔려나가고 커뮤니티에서는 해킹 정보들이 아무렇지 않게 나돈다.

"우리나라도 2000년 무렵까지 해커들이 크게 늘어났지만 이후 정부의 강력한 규제로 활동이 위축된 반면 중국은 이제 막 전성기를 누리고 있습니다. 그러면서 정치적인 색을 띠었던 예전의 해커들이 줄어들고 돈을 노리는 조직들이 늘어납니다."

'제로 데이'(zero-day, 취약점이 발견되자마자 그날 공격 툴을 만드는 것)는 수천만 원에 거래가 되고 제작자는 유명인사가 되는 게 중국의 현실이다. 한때 S3UNG라는 닉네임으로 활동했던 해커 출신의 류 대표가 CN시큐리티를 세운 이유는 이 때문이다. 중국의 보안 동향과 새로운 공격 기법을 분석해 국내 보안 전문가들이 효과적으로 방어할 수 있게 하자는 취지로, 작년 2월 중국 길림성 연길시에 중국지사를 설립한 데 이어 6월에는 한국본사가 본격적인 활동을 시작했다.

류 대표는 "중국 해커들은 공격 패턴이 보안 프로그램에 읽히는 것을 역이용해 정상적인 작업처럼 속이는 능력이 탁월하다. 변종도 하루에 수십 개 쏟아져 나오기 때문에 국내 보안 전문가들이 제대로 대응하기가 어렵다"며 혀를 내둘렀다.

CN시큐리티는 중국의 해킹 동향과 새로운 공격 기법을 분석해서 공급하는 일 외에도 중국 툴로 모의해킹을 실시해주고 대응 방안을 제시하는 컨설팅을 겸하면서, 보안관제(항공관제사가 비행 전반을 점검하는 것처럼 보안 상황을 전반을 체크하는 전문 업무)나 CERT(침해사고 대응 팀)에 직원을 파견하는 등 중국발 해킹에 대한 포괄적인 사업모델을 두루 갖추었다. 지난해 12월에는 중국 해커들의 공격 패턴과 보안기법, 취약점을 분석해 웹과 e-메일로 서비스하는 'CN SIPS'(Information Provide Service)도 시작했다.

류 대표는 "전통적인 해킹 강국인 터키와 브라질은 서버를 해킹하더라도 금전적 이익을 보는 게 아니라 메인 페이지를 바꾸는 장난(?)을 즐기지만 중국은 심각한 피해를 입힌다. 이제는 중국의 위협을 효과적으로 방어하는 전문가가 필요한 시점"이라면서 '중국통'으로서 CN시큐리티의 역할을 강조했다.

국내 업계 '중국발 해킹' 입 모아 경고

안연구소(www.ahnlab.com)는 지난 1월 발표한 '2007년 10대 보안 트렌드'에서 "지금까지 중국발 웹사이트 해킹은 온라인 게임 사용자를 겨냥해 게임 로그인 정보를 탈취하는 데 그쳤지만 앞으로는 금융자료 등 민감한 정보까지 유출해갈 것"이라고 경고했다. 바이러스 백신업체 뉴테크웨이브(www.viruschaser.com)도 '2006년 악성코드 결산 및 2007년 전망 자료'에서 "중국발 해킹으로 인한 악성코드 피해를 주의하라"고 강조했다. 한국정보보호진흥원(KISA)는 '2006년 인터넷 침해사고 동향 및 2007년 전망' 자료를 통해 "중국 해커들의 공격이 올해는 더욱 지능화, 복잡해질 것"이라고 예상했다. 이제 '중국발 해킹'은 국내 보안 업계의 숙제로 떠올랐다.