# 1.25 인터넷 대란의 원인 분석

°김은영, 박중길
국가보안기술연구소
{eykim, jgpark}@etri.re.kr

# Internet Crisises 뭘 Diagnosis

Eun-Young Kim, Joong-Gil Park
National Security Research Institute

## 요 약

2003 년 1 월 25 일. 국내· 외에 슬래머 웜의 유입으로 국내에서는 인터넷 서비스가 중단되는 등 많은 피해를 받았다. 그러나 이러한 인터넷 대란은 비단 국내뿐만 아니라 선진 여러 나라에서도 피해를 주었지만 유독 국내에서는 다른 나라보다 피해가 훨씬 컸다. 따라서 이번 인터넷 대란을 겪으면서 국내에서만 유독 피해가 컸던 그 원인에 대해 분석해보고 우리의 대책은 무엇인가에 대해 기술하겠다.

## 1. 서론

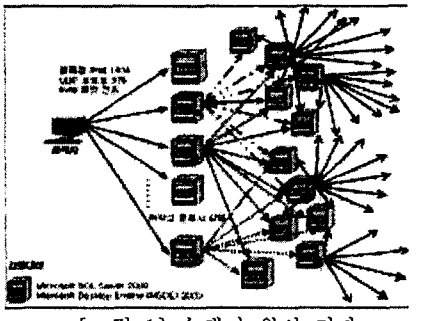
지난달 1 월 25 일 2 시경. 미국, 호주를 통해서 국내로 슬래머 웜(Slammer Worm)의 유입으로 전국의 인터넷 사용자들이 인터넷의 접속 속도가 점점 느려짐을 감지할 수 있었다. 슬래머 웜은 윈도우 2000 의 SQL 서버 취약점을 이용하며, 일단 감염되면 초당 1 만 ~ 5 만 개의 패킷(404byte)을 대량으로 생성하여 뿌림으로써 네트워크를 공격하는 악성 프로그램으로 국내에 약 8 천 8 백여 시스템을 감염시켰다. 이러한 슬래머 웜의 피해로 KT 혜화전화국의 DNS(Domain Name System) 서버가 다운되면서 IT 강국인 국내에서 전국 인터넷 망이 마비되는 사상 초유의 사태가 일어났다. 이러한 사태는 국내뿐만 아니라 미국, 영국 등 전 세계적으로 피해가 나타났다. 그러나 발달된 네트워크 통신 기반 시설과 초고속 인터넷의 높은 보급률은 인터넷 강국이라는 강점과 더불어 이번 인터넷 대란에서 최대의 피해를 주는 공격자 기반 시설로 전락하고 말았다.

따라서 본 고에서는 슬래머 웜의 특징 및 인터넷 대란의 원인 분석, 슬래머 웜으로 인한 국내· 외의 피해 상황에 대해 기술하고, 앞으로 우리의 대책은 무엇인가에 대해 기술하겠다.

## 2. 슬래머 웜의 특징

이번 인터넷 대란의 원인으로 귀결되는 슬래머 웜은 어떤 악성 프로그램인가? 슬래머 웜은 이전의 코드레드(CodeRed)나 님다(Nimda)와는 다른 감염 프로그램으로 새로운 특징을 보여주고 있다. 슬래머 웜의 특징은 크게 다음 네가지로 구분할 수 있다.

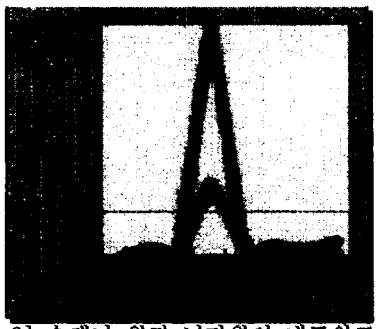
첫째, UDP 프로토콜의 사용이다. 슬래머 웜은 UDP(User Data Protocol) 패킷을 통해 인터넷에 전파된다. UDP 는 인터넷에서 흔히 사용되는 2 가지 데이터 종류중 하나이다. UDP 는 응답이 필요없는 프로토콜이므로 패킷을 보내기만 하면 된다. 이 때문에 웜은 끊임없이 임의의 주소로 계속 데이터를 보낼 수 있게 된다. 그 결과는 데이터의 홍수로, 네트워크는 과부하상태에 도달한다.



[그림 1] 슬래머 웜의 전파

둘째, 슬래머 웜은 작은 크기로 이루어진 프로그램이다. 이 웜은 어셈블리 코드로 이루어져있고 완전한 독립체이다. 하나의 데이터 패키지만 있으면 침입과 감염이 가능하기 때문에 매우 효과적으로 시스템을 감염시킬 수 있다. 즉, 슬래머 웜은 376 바이트로, 코드레드 4096 바이트, 님다 6 만 1440 바이트보다 훨씬 작다. SQL 서버의 취약점을 이용해 자신의 복제 웜들을 보냄으로써 인터넷 상의 다른 컴퓨터들을 잠식해 나간다. 크기가 작기 때문에 단일 데이터 패키지나 패킷안에 숨을 수 있으며 메모리에 상주해 컴퓨터를 감염시킨다. 또한 캘리포니아 대학, 로렌스 버클리 국립 연구소, 보안 컨설팅 회사인 실리콘 디펜스의 연구조사에 따르면 슬래머는 10 분만에 모든 취약한 서버의 90%를 감염시키는등 지금까지 가장 빠르게 전파된 웜으로 기록됐다고 한다. 반면 코드레드는 우선 취약한 서버들을 찾아내고 그 다음 복제 바이러스를 보내는 방식이다. 코드레드에 감염된 서버는 매 37 분마다 2 배로 늘어났지만, 슬래머에 감염된 서버는 8.5 초마다 2 배로 증가했다. 코드레드는

2001 년 7 월 40 만대의 컴퓨터들을 감염시켰고, 님다는 기업 네트워크를 통해 2 개월 후까지도 끈질기게 증식했다. 하지만 슬래머는 이들 두보다 더욱더 확연한 피해를 가져왔다. 다음 그림은 SQL 슬래머 웜과 님다 웜이 라우터에 기록된 네트워크 활동량으로 트래픽이 급증하기 12 시간전부터 이후 48 시간동안의 상황을 보여주고 있다.



[그림 2] 슬래머 웜과 님다웜의 네트워크 활동량

셋째, 데이터베이스의 감염이다. 데이터베이스가 감염될 수 있는 가능성은 사실 항상 존재해왔다. 그러나 대규모로 SQL 데이터 베이스를 감염시킨 웜은 슬래머가 최초였다. 대부분의 웜은 웹 서버, 이메일과 같이 사람들이 공동으로 많이 사용하는 특정 목표를 공격한다. 이번에 20 만대에 달하는 데이터베이스 서버가 감염됐다는 사실은 실력있는 해커가 공격을 하려고 마음만 먹었다면 슬래머 전에도 서버의 데이터에 손댔을 수 있었을 것이라는 사실을 보여준다.

넷째, 메모리 상주형태이다. 슬래머 웜은 하드 디스크에 어떤 파일도 남기지 않고 램(RAM)에서만 상주한다. 즉, 코드레드와 마찬가지로 시스템을 종료시키기면 슬래머 웜은 쉽게 삭제되며, 램에서 실행되므로 슬러머 웜은 빠른 속도로 실행이 가능하다.

## 3. 국내 인터넷 장애의 원인 분석

(1) 정보통신부의 인터넷 대란 원인 분석

이번 인터넷 대란의 원인을 정보통신부의 발표에 따라 분석해보면 다음과 같다.

슬래머 웜은 취약점이 있는 윈도우 서버(MS SQL 서버 2000)를 감염시켜 동 감염서버를 이용하는 대학, 연구소, 기업등 이용자의 인터넷 접속경로를 차단시켰다. 감염 서버는 자동으로 불특정 다수의 다른 컴퓨터를 공격하여 네트워크 트래픽을 폭발적으로 증가시켜 감염된 서버 주변 지역의 이용자들도 인터넷 접속경로가 차단되는 결과를 초래하였다. 또한 감염된 서버가 있는 인터넷 사이트인 경우 서비스 제공이 불가능하여 접속 경로에 장애가 없는 이용자들도 인터넷 서비스를 이용할 수 없는 상황이 발생하였다. 특히, 정보통신시설이 집적되어 있는 IDC(Internet Data Center)에서 LAN 으로 연결되어 있는 서버중의 하나가 감염된 경우 내부망 트래픽이 폭주하여 연결된 서버 전체에 인터넷 접속장애가 발생하였다. 따라서 이렇게 감염된 서버로부터 발생한 공격패킷의 목적 IP 주소는 임의로 부여되는데, 국제 인터넷 주소 할당 분포상 확률적으로 93.2%의 패킷은 국제관문국에 집중되므로 각 ISP 의 국제 관문국에서 심한 병목현상이 발생하였다. 따라서 해외 인터넷 사이트 및 해외 루트 DNS 에 접속할 수 없었고, 루트 DNS 접속 재시도를 하는 과정에서 각 ISP 들의 DNS 에 과부하가 발생하여 국내 인터넷 소통에 지장을 초래하였다라는 것이다.

(2) 인터넷 대란의 원인을 둘러싼 의혹

정보통신부가 2 월 18 일 '1.25 인터넷 대란' 의 정보통신망 침해 사고의 원인 분석 조사 결과를 발표하였지만, 의문은 여전히 있다. 그럼 '1.25 인터넷 대란' 의 원인을 둘러싼 의혹들이 어떤것인지 생각해보자.

첫째, DNS 마비는 역방향 질의(Reverse Query)와 무관하다. 1.25 인터넷 대란의 주원인은 인터넷 주소를 연결해주는 DNS 서버가 마비됐기 때문이다. 이에 대해 정보통신부와 보안 전문가들은 '슬래머 웜' 에 감염된 서버로부터의 공격 패킷 발생 외에도 DNS 서버에 다량의 역방향 질의가 유입된 것이 원인이라고 주장했다. 그러나 이번 정보통신부의 발표에는 "DNS 서버가 마비된 것은 역방향 질의와는 전혀 관계가 없다." 고 주장하였으며, 오히려 사고당시 역방향 질의는 평소보다 감소하였다고한다. 또한 슬래머 웜에 의한 네트워크 트래픽 공격으로 인해 국제회선 장애를 일으켜 해외로 가는 질의 응답(Retry Query)이 늦어지면서 DNS 서버가 재시도 질의를 많이하여 CPU 의 부하가 급증한 것이 DNS 서버 마비의 원인이라는 새로운 주장을 내놓았다.

둘째, IDC 의 피해현황은 공개하지 않는다. 정보통신부는 이번 조사결과 발표에서 IDC 에서 LAN 으로 연결돼 있는 서버 가운데 하나가 감염된 경우 내부망 트래픽이 폭주해 포털 사이트등 연결된 서버 전체에 인터넷 접속장애가 발생했다고 지적한다. 실제 주요 24 개 IDC 를 조사한 결과 IDC 전체 MS SQL 서버 3974 개 중 40.3%인 1603 개가 감염됐다는 것이다. 그러나 정보통신부는 이 같은 평균치만 밝혔을뿐 각각의 IDC 에 대한 슬래머 웜 감염 여부 등 구체적인 자료는 공개하지 않았다.

셋째, 로그 서버 없이 로그 분석이 가능하지는 않다. 정보통신부는 한국통신등 ISP 들의 로그 데이터를 분석한 결과 "지난 25 일 인터넷 장애는 ISP 내 DNS 서버와 루트 DNS 서버간 교신 장애로 ISP 내 DNS 서버의 CPU 부하가 크게 늘어남으로써 초래된 것" 이라고 밝혔다. 하지만 그동안 정보통신부와 KT 등 주요 ISP 들은 로그서버를 운영하지 않고 있기 때문에 로그 데이터 분석이 불가능하다고 말했던 것을 뒤집는 것이다.

### 4. 슬래머 웜의 국내· 피해 상황

슬래머 웜은 외국의 공공기관 및 대기업에 많은 피해를 입혔다. 전세계적으로 슬래머 웜으로 인해 피해를 당한 업체 및 피해 사례는 다음과 같다.

<표 1> 슬래머 웜의 국외 피해 상황

| 피해 업체 | 피해 사례 |
|---|---|
| 뱅크 오브 아메리카 | - 토요일에 상당수의 현금인출기의 사용불능상태, 몇가지 금융서비스가 피해 |
| 컨티넨탈 항공 | - 온라인 티켓팅 및 체크인 문제가 발생<br>- 일부 항공 스케줄이 연착/취소 |
| MS | - 윈도우 XP가 동작하지 않아 게이머들은 애셔론의 콜2 서버에 접속할 수 없음<br>- MS의 네트워크도 접속률 저하 |
| 시애틀시 | - 911 응급연락망이 다운 |
| 워싱턴 상호금융 | - 월요일까지도 현금인출기 사용 불가<br>- 일부 금융 서비스도 피해 |

※자료 : CNET 뉴스, AP.

슬래머 웜으로 인한 국내 피해상황을 수치상으로 서술하면 다음과 같다. 전세계적으로 슬래머 웜으로 감염된 시스템은 약 7 만 5 천여대이다. 이중 국내에서 감염된 시스템은 11.8%에 해당하는 8 천 8 백여대가 감염이 되었고, 이러한 수치는 일본의 약 7 배, 중국에 약 2 배에 달하는 수치이다. 이렇게 국내에서만 유독 피해가 컸던 원인은 과연 무엇일까? 단편적인 원인으로는 MS 제품의 결함, 다른 웜 바이러스 사태와 달리 KT 와 같은 상위 DNS 가 공격당해 피해가 증폭되었다라는 것이다. 그러나 국내 피해 상황이 유독 심한 원인에는 여러가지 요소가 복합적으로 작용하고 있다. 피해를 유발 할 수 있는 여러가지 복합적 원인을 분석하면 다음과 같다.

첫째, 국내처럼 초고속 인터넷 보급이 잘 된 나라가 드물며, 발달된 네트워크 통신 기반환경이 구축되어 있다. 둘째, 이번 슬래머 웜의 공격 대상이 되었던 윈도우 2000 시스템의 보급률이 외국보다 높다. 셋째, 국내에는 DNS 서버가 3 개로 집중되어있다. 참고로 미국등 선진국의 경우 DNS 서버가 여러 개로 분산되어 관리되고 있다. 넷째, 초고속 통신망 및 정보보호가 취약한 IDC 를 통해 급속히 확산되었다. 다섯째, 국내의 PC 사용자 및 보안 관리자들의 상대적인 보안의식 결여이다.

따라서 위와 같은 여러가지 원인으로 인터넷 대란을 겪으면서 앞으로의 우리의 대책은 무엇인가 생각해보자.

### 5. 사이버 테러에 대비한 보안 대책

이번 인터넷 대란을 겪으면서 국내 한 대기업의 보안 담당자는 MS 의 패치만 제때에 내려받았더라면 이번 사태는 일어나지 않았을 것임을 전제하면서, "그러나 패치를 깔면 시스템과 충돌이 일어나는 경우도 발생한다. MS 마저도 문제가 생기거나 데이터가 소실될 수 있다고 얘기를 하는데 누가 함부로 설치할 수 있겠나? 다른 회사에서 설치하는 것들을 보아서 문제가 없는 것 같으면 그때 설치할 수 밖에 없다" 고 전한다. 그렇다면 패치만으로 인터넷 대란을 해결할 수 있는 방법은 아니다. 따라서 인터넷 대란과 같은 사이버 테러에 대해 우리의 대책은 어떤것이 있는지 생각해보자.

첫째, 정보보호 관련 정부의 제도적 개선이다. 정부는 '정보보호 평가제' 와 '소프트웨어 리콜제' 및 정부· ISP, 관련 정보보호업체를 망라하는 신기반 보호 종합상황실을 구축, 해킹· 바이러스에 대한 조기예· 경보를 통해 대응체계를 갖춰 나가고 침해사고 발생 보고 등과 관련한 제도개선을 추진하는 대응조직을 확충하겠다고 발표하였다. 그러나 '정보보호' 활동을 실행하면서 가장 근간이 되는 것이 문서이므로 모든 사람들의 행동규칙의 가이드 라인을 제시하고 이를 실천할 수 있도록 권고사항으로 되어 있는 부분들을 의무사항으로 변화시켜야 할 것이다. 둘째, 개인 및 관리자의 의식 개선이 필요하다. 개인 및 관리자는 이번 인터넷 대란을 통해 자신이 사용 및 관리하는 PC 에 대해 철저한 보안 의식을 가져야 할 것이며, 보안의 허점이 될 수 있는 불법복제 프로그램을 더 이상 사용하지 말아야 할 것이다. 또한 주기적인 백신 업데이트를 통해 향후 피해를 최소화시켜야 할 것이다. 셋째, 기술적 발전을 위한 투자 개선이 필요하다. 각 IT 자원에 대하여 기술적인 취약점을 진단해주고 이를 활용하여 매월단위로 자신들이 관리하는 IT 자원들에 대하여 자체적인 취약점 진단활동을 충실히 수행하여 다양한 사고를 미연에 예방할 수 있도록 기술적 투자가 이어져야 할것이이다. 이러한 기술적 투자를 통하여 정보보호 사업을 육성 및 기술 발전 시킨다면 우리나라는 진정한 사이버 강국이 될 수 있을 것이다.

### 6. 결론

IT 강국이라 불리우는 국내에서는 지금까지 양적 팽창이 지배적이였다. 그러나 이번 인터넷 대란을 통하여 국가 차원의 시스템과 보안기술에 대해 질적 성장과 더불어 우리나라의 중요 인프라의 혁신적인 대책을 모색해봐야 할 것이며, 더 이상 소 잃고 외양간 고치는 일을 하지 말아야 할 것이다.

### 참고 문헌


1. "정보통신망 침해사고 조사결과" , 정보통신망 침해사고 합동조사단, 2003.2.18.
2. http://bgp.lcs.mit.edu/, MIT BGP 모니터 프로젝트
3. http://www.zdnet.com, "슬래머 웜 집중 분석" , Robert Lemons, 2003.2.11.
4. http://www.securitymap.net, "인터넷 붕괴의 기술적 원인 분석" , 전상훈, 2003.1.26.