특집

인터넷 침해사고 원인과 대책

정 태 명 [1)]

목 차

1. 서 론

향상된 컴퓨터와 통신기술의 발달로 인하여 사회의 정보화가 고도화되고, 우리의 경제, 사회, 문화 활동의 기반구조는 여러 분야에서 정보통신인프라에 크게 관련되어 있어서 사이버 안전의 확보는 정보화 사회에서 그 중요성이 더욱 강조되고 있다. 지난 1월 25일 발생한 인터넷 침해사고의 원인은 마이크로소프트 SQL 서버의 취약점을 이용하는 슬래머 웜 공격으로 네트워크 트래픽이 급증했기 때문인 것으로 최종 확인됐다. 슬래머 웜은 UDP(User Datagram Protocol) 1434 포트를 통해 전파되는 404바이트 크기(보내지는 패킷의 크기는 웜 코드 376Byte에 목적지 IP 등 부가정보가 포함되어 약 404Byte)의 메모리 상주형 웜으로서 2002년 7월 24일 공표 된 "마이크로소프트 SQL 서버 2000 및 마이크로소프트 데스크탑 엔진(MSDE) 시스템의 버퍼 오버플로우 취약점"을 이용하여 전파된다. SQL DB서버는 사용 가능한 포트인 총 1~65535 포트 중에서 일반적으로 웹서비스용으로는 80포트, DB용으로 UDP 1434포트나 TCP 1433포트를 주로 사용하는데, 공격의 주 대상이 된 DB용인 UDP 1434 포트는 외부에서 내부로 접속하기 위한 대문과 같은 역할을 하는 포트다.

이 슬래머 웜은 UDP 특성을 이용해 공격을 감행하므로 확산이 급격히 진행되었는데, TCP는 통신 채널의 설정 과정이 필요하지만, UDP에선 세션을 설정하지 않고 데이터를 상대 주소로 전송하므로 확산속도가 빠르다. 이번의 슬래머 웜은 수십 분만에 전 세계적으로 7만5000개의 시스템을 감염시켰는데, 국내에는 지난 1월 25일 14시 10분쯤 미국 · 호주 등지에서 유입, 전 세계 감염대수의 11.8%에 해당하는 8,800여 개가 감염된 것으로 밝혀졌다[1]. 이러한 슬래머 웜의 재감염과 확산을 근본적으로 예방하기 위해서는 MS에서 제공하는 SQL 서버용 보안패치나 SQL 서비스 팩 3을 내려 받아 설치를 해야한다. 서버나 방화벽에서 UDP 1434 포트를 차단한 경우에는 감염이 되지 않았다. SQL(Structured Query Language · 구조화 질의어)는 지난 70년대 미국 IBM이 개발한 관계데이터베이스용 질의 언어의 일종으로 SQL 서버는 이를 기반으로 한 DB 서버를 뜻한다.

1) 성균관대학교 정보통신공학부 부교수

일반적으로 사용자에게 피해를 주는 악성 프로그램은 크게 컴퓨터 바이러스, 트로이목마, 웜 등으로 분류된다. 바이러스는 컴퓨터 프로그램의 정상적인 작동을 방해하거나 변형, 삭제하는 악성코드를 말하며, 웜은 실행코드 자체로 번식을 통해서 다른 사람에게 전파되는 프로그램을 의미하는데 바이러스는 감염대상을 가지고 있지만 웜은 감염대상을 가지지 않는 것이 차이점이다. 트로이목마는 일종의 해킹 프로그램으로 데이터를 조작하거나 훔치기 위해 설치되며, 전염성을 가지고 전파되지는 않는다.

이번의 인터넷 침해사고에서 우리 나라는 다른 나라에 비해서 슬래머 웜에 의한 피해가 더 크게 발생하였는데, 이러한 피해를 발생시킨 사이버 공격에 대한 원인을 살펴보고, 그에 대한 대비책을 제시함으로써 갈수록 지능화 · 고도화 되어가고 있는 사이버 범죄에 효율적으로 대처할 수 있는 방안을 찾고자 한다.

2. 피해 현황

슬패머 웜으로 인한 피해는 우리나라가 가장 컸는데, 주요 ISP의 인터넷 서비스가 5시간 이상 불통되었다. CAIDA(Cooperative Association for Internet Data Analysis)의 분석보고서에 의하면 한국이 전체 슬래머 웜 중에서 11.8%를 보유하고 있어서 세계 2위로 감염률이 높았다는 것을 알 수 있다. 아래의 〈표 1〉은 슬래머 웜의 지역 분포를 나타낸 것이다.

〈표 1〉 슬래머 웜의 지역 분포

순위	지 역	피해정도(%)	순위	지 역	피해정도(%)
1	미국	42.87	6	캐나다	2.88
2	한국	11.82	7	오스트레일리아	2.38
3	Unknown	6.96	8	영국	2.02
4	중국	6.29	9	일본	1.72
5	대만	3.98	10	네덜란드	1.53

(출처 : 인터넷데이터분석협력협회(CAIDA))

우리나라의 피해 현황에 대한 삼성경제연구소 자료에 의하면, 온라인 쇼핑몰은 설 대목 거래 중단으로 업체 당 2~5억원 가량 매출의 피해가 발생하였고, 온라인 스케줄 조회 불가와 예약 취소로 항공 및 여행 업계가 매출이 감소하였다. 또한, 은행 및 증권 업체는 일일 300만건 거래되는 인터넷 뱅킹이 마비되었으며, PC방에서는 인터넷 불능으로 약 225억원의 피해가 발생한 것으로 조사되었다[4]. 우리나라의 피해는 외국보다도 크게 발생하였는데, 그 이유를 들면 다음과 같다. 첫 번째로, 초고속 인터넷이 보편화되어 있어서 빠른 인터넷 속도가 웜의 확산을 가속화 시켰다. 두 번째로는 국내에 루트 DNS가 없어 국제 회선 포화에 따른 국내 DNS 과부하 현상이 심각하고, 세 번째로는 기 구축된 초고속통신망과 IDC를 통해 급속히 확산되었기 때문이다. 네 번째로 가장 중요한 이유는 서버 담당자들의 보안의식이 낮아서 보안 패치나 백신 업데이트를 잘하지 않았기 때문이다[1].

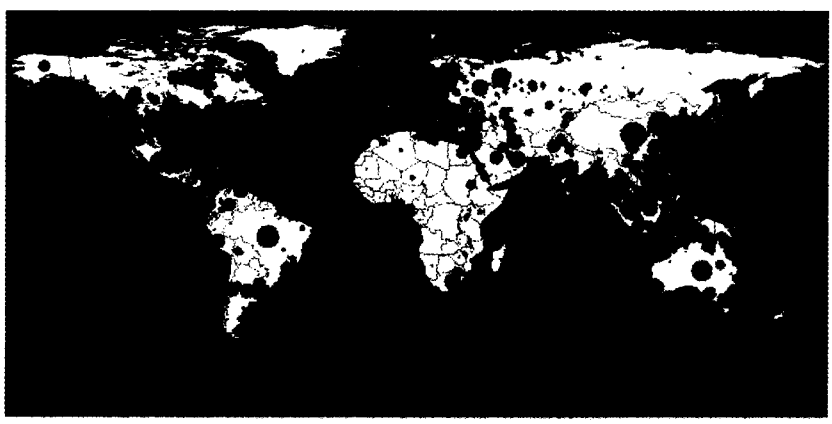
해외의 피해 상황으로는 미국의 경우 Bank of America의 1만3천 여대의 현금자동인출기(ATM)가 작동이 불가능하였으며, 미 연방정부 중 국무부, 농무부, 상무부와 국방부 일부 부서에서 시스템의 지체가 발생하였고, American Express 및 주택융자전문회사인 Countrywide Financial Corp.의 웹사이트 서비스가 한때 중단되었다. 또한, 미국 대형 항공사인 컨티넨탈 항공사는 전산시스템의 지체 등으로 수작업으로 고객 서비스를 시행하였다. 일본에서는 25일 오후 수십 개의 기업 및 대학에서 인터넷 접속이 안되거나 전송이 지연되는 사태가 발생하여 상대적으로 피해가 적었는데 이는 대부분의 UDP 1434 포트가 필터링 되고 있었으며, 꼭 필요한 포트만 개방하는 접근 제어 규칙을 적용하기 때문인 것으로 나타났다. 영국의 경우에는 주요 전자상거래 사이트가 웜 바이러스로 인해 업무가 마비되는 등 유

럽 곳곳에서 인터넷서비스가 중단되거나 전송속도가 떨어지는 피해가 발생하였다. 포르투갈에서는 25일 케이블(Netcabo) 가입자 3십만 명이 12시간 이상 인터넷 접속을 못하였고, 호주에서는 평소 트래픽 보다 3~4배 가량 더 많은 트래픽이 발생하였고, 일부 구간은 완전히 불통되었다. 중국은 백신 업체인 KV(강민)에 따르면 1월 26일 오후 2시에 슬래머 웜에 의해 감염된 업체는 당정기관 단위 80개, 기업사업단위 90개, 학교단위 70개, 전자상거래업체 20개, 기타 30개, 각급성, 자치구, 직할시 등 대부분의 네트워크가 발달한 도시에서 피해가 나타나고 있다고 보고되었다. CAIDA(Cooperative Association for Internet Data Analysis)의 보고에 따르면, 1월 25일 출현한 웜에 의해 전세계의 취약점이 존재하는(패치가 안된) Microsoft SQL 서버 2000의 90%가 10분 이내에 감염되었다[3]. 아래의 (그림 1)은 전세계적으로 30분간 슬래머 웜이 확산된 분포를 나타낸 것이다.

3. 인터넷 침해사고 원인분석

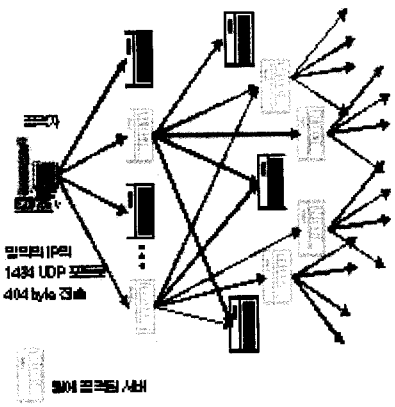
먼저 슬래머 웜은 취약점이 있는 윈도우 서버(Microsoft SQL서버 2000)를 감염시켰고, 이 서버가 스스로 초당 1만~5만개의 공격패킷을 만들며 여러 대의 다른 컴퓨터를 공격해 네트워크 트래픽을 폭발적으로 증가시켰다. 이 때문에 감염 서버가 있는 대학 · 연구소 · 기업은 물론 주변 지역 이용자들도 인터넷 접속경로가 차단됐다. 또 감염된 서버가 있는 인터넷 사이트는 서비스를 제공할 수 없게 돼 접속경로에 장애가 없는 이용자들도 인터넷 서비스를 이용할 수 없었다. 특히 정보통신시설이 모인 인터넷데이터센터(IDC)에서 랜(LAN)으로 연결된 서버 중 하나가 감염된 경우 내부망 트래픽이 폭주해 연결된 서버 전체(포탈 · 쇼핑몰 · 게임 등)에 인터넷 접속장애가 생겼다. 실제 주요 24개 IDC를 조사한 결과, IDC에 있는 전체 MS-SQL 서버 3,974개 가운데 40.3%인 1,603개가 감염된 것으로 나타났다[2]. 이렇게 감염된 서버에서 만들어진 공격패킷의 목적지 IP 주소는 임의로 부여되는데, 국제 인터넷 주소 할당 분포 상 확률적으로 93.2%가 국제관문국에 집중되므로 각 인터넷서비스 업체(ISP) 국제관문국에서 심한 병목현상이 생겨 해외 루트 DNS에 접속할 수 없었다. 아울러 재접속을 시도하면서 각 ISP들의 DNS에 과부하가

(출처 : 인터넷데이터분석협력협회(CAIDA))



(그림 1) 30분간 슬래머 웜 확산분포

생겼고 이것이 국내 인터넷 소통에 지장을 준 것으로 분석됐다[1].
아래의 (그림 2)는 슬래머 웜의 전파되는 경로를 나타낸 것이다.



(그림 2) 슬래머 웜의 전파 경로

슬래머 웜의 동작방식은 SQL 서버가 SQL 모니터 포트로 전송된 데이터를 처리하지 못해서 발생하는 버퍼 오버플로우 결함을 이용한 것으로 크게 4단계로 구분할 수 있으며, 마지막 단계는 무한히 수행된다[4].

- 스택에 원하는 값을 채우는 단계 : 스택에 원하는 리턴값과 쓰레기 값을 저장한다.
- 활동을 위해 필요한 함수를 얻기 위한 준비 단계 : 필요한 함수를 사용하기 위해 엔트리포인트를 얻는 작업을 수행한다.
- 통신을 시작하기 위한 설정 단계 : 목적지 IP를 랜덤하게 설정하기 위한 작업과 공격할 포트를 UDP에 1434번으로 설정한 후, socket을 열고 sendto 함수를 사용할 준비를 한다.
- 무한루프를 돌면서 데이터를 전송하는 단계 : 무한루프를 돌면서 데이터를 전송하며, 이로 인해 시스템의 CPU를 거의 100%까지 점유하게 된다.

공격패킷의 유입으로 감염된 서버는 다른 서버로 웜을 전파하기 위해 공격패킷을 반복적으로 생성하여 전송한다. 감염된 서버는 과부하가 발생하여 다른 일을 하지 못해 결과적으로는 서버에 대한 서비스 거부(DoS : Denial of Service) 공격을 받은 것과 같은 결과를 초래하게 되며, 슬래머 웜은 취약점이 있는 서버 뿐만이 아니라, 임의의 IP 주소를 선택하여 공격패킷을 보냄으로써 네트워크 과부하를 유발시킨다.

4. 사이버 공격에 대한 대책

1.25 인터넷 침해사고의 경험을 감안하여, 향후 국가적 차원에서 정보보호수준이 획기적으로 제고될 수 있도록 정보보호강화 대책의 수립이 요구되며, 그에 대한 대비책으로 크게 정책적인 방안과 기술적인 방안으로 나누어 볼 수 있다.

4.1 정책적 방안

4.1.1 정보보호에 대한 인식제고

서버관리자 및 일반 PC 사용자들에 대한 인식을 제고하여 보안패치, 백신업데이트 등 정보보호 활동을 생활화해야 한다.

4.1.2 루트 네임 서버의 한국내 유치

국제회선 장애로 인한 국내 네임 서버의 장애를 예방하기 위해 루트 네임 서버의 국내 유치가 필요하다. 현재 13개 루트서버는 미국 10개, 유럽 2개, 일본 1개이다. 이는 사이버 공격에 의해서 해외 네트워크가 마비되었다 하여도 루트 서버가 국내에 있다면 인터넷 서비스는 지속될 수 있기 때문이다.

4.1.3 이상 트래픽에 대한 조기대응체제 구축

이상 트래픽의 발생을 조기에 모니터링하여 이를 예·경보할 수 있는 시스템을 개발하고, 이를 활용하여 수분 이내로 인터넷 전체에 트래픽을 차단할 수 있는 조기대응체계를 구축하여야 한다.

4.1.4 전문가 인력 Pool 운영

정보통신망 침해사고 발생시 긴급대응 및 효과적인 사후처리를 위해 동원가능한 산·학·연의 전문가 Pool을 구성하여 운영해야 한다.

4.1.5 보안기술 연구개발에 투자 증대

네트워크 보안과 AntiVirus 관련 연구기술의 투자 확대가 요구되며, 계속적으로 연구 및 제품 개발이 이루어져야 한다.

4.2 기술적 방안

4.2.1 자동 보안패치 시스템의 개발

서버의 핵심 기능에 영향을 미치지 않으면서 자동으로 보안패치를 설치할 수 있는 시스템의 개발이 필요하다. 이를 통하여 시스템 담당자의 업무의 부하를 크게 줄일 수 있으며, 보안위협에 효율적으로 대비할 수 있다.

4.2.2 장비들에 대한 운영 기술의 향상

많은 방화벽과 IDS(Intrusion Detection System) 들이 결국 슬래머 웜의 공격에 모두 적절한 대응을 하지 못하였는데, 보안장비의 효과적인 활용이나 주요 네트워크 장비(Core Router, Core Switch)에서 모니터링과 방어 요령에 대한 습득으로 사이버 공격에 대한 능동적인 대응이 필요하다.

4.2.3 AntiVirus 기술과 보안 기술의 통합

바이러스 기술과 해킹 기술이 접목된 웜의 추가 발생 가능성이 높으므로, AntiVirus 기술과 보안 기술을 통합하는 노력이 필요하다.

참고문헌

[1] http://www.mic.go.kr/jsp/mic_p/p100-0002-1.jsp?m_code=d100-2948-1

[2] 정보통신망 침해사고 합동조사반, 정보통신망 침해사고 조사결과, 2003년 2월 18일

[3] http://www.caida.org/outreach/papers/2003/sapphire/sapphire.html

[4] 안철수연구소 기술기획실, SQL_Overflow 웜의 분석 보고서(Technical Report)

저자약력

정 태 명

1981년 연세대학교 전기공학(학사)

1984년 University of Illinois Chicago, 전자계산학과 학사

1987년 University of Illinois Chicago, 컴퓨터공학과 석사

1995년 Purdue University, 컴퓨터공학 박사

1985년 ~ 1987년 : Waldner and Co., System Engineer

1987년 ~ 1990년 : Bolt Bernek and Newman Labs., Staff Scientist

현재 성균관대학교 정보통신공학부 부교수

e-mail : tmchung@ece.skku.ac.kr

관심분야 : 실시간시스템, 네트워크 관리, 네트워크 보안, 시스템 보안, 그리드 네트워크, 전자상거래