특집

정보통신 인프라 침해사고현황 및 대응체계

한국정보보호진흥원 침해사고대응지원센터 김우한, 최중섭, 홍관희

차 례

요 약

최근의 인터넷침해사고는 개별시스템에 대한 침입이나 바이러스 등에 의한 파일의 변조 등 개별적인 시스템에 대한 공격보다는 인터넷 기반 등에 대한 직·간접적인 공격으로 진화하였다. 이와 같은 공격의 변화에 따라 인터넷 기반에 공격에 의한 피해가 발생할 경우 막대한 경제적 피해는 물론이고 사회적인 충격 또한 클 것으로 예측된다.

인터넷침해사고대응지원센터는 이와 같은 인터넷 침해사고를 신속히 탐지하고 대응하기 위한 능동적인 정보수집 및 대응체계를 구축하였다. 인터넷침해사고대응체계는 침해사고관련정보 수집, 인터넷의 상황 분석, 상황 전파 및 대응, 복구의 4단계로 구성된다. 이러한 대응체계 구축을 통해 이전에 확인할 수 없었던 인터넷 상황에 대한 정확한 측정 데이터를 확보하고 신속한 침해사고 탐지 및 효과적인 대응이 가능하게 되었다

I. 서 론

2003년 1월 25일은 여느 날처럼 평온한 주말이었지만 불과 400여 바이트의 네트워크 패킷들에 의하여 시작된 네트워크 침해사고로 정보기술 종사자들에게는 잊지 못할 날이 되어버렸다. 슬래머라고 불리우는 웜에 의한 이 사고는 불과 10여분 만에 최소한 75,000대의 호스트를 감염시켜 항공기의 출발이 취소시키고, 인터넷을 통한 거래를 전면 중단키는 등 수십억불에 달할 정도로 큰 경제적 피해를 발생시켰다. 또한 사회적으로도 기반시설에 대한 침해사고가 가지는 파괴력이

어떤 것인지 여실히 보여준 큰 사건이었다.

최근, 초고속 인터넷이 급속하게 보급되면서 정보통신 산업, 과학기술 분야 등의 전문분야 뿐만 아니라 일반인들의 경제활동, 문화 등 사회 전반에 걸쳐 인터넷에 대한 의존도가 높아지고 있다. 그러나 인터넷의 발전으로 얻어지는 경제적 이익이나 사회적 기여의 이면에는 해킹, 인터넷을 통하여 전파되는 웜이나 바이러스에 의한 피해 등 정보화 역기능이 갈수록 늘어나고 있고 공격유형도 갈수록 지능화되어 가고 있다. 또한. 사회 전체적으로 높아진 인터넷 의존도로 인해 인터넷 침해사고는 이제 특정개인이나 기업만의 문제가 아닌 국가적 이슈가 되어가고 있다.

기존의 침해사고 대응은 웜/바이러스, 해킹 등 침해사고 피해자의 신고에 의하여 이루어지는 수동적인 대응체계였다. 이러한 대응체계는 인터넷 웜과 같이 네트워크를 통하여 급속하게 확산되는 최근의 침해사고 유형에 효과적 대응이 불가능하므로 인터넷에 대한 적극적인 모니터링을 통한 침해사고의 예측과 조기 대응 체계가 매우 필요하게 되었다. 이러한 능동적 대응체계의 필요성 대두에 따라 KISA에서는 기존체계를 대폭 발전시킨 침해사고대응지원센터를 구축하고 침해사고 대응활동을 수행하고 있다.

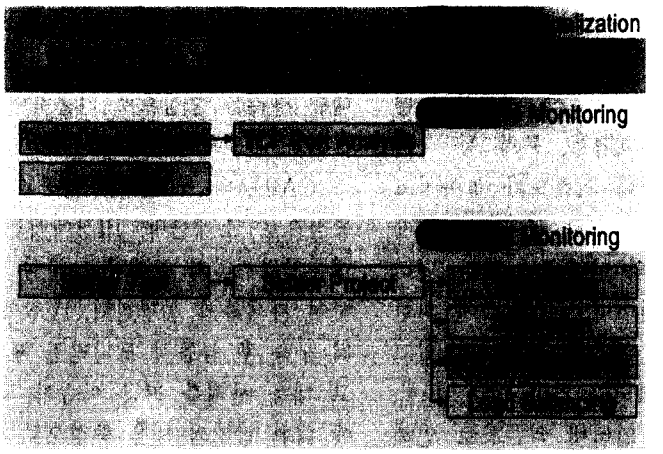
이 논문에서는 정보통신 인프라에 대한 침해사고 대응체계 구축현황과 이를 통한 침해사고 대응 사례를 중심으로 기술하며, 다음과 같이 구성된다. II장에서는 국내외의 대응체계 사례를 미국 CAIDA의 모니터링 활동과 국내의 RTSD를 중심으로 소개한다. III장에서는 인터넷침해사고대응지원센터의 침해사고 분석 및 대응체계에 대하여 자세하게 설명한다. IV장에서는 대응지원센터 구축 후 능동적 모니터링 체계에 의한 침해사고 대응 사례를 최근 이슈가 되고 있는 Bot 웜에 대한 탐지와 대응 중심으로 설명한다.

II. 침해사고 양상의 변화 및 침해사고 대응체계 사례

1. 침해사고 양상의 변화와 모니터링 체계의 필요성

1.25 인터넷침해사고 이전의 침해사고는 바이러스 감염에 의한 파일 손상이나 시스템의 파괴, 불법침입자에 의한 정보의 유출이나 파괴 등이 대표적인 예였다. 이들의 피해 유형은 숙주에 의해 전파되거나 특정 시스템에 대한 침투 등 확산

〔그림 1〕 슬래머 웜 전파 30분 후 전 세계 호스트 감염 현황



〔그림 2〕 CAIDA의 인터넷 모니터링 체계

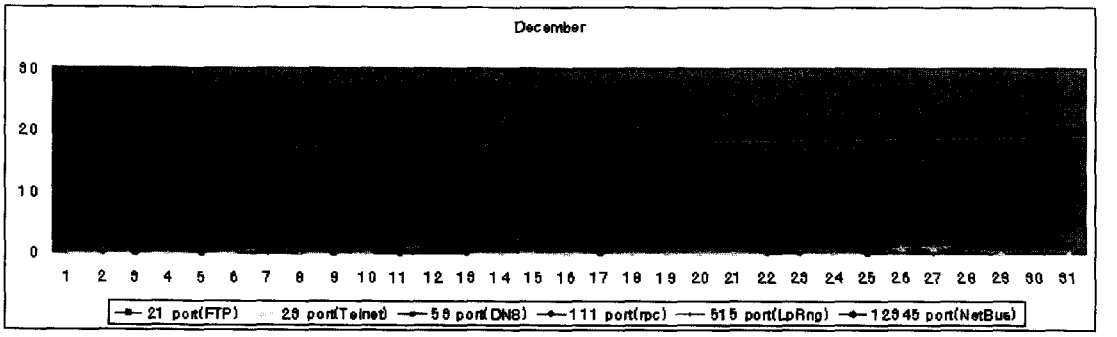
속도가 느리고 피해범위도 지역적인 특징을 가지고 있었다. 그러나 코드레드 등 인터넷 웜이 발전하기 시작하면서 확산 속도가 빨라지고 피해범위도 확대되기 시작했다. [그림 1]은 2003년 1월 25일 발생한 슬래머 웜[1]이 전파되기 시작한지 30분 후의 감염현황이다. 슬래머 웜은 400여 바이트의 UDP 패킷으로 되어있고 자체에 시스템 파괴 등 악성 행위를 하는 코드를 포함하고 있지는 않았지만 빠른 전파 속도와 많은 트래픽을 발생시켜 인터넷 기반을 붕괴시키는 결과를 초래하였다. 또한 블래스터 웜, 웰치아 웜 등 연이어 발생한 최근의 웜들은 개인 PC에 대한 피해 유발뿐 아니라 네트워크 자체를 공격하여 서비스가 불가능하게 하는 특징을 가지고 있고, 바이러스와 같이 숙주에 의하지 않고 네트워크를 통해 전파되기 때문에 전파 속도로 매우 빨라졌다.

이와 같이 침해사고의 위협이 개인 혹은 서버 등에서 네트워크 기반으로 옮겨감에 따라 침해사고 발생시 대규모의 피해가 예상되고 있으며, 이에 따라 인터넷 기반구조에 대한 모니터링 체계의 구축이 요구되고 있다.

2. 국내외의 네트워크 모니터링 사례

CAIDA[1](Cooperative Association for Internet Data Analysis)는 인터넷의 트래픽 측정을 통한 인터넷의 구조 개선, 보안기술 연구 등을 위하여 UCSD(University of California San Diego)의 수퍼컴퓨팅센터에 설립되었다. CAIDA에서는 전세계 인터넷에 대한 트래픽 토폴로지, 인터넷 소통상태 등을 모니터링하여 인터넷 구조의 개선 등을 위하여 자료를 제공하고 있다.

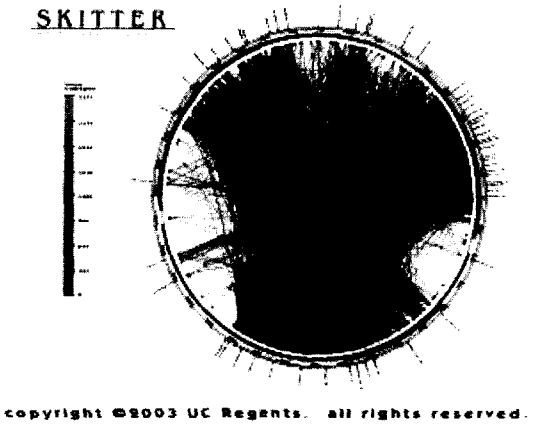
CAIDA는 능동적 모니터링 기법과 수동적 모니터링 기법을 병행하여 네트워크의 상태를 측정하고 있다. 능동적 네트워크 모니터링은 스키터(Skitter)라고 하는 도구를 사용한다. 스키터는 인터넷의 코어 AS 네트워크간 연결, 각 연결별 네트워크 소통상태 등을 모니터링 한다. 이 모니터링은 네트워크 관리자들이 일반적으로 사용하는 네트워크의 연결상태 확인 도구인 traceroute (경로추적) 명령을 주기적으로 수행함으로써 각 네트워크 접점간의 연결 상태와 지연 시간을 측정하고, 또한 AS 코어 네트워크의 연결 및 트래픽 상황 등 네트워크의 상태를 측정하여 표현하도록 구성되어 있다.



〔그림 3〕 RTSD 통계 화면 예

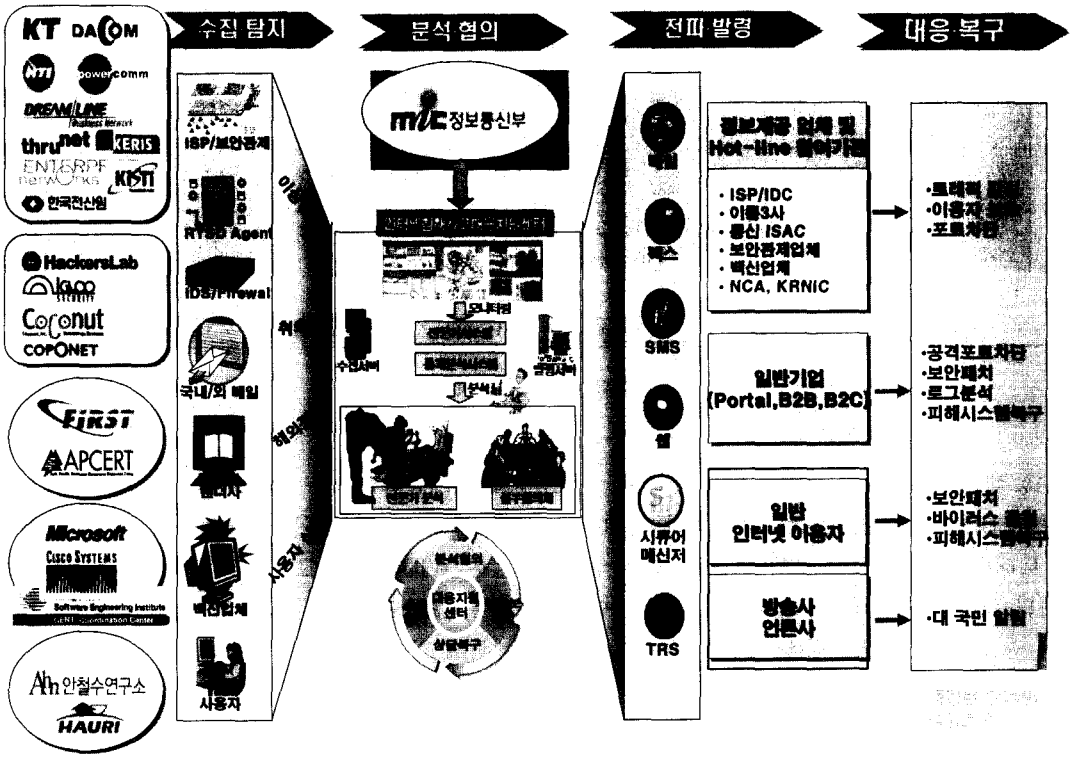
수동적 모니터링에서는 TCP의 트래픽 포트 정보와 DDoS나 포트 스캔 등에 의하여 발생하는 트래픽을 수집한다. CAIDA는 이러한 측정 데이터를 통해 인터넷상에서 발생하는 공격의 종류나 공격대상 호스트, 웜에 감염된 호스트 등의 정보를 식별할 수 있는 체계를 갖추었다.

일본은 텔레콤 ISAC(Information Share and Analysis Center, 정보공유및분석센터)를 중심으로 회원 ISP들의 정보를 공유하는 체계를 구축하고 있다. 이 체계는 회원사의 망에 IDS, 침입차단시스템, 네트워크 트래픽 측정 센서 등을 설치하여 공격상황을 통합하고, 각 ISP에 대한 위협 식별 및 공동대응에 활용하고 있다. 또한 일본은 WIDE[3] 프로젝트를 통해 미국 CAIDA와 네트워크 모니터링 및 측정 활동을 공동으로 수행하고 있다.



〔그림 4〕 CAIDA의 SKITTER 그래프

국내의 네트워크 모니터링은 주로 RTSD(Real-time Scan Detector,실시간스캔탐지기)[4]에 의한 스캔 공격 탐지 활동이 네트워크 모니터링과 관련된 주된 활동이었다. RTSD는 공격자들이 대상을 식별하기 위하여 특정 시스템 정보를 확인하거나 웜 등에 의하여 발생하는 스캔 공격을 탐지하는 시스템이다. 이 시스템의 탐지센서는 자신에 대한 공격 정보를 제공하기로 동의한 사용자가 자발적으로 설치하여 정보를 제공하고 있으며, 2002년까지 발생한 네트워크 웜 및 해킹 사고의 동향을 파악하는 중요한 역할을 하였다. 그러나 이 시스템은 정보사용에 동의한 제한된 개별 시스템에서만 스캔 공격을 탐지할 수 있기 때문에 전체 네트워크에서 일어나는 공격상황을 정확하게 탐지하는 데에는 한계가 있다.



〔그림 5〕 인터넷침해사고 대응체계

III. 인터넷 침해사고 분석 및 대응 체계

1. 인터넷침해사고 대응 체계의 구축

정보통신망법[1]에서 인터넷침해사고란 『"침해사고"라 함은 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등에 의하여 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위로 인하여 발생한 사태』로 정의하고 있으며, 이는 인터넷 서비스 제공자 (ISP), 집적정보통신시설 (IDC) 등과 주요 통신사업자 등 인터넷과 관련된 주요 시설과 관련 시스템에 대한 공격을 의미한다. 즉, 이 법률의 침해사고 정의는 2003년 연초부터 연이어 발생한 인터넷 기반에 대한 침해사고의 특성을 반영한 것이며, 보호의 대상이 기존의 해킹·바이러스로 인한 단위 시스템 피해에서 인터넷 기반에 대한 공격까지 확장되었다.

이전의 침해사고에 대한 대응체계는 침해사고 피해자의 자발적인 신고에 의존하였다. 이와 같은 수동적 대응체계에서는 신고에 의해 얻어지는 사고 정보를 상담자의 경험과 지식에 의존하게 되므로 체계적으로 분석하기 어렵고, 인터넷 웜과 같이 네트워크를 통하여 고속으로 전파되는 최근의 침해사고의 특징 때문에 피해의 양상과 범위를 예측하고 신속한 대응조치를 취하는 것은

1) 정보통신망이용및정보보호에대한법률, 2004.1.29 개정, 2004.7 시행령개정

매우 어려웠다.

이와 같은 문제점을 해결하기 위하여 침해사고 대응체계를 침해사고 정보의 능동적 수집, 자동화된 분석 및 전문가의 분석기능 강화, 탐지된 침해사고 징후의 효과적인 전파, 그리고, 사후 피해 복구의 단계로 이루어지는 다단계 시스템으로 구축함으로써 능동적이고 효과적인 침해사고 대응이 가능하도록 하였다.[6]

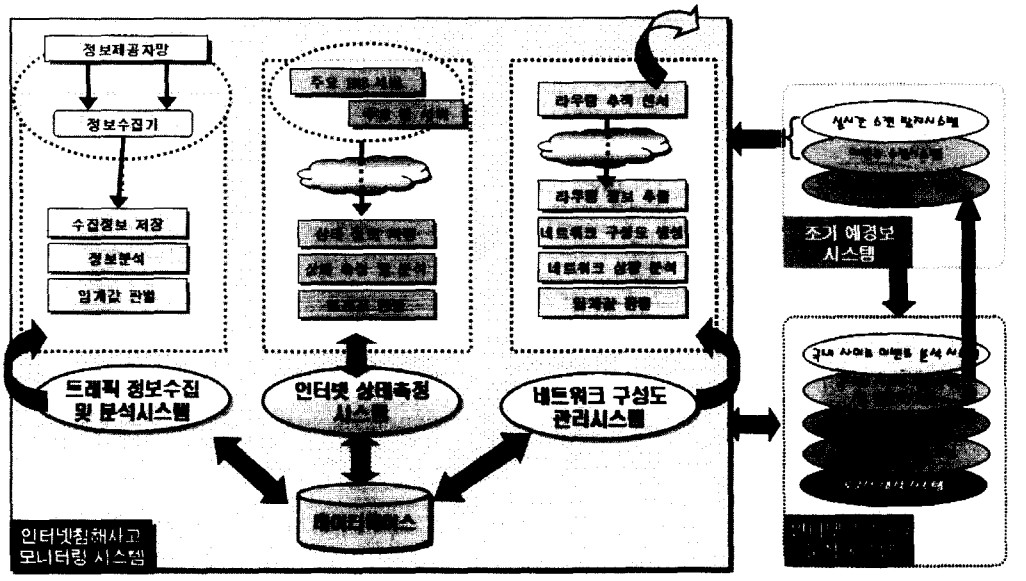
2. 인터넷 침해사고 대응 체계

가. 인터넷 트래픽 정보 수집 및 침해사고 이상징후 탐지 단계

최근의 인터넷 침해사고는 인터넷 웜에 의해 인터넷에 과다한 트래픽을 발생시키거나 관련 시스템에 과부하를 유발시키는 것이 전형적인 예이며, 전파 속도가 매우 빨라 일단 사고가 발생하면 대응이 매우 어렵다. 그러므로 침해사고를 유발할 수 있는 이벤트에 대한 사전 정보 수집이 매우 중요하다. 이에 따라 침해사고 대응체계의 첫 번째 단계로써 인터넷서비스제공자 (ISP), 백신소프트웨어 제조자, 주요 소프트웨어 제조자, 주요 장비 제조사, 보안관제서비스업체 등을 연계하여 인터넷침해사고에 관련된 인터넷 소통정보, 보안취약점 및 패치정보, 웜·바이러스 및 백신 정보, 국외의 침해사고 정보 등을 능동적이고 신속하게 수집할 수 있는 체계를 구축하였다.

먼저, 주요 ISP를 통하여 국제 관문국 등 주요 노드 사이의 트래픽 변화를 감시함으로써 웜 출현 및 비정상적인 트래픽의 증가 등을 탐지할 수 있도록 하였다. 각 ISP에서 제공하는 트래픽 정보는 ISP 별 트래픽 증가, 프로토콜 별 트래픽 양 등의 기본적인 통계 자료들이다.

또한 국내 각 지역에 인터넷 공격 이벤트를 수집하기 위한 시스템을 설치하였다. 이 시스템에는 IDS와 침입차단시스템을 설치하여 공격 현황, 침입차단시스템의 보안 룰 위반 정보 등을 얻을 수 있으며 이를 통하여 지역별 공격 상황과 공격



〔그림 6〕 인터넷침해사고 모니터링시스템의 구조

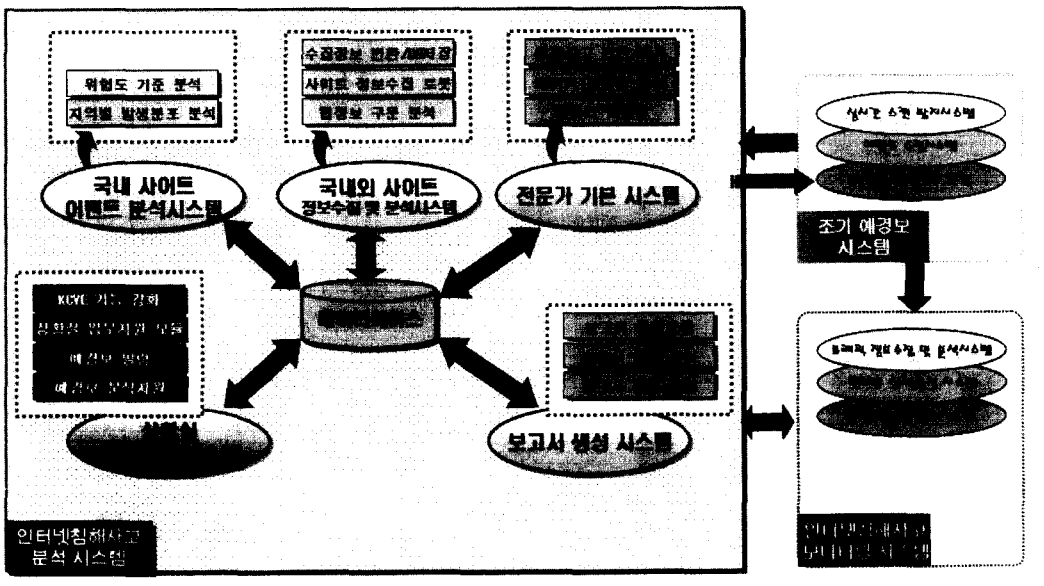
유형 등을 판단할 수 있도록 하였다. 또한 국내 인터넷의 소통에 큰 영향을 미치는 루트 DNS와 국내 주요 DNS의 상태 측정 시스템을 구축하고, 국내외 사이트에서 제공하는 웜·바이러스 정보와 취약성 정보, 그리고 국내 주요 관제 서비스 회사들에서 얻어지는 공격 정보 등을 수집함으로써 인터넷 침해사고 징후를 신속하게 판단할 수 있는 체계를 구축하였다.

나. 분석 및 협의 단계

침해사고대응체계의 2단계에서는 인터넷상의 침해사고 징후를 식별하기 위하여 수집단계에서 수집된 여러 가지 상태 정보에 대한 분석을 행한다. 먼저, 수집한 데이터들에 대한 통계 처리를 통하여 실시간으로 수집되는 데이터들이 정상적인 범위를 벗어났는지 점검한다. 즉, 특정 트래픽이 급격히 증가하는 것을 확인할 수 있도록 전체 트래픽 양 및 포트별 트래픽 양의 변화를 분석한다. 또한 트래픽의 변화가 어떤 공격에 의한 것인지 확인할 수 있도록 해당 시간대에 나타나는 공격 유형 정보도 같이 제공함으로써 시스템 사용자가 상황을 신속하게 인지할 수 있도록 지원한다.

트래픽의 급격한 증가와 같이 표면적으로 나타나는 네트워크의 이상징후와 함께 웜의 발생, 취약점의 발표 등 관련된 상황에 내재되어 있는 침해사고의 가능성을 발견하기 위한 기능이 침해사고 예방에 필수적이다. 이를 위하여 인터넷 상태 정보를 다면적으로 분석하여 침해사고의 가능성을 예측하기 위한 전문가시스템을 구축하였다. 전문가시스템은 ISP 등 정보수집 기관의 정보, 관제업체의 공격 상황 정보를 연관하여 이상징후의 발생 가능성을 예측하고, 이상징후 발생시 원인이 된 이벤트를 식별할 수 있도록 도와주며, 발생한 이상징후의 확산 양상이나 방향을 예측할 수 있도록 지원한다.

보안 관련 취약성이나 신규 웜·바이러스의 출현하는 경우 이러한 요인이 인터넷의 안전성에



〔그림 7〕 인터넷침해사고 분석시스템의 구조

미치는 영향도 항상 고려되어야 한다. 이와 같은 정보는 소프트웨어 수집 로봇을 사용하여 수집하고, 시스템은 각각의 요인들이 인터넷 기반에 미치는 영향을 평가하기 위한 도구를 제공하여 객관적인 판단을 할 수 있도록 지원해 준다.

다. 전파·발령/대응·복구단계

위험성이 큰 웜·바이러스가 발생하거나 침해사고 이상징후가 발생되는 경우 이상 징후 상황의 신속한 전파는 피해의 최소화를 위하여 매우 중요하므로 신속한 상황의 전파를 위한 시스템과 체계가 필수적이다. 그러므로 주의를 필요로 하는 상황이 발생하면 이에 해당하는 예·경보를 관련기관 및 사용자들에게 신속히 전파하기 위하여 단문메시지, 방송매체 등을 활용하여 전달하고, ISP 등 주요 기관과는 주파수 공용 통신 (TRS)등의 체계를 구축하여 신속한 대응 및 복구활동을 할 수 있도록 시스템을 정비하였다.

3. 국제 공동 대응체계 구축

인터넷은 특정 기관이나 지역에 국한되지 않고 전세계적으로 연동되기 때문에 침해사고 발생시에는 발생국 뿐 아니라 전세계적으로 급속히 확산된다. 그러므로 인터넷 침해사고의 대응을 위한 타 국가와의 침해정보 공유 및 공동 대응이 매우 중요하다.

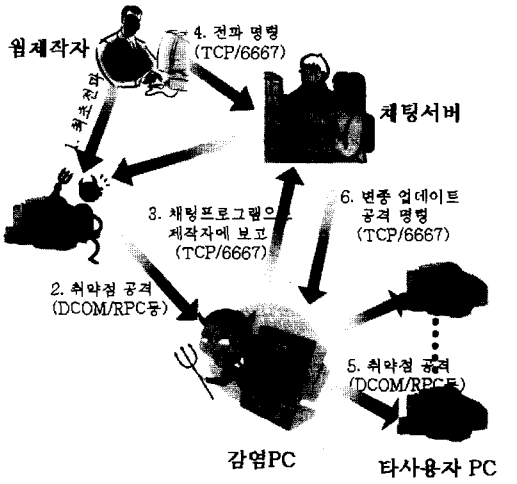
특히 인터넷이 직접적으로 연결되어있는 주변국의 침해사고는 직·간접적으로 국내 인터넷에 영향을 미칠 수 있으므로 이들 국가간 정보공유 및 공동대응 활동은 매우 중요하다.

이러한 국가간 공동대응을 위하여 FIRST, APCERT 등 침해사고 대응관련 국제기구에 활발한 참여 및 정보 공유 활동과 일본, 중국 등 주변국과의 침해사고 공동대응 체계 구축을 추진하고 있다.

IV. 침해사고 대응 사례

1. Bot 웜의 특징[7,8]

인터넷침해사고대응지원센터가 구축된 12월 이후 강화된 인터넷 트래픽 모니터링에 의하여 최근까지 인지하지 못했던 여러 가지 상황에 대하여 인지하는 것이 가능해졌다. 특이할 만한 것은 2003년 후반부터 인터넷에 확산되기 시작한 특정한 종류의 웜인 xBot들에 대한 탐지이다.



〔그림 8〕 Bot 계열 웜의 전파 및 공격 방법

Bot 웜은 윈도우즈 취약점을 통하여 확산되고 감염된 PC들은 유포자의 의도에 따라 조종되어 특정사이트에 대한 서비스 거부공격 등이 가능하도록 개발된 고도로 발달된 웜이다. 또한 이 웜은 확산 단계에서도 주변 시스템의 취약점을 스캔하기 위해 발생시키는 다량의 네트워크 트래픽 때문에 감염기관이나 감염자 PC의 네트워크 사용을 불가능하게 하는 악성 웜이다. 이 웜의 유포자는 인터넷 채팅 시스템인 IRC를 통하여 감염시스템들을 성능이 강화된 변종 웜으로 업그

레이드하거나 다른 시스템을 공격하도록 조종하는 등 악성행위를 하고 있다. 최근에는 이 웜의 변종이 무려 2000여 종을 돌파하여, 바이러스 백신 등을 통해서도 완전히 탐지되지 않아 대응이 어렵고, 또한 광범위하게 퍼진 웜들을 사용한 특정 사이트에 대한 서비스거부공격 위험성 때문에 관련 기관들의 이목을 집중시키고 있다.

2. 이상 트래픽 발생 인지 및 차단 활동

이 웜은 IRC에 사용되는 TCP/6667 트래픽과 함께 윈도우즈 운영체제의 DCOM/RPC, WebDav, LSASS 등의 취약점 등을 악용하기 위한 트래픽을 동시에 증가시킨다. 그러므로 이들 트래픽을 집중적으로 감시함으로써 피해 현황과 공격 현황을 예측할 수 있다. 또한 Bot 계열 웜들은 웜 유포자가 관리하는 IRC 서버에 특정 포트를 통하여 접속한 다음 공격 명령을 기다리므로 웜의 서버 접속 시도를 분석하면 어떤 시스템이 bot를 제어하기 위하여 사용되고 있는지 확인하는 것이 가능하다.

트래픽 모니터링 시스템은 2003년 말부터 취약점 스캐닝과 IRC 관련 트래픽이 비정상적으로 증가하는 것을 탐지하였다. 이와 같은 트래픽의 증가와 해외의 웜·바이러스 정보와 입수한 웜 샘플을 분석하여 확인한 결과 Bot 계열의 웜들에 의한 것임을 확인하였다. [그림 9]는 Bot 웜이 활동한 시간대에 침해사고대응지원시스템에 나타난 트래픽 현황이다. 이 그림에 표시된 IRC 트래픽은 평상시에는 낮은 사용률을 보이는 트래픽이지만 그림과 같은 급격한 증가는 웜 유포자와 웜의 통신이나 업데이트 등의 활동에 의해 발생한 비정상 트래픽으로 추정할 수 있다.

이와 같이 트래픽 발생 상황 인지 후 웜 관련 사고가 발생한 기관에 대한 사고 대응을 지원하는 과정에서 확인된 Bot네트의 숙주 서버를 확인하고 차단함으로써 공격에 악용되는 것을 방지하는 활동을 지속적으로 수행하고 있다. Bot-net를 처리하는 과정에서 확인된 피해 서버들은 수천개 이상의 감염 PC들을 조정하고 있었으며, 이들이 특정 사이트에 대한 공격을 시도했다면 공격 대상 기관 및 인터넷기반에 매우 큰 피해가 있었을 것으로 판단된다.

V. 결론 및 향후 추진 과제

최근 인터넷은 우리의 생활에 광범위하게 영향을 미치고 있으며, 이에 따라 인터넷 기반의 안전성 확보는 국가의 안위와도 관련되는 매우 중요한 분야로 부상하게 되었다. 또한 침해사고도 이전의 개인 PC나 학교의 실습용 서버 등에 대한 해킹이나 자료 파일 등 개인에게 피해를 입히는 수준의 지역적인 공격에서 현재는 인터넷 기반으로 공격대상이 확대되어 단 한번의 침해사고로도 매우 큰 경제적, 사회적 피해가 유발될 것으로 예측된다.

이와 같은 인터넷침해사고 예방을 위해서는 인터넷의 상황과 관련된 보안정보, 웜바이러스의 네트워크 영향력 등을 종합적으로 분석하고 이에 따라 침해사고의 확산 범위 및 방향을 예측하고 확산을 방지하는 것이 매우 중요하다. 이러한 활동을 위하여 KISA에서는 체계는 365일 24시간에 걸친 네트워크 이상상황을 감시와 분석 체제를 구축하고 예방활동을 수행하고 있다.

인터넷 침해사고 대응체제는 침해사고 대응의 각 단계를 지원하는 인터넷침해사고대응지원시스템을 통하여 구현된다. 이 시스템은 인터넷 트래픽, 보안정보 등을 수집하여 분석함으로서 인터넷의 이상 징후를 탐지하고 적절한 대응활동을 행할 수 있도록 지원하는 역할을 수행한다.

인터넷 침해사고 대응은 신속한 대응이 매우 중요하다. 최근 일반화된 인터넷 웜들의 확산 추

세를 보면 이전에 수일 혹은 수개월에 걸쳐 확산되던 것이 최근에는 하루 이내에 전 세계로 확산되는 것을 관찰할 수 있고, 또한 수시간 이내에 전세계로 확산될 수 있는 수퍼웜의 출현도 예상되고 있다.

현재의 인터넷 침해사고 대응체제는 침해사고 발생 후 30분 이내에 대응을 완료할 수 있는 체계를 구축하는 것이 목적이다. 그러나, 침해사고 확산속도의 급격한 증가와 웜·바이러스의 악성화 등으로 가까운 장래에는 이보다 훨씬 빠른 대응이 요구될 것으로 예측된다. 그러므로, 대응지원시스템은 수집한 정보의 다면적 분석 강화와 전문가시스템 등 자동화된 분석체계의 고도화를 통하여 이와 같은 위협에 적극적으로 대응하여 나가는 것이 필수적이다.

참 고 자 료

[1] David Moore, *et.al.* Inside the Slammer Worm, IEEE Security and Privacy, pp. 33-39, July 2003

[2] CAIDA, http://www.caida.org

[3] http://www.wide.ad.jp

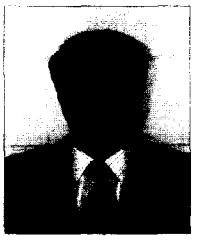
[4] 네트워크 스캔공격 탐지 통계 분석, 2000, KISA

[5] 2003 *정보시스템 해킹·바이러스 현황 및 대응*, 2003, 한국정보보호진흥원

[6] 인터넷침해사고대응지원센터구축, 2003, 한국정보보호진흥원

[7] Agobot(rbot) 웜 최신변종 분석 보고서, http://www.krcert.or.kr, 한국정보보호진흥원

[8] Agobot 계열 웜 분석 보고서, http://www.krcert.or.kr, 한국정보보호진흥원



김 우 한

2003년 ~ 현재 : 한국정보보호진흥원 인터넷침해사고대응지원센터 본부장

2001년 ~ 2003년 : ㈜한솔아이글로브 전무이사

1983년 ~ 2001년 : ㈜데이콤 상무이사

1979년 : 성균관대학교 전자공학과 공학사

<관심분야> 기본통신 및 IP 통신망, e-Biz, 네트워크 보안, 해킹바이러스 분야 등

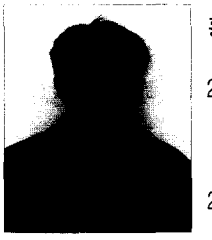
최 중 섭

2000년 ~ 현재 : 한국정보보호진흥원 인터넷침해사고대응지원센터 선임연구원

1996년 ~ 2000년 : 숭실대학교 대학원, 공학박사

1993년 ~ 1995년 : 숭실대학교 대학원, 공학석사

<관심분야> 인터넷보안기술, 분산실시간시스템, 운영체제



홍 관 희

2003년 ~ 현재 : 한국정보보호진흥원 인터넷침해사고대응지원센터 연구원

2001년 ~ 2003년 : 이글루시큐리티 기술지원팀

2000년 ~ 2001년 : iAsiaWorks Korea 보안팀

1997년 ~ 2000년 : Ford Motor FSIC LD&I 팀

1996년 ~ 1998년 : University Of Detroit Mercy 공학석사

<관심분야> 네트워크보안, 해킹·바이러스 대응기술, 포렌식 기술