최근 해킹 · 바이러스 대응기술동향

한국정보보호진흥원 전완근 · 임재명

1. 서 론

최근의 해킹 · 바이러스 특징을 한마디로 표현하면 바이러스와 해킹기법인 백도어, 트로이목마 등의 기술이 복합적으로 결합되어 제작되고 인터넷을 통하여 빠르게 전파되는 인터넷 웜이라고 할 수 있다[1]. 2001년 초기에 등장하여 인터넷 웜의 시대를 예고했던 라멘(Ramen), 라이언(Li0n), 레드(Red), 카코(Carko), 치즈(Cheese) 등과 같은 주로 유닉스 운영체제의 서버급 시스템을 주요 공격목표로 하는 인터넷 웜들이 기승을 부렸고, 2001년 하반기에 들어서면서 공격목표는 유닉스 시스템에서 윈도우 계열의 운영체제를 사용하는 개인용PC로 바뀌어 갔다.

7월에는 서캠(Sircam) 바이러스로 인해 개인이나 회사의 중요정보가 유출되는 피해사례들이 속출했으며, 곧이어 코드레드(CodeRed) 웜으로 인하여 국내 수 만대의 윈도우 환경의 시스템들이 해킹 당하여 네트워크 사용이 불가능한 사태까지 발생하는 등 엄청난 혼란이 일어나기도 했다. 9월에는 웹 메일, 공유폴더 등 다양한 경로를 통해 모든 윈도우 계열의 운영체제 시스템을 감염시키는 복합식 웜인 님다(Nimda) 웜이 전국을 휩쓸기도 하였다[1,2].

2002년에 들어와서 상반기에는 이러한 인터넷 웜이 해킹 · 바이러스의 주류를 이루고 있으며, 특히, 4월에 발생한 클레즈변종(Klez.H)웜 등이 출현하여 현재까지 많은 피해를 일으키고 있다. 또한, NetBus와 같은 스캔 도구를 이용한 스캔 공격과 Unix계열의 SSH 취약점을 이용한 해킹이 기승을 부리고, 스팸메일의 피해 증가와 MS-SQL 서버의 취약점을 이용한 스피다(Spida)웜의 증가로 인해 해킹사고가 꾸준히 증가하고 있으며, Instant Messenger의 대중화에 따라 MSN, IRC 등과 같은 Instant Messenger의 보안 취약점이나 사회 공학적 접근을 이용한 해킹기법이 발생하고 있다[1,3].

이러한 현실에서 인터넷 웜과 트로이목마를 이용한 해킹 기법까지 포함한 바이러스의 피해는 이제 단순한 개인적인 호기심의 수준을 뛰어 넘어 집단적으로 광범위하게 이루어지고 있는 실정으로 이제는 IT 업계에 종사하지 않는 사람들에게까지도 해킹과 바이러스의 짓궂은 장난은 불편한 것 이상이 되고 있다.

이에 본고에서는 먼저 최근 이루어지고 있는 해킹과 바이러스의 공격대응 분야에 대하여 알아보고, 3장에서는 이러한 해킹과 바이러스 공격에 대한 CSIRT (Computer Security Incident Response Team)의 공조체계와 국내 · 외의 대응기술 동향을 살펴보고, 4장에서는 한국정보보호진흥원의 해킹 · 바이러스 관련하여 진행 중에 있는 4개의 연구과제들에 대해 간략하게 살펴보고, 5장에서는 결론을 맺는다.

2. 해킹 · 바이러스 공격대응 분야

해킹 · 바이러스의 공격기법은 현존하는 보안 시스템을 우회하여 네트워크의 가장 취약한 부분을 찾아 공격하거나 사용자 · 관리자의 빈틈이나 실수를 이용하여 악성코드를 유포하려는 노력의 결과라고 볼 수 있다. 그리고 이러한 변화는 바이러스 대응 분야와 침해사고 대응분야의 공통된 점이라고 볼 수 있다.

2.1 침해사고

사실 바이러스나 인터넷 웜의 공격과 시스템 침입 공격은 서로 비슷한 의미를 가진다. 바이러스는 자기복제가 가능하고 감염된 프로그램 · 시스템에서 불특정 다수의 다른 프로그램 · 시스템으로 감염되어 공격이 전이되는 형태를 가진다. 인터넷 웜은 여러 취약점을 이용하여 자동으로 네트워크상의 시스템에 침입하는 프로그램으로 독립적으로 복제되고 유포된

다. 이는 시스템 침입공격의 분산공격, 자동공격의 개념범주에 속한다. 따라서 바이러스나 인터넷웜에 대한 보다 효과적인 대응방법을 침해사고 대응방법에서 찾아볼 수도 있을 것이다.

침해사고대응 분야는 2000년 초 분산서비스거부공격(DDOS, Distributed Denial of Service Attack) 사고를 경험하면서 그 대응방법에 많은 변화가 일어나고 있다[4]. 무엇보다 침해사고에 대한 정보공유를 통하여 보다 빠르게 침해사고를 발견하여 예방하려고 하는 노력이 증가되었다.

침입탐지를 위해 IDS에만 의존하기보다는 네트워크 트래픽에 대한 모니터링이나 메일링 리스트를 통해 알려지지 않은 새로운 공격을 조기에 탐지하고자 하는 시도가 많아지고 있다. 또한 많은 전문가들이 시기적절하게 특정 보안문제에 대한 대응기술 및 지침을 템플릿 형태로 제공하고 있으며, 실제로 이러한 인터넷 커뮤니티 차원에서의 활동은 많은 일반 관리자들에게 올바른 보안인식과 기술력 향상을 가져왔으며, 새로운 공격에 보다 빨리 대응할 수 있는 능력을 향상시키고 있다.

2.2 바이러스 백신

바이러스 백신분야에 있어서 사용자들은 백신프로그램에 대한 강력한 해결책을 요구하고 있다. 첫 번째가 철저한 방어체제 구축이고, 두 번째는 사용자들이 필요로 하는 것을 조사하여 제품에 반영하도록 하는 것이다. 모든 시스템들은 알려지지 않은 바이러스 혹은 악성프로그램으로부터 공격을 받을 수 있으므로 최근의 백신기술은 이미 알려진 바이러스나 혹은 알려지지 않은 바이러스 모두에 대하여 연구하여야 한다.

현재 대부분의 백신 프로그램은 주로 시그니쳐 기반의 탐지기법으로 바이러스를 분별해내며, 새롭거나 이미 알려지지 않은 바이러스일 경우에는 탐지하지 못할 가능성이나 문제점을 일으킬 가능성을 지니고 있다. 바이러스에 의해 인터넷과 인트라넷 등에 감염된 파일을 배포하여 피해가 발생하기 전에 바이러스를 퇴치하기 위해 여러 가지 기법 등이 사용되고 있다. 이중 휴리스틱 진단기법은 백신엔진에서 새로운 바이러스라고 분류되지 않았으나 바이러스 군으로 의심되는 경우에는 이전에 가지고 있는 바이러스를 통하여 예견하는 것이다. 휴리스틱 스캐닝은 프로그램 기능에서 바이러스와 같은 행위를 하는 기법을 찾는다.

예를 들면 파일을 변경하거나, 백그라운드에서 함수호출, 전자우편 클라이언트에 접속 시도, 혹은 바이러스가 자기 자신을 복사하는 방법 등으로 이와 같은 유형의 행위들이나 혹은 그러한 성질을 가지고 있다면 엔진은 그 프로그램을 바이러스라고 판단을 한다.

2.3 실시간 스캔탐지(RTSD)

한국침해사고대응센터(CERTCC-KR)에서는 네트워크 스캔공격 모니터링을 위해 RTSD(Real Time Scan Detector)[5]을 배포하여 많은 사이트 관리자들이 사용하고 있으며, 탐지된 정보를 CERTCC-KR로 보고하고 있다. 이러한 정보는 국내 네트워크에 대한 공격 현황뿐만 아니라 새로운 인터넷 웜의 유포현황을 조기에 파악할 수 있도록 해 주고 있다.

3. 국내 · 외 대응기술 동향

3.1 국내 대응기술 동향

지금까지 FIRST(Forum of Incident Response and Security Teams)[6]를 중심으로 세계 각국의 CSIRT(Computer Security Incident Response Team, 침해사고대응팀)에서 침해사고예방 및 대응을 위해 노력해왔다. 하지만 대부분 org로서의 역할을 하기 때문에 적극적인 사고대응이 어려웠으며, 각 국가별 CSIRT간의 협조체계의 미비로 해킹사고에 대한 연계대응이나 정보공유에 있어서 한계점이 있었다. 현재 CERTCC-KR에서는 2002년 5월부터 호주, 일본, 싱가포르, 홍콩과 .APCERTF(AP CERT Task Force)을 구성하여 각 국가의 CERT간에 공조체계 확립을 위한 노력을 진행 중이다.

3.1.1 한국과학기술원

인터넷 트래픽 측정연구의 일환으로 트래픽 측정도구들의 적용 사례연구를 실시하고 있으며, 망의 유지 보수 및 관리를 위한 인터넷 트래픽 측정도구를 개발하여 망의 사용 성격 및 망 기기의 정상 작동을 확인하여 네트워크 트래픽을 모니터링하고 있다.

3.1.2 한국인터넷정보센터(KRNIC)

한국전자통신연구원(ETRI)과 공동으로 인터넷 트래픽 통계산출 시스템[7]을 개발하여 2001년 9월부

터 실험적용을 실시하여 ISP의 네트워크에 대한 패킷전송트래픽, 손실율 등의 정보를 수집하고 있다.

표 1 각 국가별 CERT 현황

국가	홈페이지
미국	http://www.cert.org
호주	http://www.auscert.org.au
일본	http://www.jpcert.or.jp
말레이지아	http://www.mycert.mimos.my
싱가포르	http://www.singcert.org.sg
중국	http://www.cert.org.cn
인도네시아	http://www.cert.or.id
대만	http://www.twcert.org.tw/eng
홍콩	http://www.hkcert.org
태국	http://thaicert.nectec.or.th
폴란드	http://www.nask.pl
캐나다	http://www.cancert.ca
네덜란드	http://cert-nl.surfnet.nl/
프랑스	http://www.renater.fr/
독일	http://www.cert.dfn.de/
덴마크	http://www.cert.dk/

3.2 국외 대응기술 동향

3.2.1 Incidents.org

Incidents.org[8]는 SANS(미국)가 운영하는 기구로 전 세계적으로 침입탐지, Forensics, 사고처리 등을 24시간 후 사고정보에 대한 서비스를 제공하는 사이트로 서비스에 필요한 데이터는 전 세계 60개국의 3000개 방화벽에서 수집하여 분석하고 있으며, 서비스 내용은 10개 주요 프로토콜 변화, 10대 공격 이용 서버 리스트, 주요 침입사례 등이다.

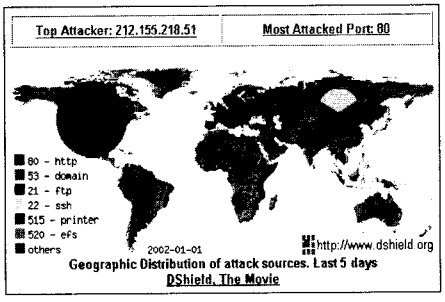


그림 1 Incidents.org

3.2.2 CAIDA(Cooperative Association for Internet Data Analysis)

인터넷의 효율적인 관리를 위하여 관련 모니터링 · 통계분석 · 3차원 표시도구를 개발하여 부하, 라우팅, 효율 등의 통계지수를 서비스하고 있다[9].

3.2.3 Security Focus사

Bugtraq 메일링 리스트와 취약점 데이터베이스를 보유하고 있는 Security Focus에서는 ARIS(Attack Registry & Intelligence Service)를 운영하여 해킹 · 바이러스에 대한 예방 및 대응활동을 수행하고 있다[10].

ARIS predictor는 IDS에서 발생하는 ATTACK DATA를 Attack Correlation Engine에서 수집하여 수집된 정보를 ARIS Database에 저장하고, ARIS의 전문가들에 의해서 수집된 정보를 분석한다. 그리고 그 분석된 결과에 따라 Alerts 또는 분석 결과를 관련 기관에 통보한다.

ARIS 특징으로는 다음과 같다.

- 글로벌 네트워크를 통한 침입경향 파악(105개국)
- IDS 만을 대상으로 분석
- 웹으로 정보를 쉽게 확인
- E-mail로 Alert와 분석 Report를 제공
- 체계적인 분석으로 각 기관의 보안관리 용이

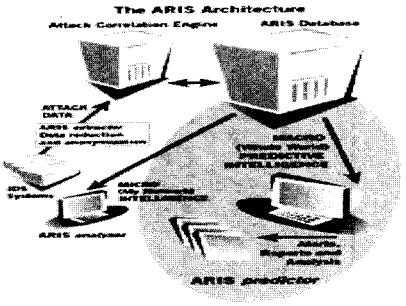


그림 2 ARIS Flow

3.2.4 CDA(Cyber Defence Alliance)

CDA(Cyber Defence Alliance)는 유럽국가들의 정보사회구현을 위한 노력의 일환의 하나로, 공동의 노력을 통하여 보다 더 안전하고 친숙한 정보사회를 만들기 위한 목적에 있다. CDA는 이와 같은 목적을 달성하기 위해 법률적, 기술적 조치들과 함께 각 기관이나 조직간 공동의 노력 등을 통하여 아래와 같은 일을 하고 있다[11].

- 백신업체와 보안기구들과의 범 국가적 공동 협력
- 사이버 범죄에 대한 유럽의회 지원

- 유럽간 정보보호기술(IST-Information Security Technology) 프로그램 지원.
- 바이러스 경보 · 보고
- 표준화 및 자동 보고기능
- 중앙집중 악성코드의 데이터베이스화
- 바이러스 명명법 통일화
- 백신 전문가들의 평가기준 및 요구조건 전문화
- 라이센스 및 자격증 제도
- 교육 등

4. 해킹 · 바이러스 대응 관련 연구과제

4.1 예 · 경보 자동화 시스템

현재 개발 중에 있는 해킹 · 바이러스 예 · 경보 자동화 시스템은 기존에 별도의 관리를 통해서 산재되어 있던 해킹 · 바이러스 대응 시스템들을 통합하고 수작업으로 이루어졌던 대응 프로세스를 자동화함으로서 시간적 지연을 최소화하며, 호스트 기반의 대응체계에서 벗어나 네트워크 기반의 대응체계를 구축함으로서 호스트 기반의 대응체계의 한계점을 극복하며 나아가 이러한 모든 시스템들을 통합함으로서 연계분석체계를 확립하여 빠른 예 · 경보와 예 · 경보 오류의 최소화를 목표로 한다.

표 2 예·경보 통합 시스템 구성요소

구분	예 · 경보 통합 시스템
데이터 수집범위	· 해킹사고접수 · 보안관련 국외 사이트 및 메일링리스트 · 국가 CERT팀간 공조정보 · 백신업체 제공 통계 및 바이러스정보 · 취약성DB · 네트웍 트래픽 측정 · 분석 시스템 · 보안장비 로그 수집/변환/분석 시스템
예 · 경보 배포채널	· Secure Messenger · 메일링 리스트 (CONCERT, Sec-INFO) · CERTCC 홈페이지 · 문자 메시지 발송 시스템
서비스/기능	· 확대된 예 · 경보 정보 · 자동화 처리로 신속한 대응 · 범국가적인 피해 통계 산출

4.2 컴퓨터 해킹 · 바이러스 피해액 산출방법에 관한 연구

컴퓨터 해킹 · 바이러스 피해액 산출방법에 관한 연구는 인터넷 이용의 활성화와 함께 급증하고 있는 컴퓨터 해킹 · 바이러스 사고로 인한 경제적 피해를 산출함으로써, 효과적인 컴퓨터 해킹 · 바이러스 방지대책 수립의 경제적 근거를 마련하고, 컴퓨터 해킹 · 바이러스 사고와 관련된 피해액 산출 방법 연구를 통한 기준을 마련한다.

4.3 바이러스 분류지침 및 통계자동화 S/W 개발

바이러스 분류지침 및 통계자동화 S/W 개발연구는 각각의 안티-바이러스 업체들의 바이러스에 관한 정보들의 불일치와 서로 다른 명명법 그리고 분류에 대한 명확한 기준이 부재로 없는 실정이다. 이에 따라, 바이러스 관련 분야의 기술들을 분석하여 세부적으로 분류하며 각각의 정보들간의 관계성을 명확히 하고, 이들 분류를 체계적으로 수립하는데 목적이 있다.

4.4 공개용 보안도구에 의한 해킹 · 바이러스 대응 모델 개발

공개용 보안도구에 의한 해킹 · 바이러스 대응 모델 개발은 공개 소스 보안도구들은 그 소스가 공개되어 있거나, 상용제품으로 변신하는 과정에서도 기본적인 기능을 가진 제품을 공개하고 있고, 비상업적인 용도로는 자유롭게 사용할 수 있도록 하고 있다. 이 과제에서는 이러한 다양한 공개용 보안도구들을 체계적인 분류를 통해 어떤 기능들이 어떻게 구현되고 사용할 수 있는지에 분석하고자 하며, 이러한 분류를 통해 추후 개발하고자 하는 해킹 · 바이러스 대응 모델을 구성할 제품을 선택하고 그에 대한 상세한 지침을 개발하며 사용자들이 무료로 사용할 수 있는 해킹 · 바이러스 대응 모델을 개발한다.

5. 결 론

해킹과 바이러스의 공격기법이 예전에는 단순히 특정 시스템의 버그를 공격하는 기법 및 이러한 취약점을 찾아주는 스캔 공격들이 주류를 이루었다. 그리고 좀더 나아가 침입차단시스템 및 기타 보안 시스템을 우회하기 위한 좀더 진보된 종류의 공격기법들이 나타났다. 하지만 최근에는 백오리피스로 대표되는 트로이목마, 그리고 인터넷 웜, 백도어 형태의 공격기법이 많이 등장하고 있으며, 이중 일부 공격도구들은 원격 제어까지 가능하다.

최근에 발견되는 해킹 · 바이러스 공격기법의 특

징을 종합해 보면 은닉화(Stealth), 분산화(Distributed), 에이전트화(Agent), 그리고 자동화(Automation)의 특징을 가지고 있다. 바이러스 또한 인터넷 웜과 트로이목마 같은 해킹 기술을 접목한 바이러스가 많이 등장하여 해킹과 바이러스의 경계가 모호해지고 있는 실정이다.

2000년에는 LKM 공격기법, Firewall 우회기법, Covert channel 기법, 에이전트 기법, 트로이잔 Planting 기법 등 깊이 있는 해킹기법의 문서 및 도구들이 많이 나왔다. 이러한 고도의 공격을 위한 충분한 자료가 인터넷을 통해 공개되어 있기 때문에 누구나 관심을 가지고 있는 사람은 손쉽게 제작할 수 있으며, 해외의 경우 조직적인 제작 그룹이 있어 지속적으로 기술이 발전되고 있는 추세이다. 따라서 최근의 해킹 · 바이러스 공격기법은 누구도 어떤 새로운 기능으로 나타나게 될지 예상할 수 없다.

또한 최근에는 해외의 해커들이 국내로 침입하는 사례가 매우 급격하게 증가하였으며 해킹 발생건수도 전년도에 비해 3배 이상 증가하였다. 대량의 호스트의 취약점을 손쉽게 알아내는 해킹도구를 이용하거나, 네트워크의 정상적인 동작을 방해하는 해킹수법 등 보다 지능적이고 자동화된 해킹기법을 이용하는 양상을 보이고 있다.

이에 본고에서는 국내 · 외의 해킹 · 바이러스에 대한 대응기술 동향을 살펴보았고, 현재 해킹 · 바이러스에 대한 한국정보보호진흥원의 연구과제들에 대하여 간략하게 알아보았다. 위에서 연구중인 과제를 통해 컴퓨터 해킹 · 바이러스 사고로 인한 경제적 피해를 정확하게 산출함으로써 효과적인 컴퓨터 해킹 · 바이러스 방지대책 수립의 경제적 근거를 마련하고, 서로 다른 업체들의 바이러스에 관한 정보들간의 관계와 분류를 체계적으로 수립하고있으며, 사용자들이 무료로 사용할 수 있는 해킹 · 바이러스 대응 모델이 개발되고 있다. 그리고, 기존의 시스템과 신규개발 시스템을 통합하여 해킹 · 바이러스 예 · 경보 시스템을 구축하고 있으며, 이에 따라 모든 대응 프로세스를 자동화하여 신속하고 정확하게 일반사용자에게 예 · 경보함으로서 해킹 · 바이러스로 인한 피해를 최소화할 수 있다는 것을 알아보았다. 앞으로 한국정보보호진흥원에서는 이 시스템을 더욱 보완 · 발전 시켜 해킹 · 바이러스 공격에 대한 보다 양질의 정보를 제공하기 위해 노력해야 할 것이다.

참고문헌

[1] 전완근, 2002년도 상반기 주요 바이러스 피해현황 및 동향 분석, http://www.certcc.or.kr/statistics/virus/virus-1.html

[2] 국내외 바이러스 발생현황, http://www.certcc.or.kr/statistics/virus/virus.htm

[3] 침해사고 접수 및 처리현황, http://www.certcc.or.kr/statistics/hack/hack.htm

[4] 조용상, Stacheldraht에 의한 서비스 거부공격 분석보고서, http://www.certcc.or.kr/paper/tr2000/2000-03/tr2000-03.html

[5] 실시간 네트워크 불법 Scan 자동탐지 도구, http://www.certcc.or.kr/cvirc/y2kvirus/down/RTSD/register.html

[6] FIRST(세계침해사고대응협의회), http://www.first.org

[7] KRNIC(한국인터넷정보센터), http://traffic.nic.or.kr/imap/sysconfig.html

[8] http://isc.incidents.org/about.html

[9] CAIDA(Cooperative Assoc-iationfor Internet Data Analysis), http://www.caida.org

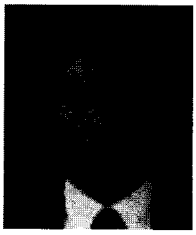
[10] Security Focus, http://aris.securityfocus.com/

[11] http://www.eicar.org/cda/index.htm

전 완 근

1998 한서대학교 전산정보학과(이학사)
2000 한서대학교 전산학과(이학석사)
2000 ~ 현재 한국정보보호진흥원 해킹바이러스상담지원센터 연구원
관심분야 : 컴퓨터 바이러스, 해킹, 인터넷 라우팅
E-mail : wkjeon@kisa.or.kr

임 재 명



1981 한양대학교 전자공학과(학사)
1983 한양대학교 전자공학과(석사)
1991 한양대학교 전자공학과(박사과정 수료)
2000~현재 한국정보보호진흥원 해킹바이러스상담지원센터 센터장
관심분야 : BIOS, 인터넷 네트워크 트래픽, QOS, RTOS, 컴퓨터 해킹 · 바이러스
E-mail : jmlim@certcc.or.kr