情 報 保 護 學 會 誌
第18卷 第1號, 2008. 2

인터넷 보안 동향 회고와 전망 분석

전 용 희*

요 약

작년 한 해 동안 국내 정보보호분야에서는 악성코드의 증가, 정보통신망법 개정, i-PIN 도입 등 커다란 사안이 많았다. 특히 통합보안솔루션의 부상과 시장 확대가 국내외의 화두가 되기도 하였다. 본고에서는 작년 국내외의 보안 기술 동향에 대하여 회고하여 보고, 금년 한 해 동안의 전망에 대하여 시만텍 등의 분석 보고서를 중심으로 기술하고자 한다. 이를 통하여 효과적인 보안 기술의 연구개발과 정책 수립에 지침이 되었으면 한다.

Ⅰ. 서 론

2008년 새해가 되기 전부터 국내외의 보안회사들은 새해 보안 동향에 대하여 분석 제시하고 있다. 특히 인프라 보안 분야의 전문회사인 시만텍(Symantec)사에서는 여러 가지의 보안 분석 보고서를 내놓고 있다[1-4]. 본고에서는 시만텍 사에서 제시한 2007년 보안 동향 회고에 대하여 기술하고, 2008년 보안 동향 전망에 대하여 살펴보고자 한다. 아울러 McAfee와 국내의 보안 기술 회고 및 동향 전망에 대하여도 소개하고자 한다[1, 5].

Ⅱ. 회 고

시만텍 사에 의하면 2007년에는 데이터 침해(data breach), 윈도 비스타, 스팸, 사이버범죄의 전문화가 보안 위협의 주류를 이루었다고 회고했다. 시만텍이 분석한 2007년 인터넷 보안동향은 아래와 같다[2]:

• 데이터 침해: Ponemon Institute의 2006년도 연구에 의하면 데이터 침해는 사고 당 평균 470만 달러의 손해를 발생시켰으며, 앞으로 더욱 더 많은 비용을 증가시킬 것이라고 예측하고 있다. 데이터 침해는 단순한 형태의 공격에서 특정 목표를 대상으로 하는 금전적인 동기를 가지고 있는 공격으로 공격 양상이 이동되고 있는 것으로 나타났다. 따라서 데이터 손실 방지 기술 및 전략에 대한 중요성이 점차 증대될 것으로 기대된다.

장비의 손실로 인한 데이터 침해도 심각하다. 모든 데이터 침해에서 컴퓨터나 데이터 저장 장치의 손실로 인한 데이터 침해가 46%로 나타났다.

Garter사의 전 IT 보안 분석가인 Amrit Williams에 의하면 어떤 공격의 목표가 금전적인 이득인 경우, 공격자는 시스템을 무조건 다운 시키는 것을 추구하는 것이 아니라, 정보 자체를 추구하는 것이므로, 공격은 조용하게 진행되게 되므로, 그 만큼 탐지 및 대응이 어려울 것으로 지적하고 있다. 이와 같은 경향에 따라 시만텍은 작년 11월에 데이터-누설 방지 회사인 Vontu사를 흡수하기로 약정을 맺었다. Cisco, Trend Micro, Websense 같은 경쟁 회사들도 유사한 인수를 하였다.

• 비스타 도입: 비스타의 채택이 증가함에 따라 악성 코드 작성자들에 의한 비스타에 대한 공격 관심도가 증가되었다. 이에 따라 윈도우 비스타 도입 이후 많은 보안 패치들이 발행되었다.

• 스팸(spam): 스팸 공격이 기승을 부렸으며, 이미지 스팸, PDF 스팸, MP3 스팸, 카드 스팸 등 새로운 대량 스팸들이 서버 자원을 더욱 고갈 시킬 것으로 예상된다. 사이버 마피아들이 생성하는 이런 쓰레기(garbage)들을 청소하는 것이 주요한 보안 산업이 되고 있다. 새로운 기법으로 봇넷(botnet)-구동 스팸이 발생되고 있다.

• 전문적인 공격 킷: 공격자들이 점차적으로 정교하고 조직화되는 경향이며 전통적인 소프트웨어와 유사한 방법을 채택하기 시작하였다는 분석이다. 그리고 야심찬 공격자를 위한 전문적인 툴 킷이 생성되고 있다.

* 대구가톨릭대학교 컴퓨터정보통신공학부(yhjeon@cu.ac.kr)

MPack이 이런 현상의 한 예를 보여준다.

• 피싱(phishing): 작년 전반기에 피싱 사이트의 증가율이 18%에 이르렀으며, 관측되었든 피싱 웹사이트의 42%가 세 가지의 피싱 공격 킷과 연관된 것으로 분석되었다. WebAttacker와 MPack와 같은 킷들은 다운로드만 하면 금방 구할 수 있는 것이다. 이런 툴 킷이 문제를 발생하는 것으로 조사되었다.

• 피싱으로 신뢰 브랜드의 공격: 신뢰된 웹 환경 공격을 통하여, 공격자는 희생자가 그 시스템에 올 때까지 기다리는 경향이 있다.

• 봇넷: 봇(Bot)과 봇넷(Botnet)이 비신뢰 컴퓨터로 잠입하고 있으며 다양한 악성 행위를 자행한다.

• 웹 플러그인 취약성: 웹 플러그인 취약성과 익스플로잇이 지속적으로 문제되고 있다. 액티브-X 제어가 대부분의 플러그인 취약성을 차지하고 여러 가지의 보안 위협을 제시하고 있으며, 취약 컴퓨터의 이용성, 기밀성과 무결성을 침해할 수 있다.

• 취약성 판매: 공개되지 않은 보안 취약성을 판매하기 위한 시장이 생성되고 있다. 이렇게 되면 보안 비용이 생각보다 많이 들것으로 예상된다. 예를 들어 WabiSabiLabi가 등장하여 취약성 정보를 팔기위한 경매 형태의 시스템을 제공한다.

• 가상화(virtualization): 가상화는 컴퓨터에서 컴퓨터 자원의 추출을 일컫는 광범위한 용어로 사용되고 있다. "물리적인 컴퓨터 자원의 특징을 다른 시스템, 응용프로그램, 최종 사용자들이 자원과 상호 작용하는 방식으로부터 감추는 기술"로 정의할 수 있다. 이로 인하여 하나의 시스템 안에 하나의 운영체제라는 틀에 더 이상 얽매일 필요가 없게 된다. 가상화에 대한 보안 문제는 아직 완전하게 이해되지 않은 보안 쟁점으로, 보안연구가들은 가상화 기술의 보안 의미에 대하여 연구하고 있다.

한편 국내에서는 악성코드 증가, 통합보안솔루션 시장의 확대, i-PIN 도입 등 여러 가지 일이 있었다. '정보보호 21c'에서는 아래와 같이 '2007 정보보호 HOT ISSUE 10'을 선정한바 있다[5].

• '정보통신망법'이 방송통신시스템보호법, 개인정보보호법, 정보통신망 이용자 보호법으로 확대 개정

• 인터넷 상에서 사용할 수 있는 주민번호 대체 수단인 i-PIN(Internet Personal Identification Number)의 도입 의무화

• 국내 PC 보안 및 개인정보 보안의 통합서비스화

• 신종 악성 코드 기승으로 인한 피해 증가

• 통합위험관리 UTM(Unified Threat Management) 시장의 확대

• 새로운 네트워크 방어체제인 NAC(Network Access Control) 제품의 보안시장 부상

• 일회용 비밀번호 보안 솔루션 OTP(One Time Password) 시스템 확대

• 전 세계 피싱(phishing) 사이트 15%가 국내에서 발생

• CC 인증의 민간평가기관으로 확대

• 통합정보보호 구축전략 컨퍼런스의 개최

보다 자세한 내용은 지면관계상 생략하며 [5]를 참조할 수 있다.

Ⅲ. 전 망

Symantec Global Intelligence Network로부터 수집된 자료와 200여명의 보안 분석가들이 내놓은 2008년 인터넷 보안 전망은 아래와 같다[3]:

• 더욱 강하고 복잡한 봇넷: 서비스 거부(DoS: Denial of Service) 공격과 스팸 전송 같은 공격에 봇이 이용되며, 행동이 다양화되고 진화될 전망이다. 봇넷은 은닉 수단의 새로운 방법이 되고 있으며 봇 좀비(Bot Zombie)에 의한 피싱 사이트도 예상된다.

• 진보된 웹 위협: 이용 가능한 웹 서비스의 수가 증가하고 브라우저가 JavaScript와 같은 통일된 스크립트 언어 표준화 경향에 따라 새로운 웹-기반 위협의 수가 증가될 것으로 전망한다. 예를 들어, AJAX와 같은 웹 2.0 기술을 이용한 멀웨어 위협이 있다.

• 모바일 플랫폼: 모바일 플랫폼이 광범위하게 사용됨에 따라, 모바일 장치를 목적으로 하는 보다 많은 수의 공격이 예상된다. 이에 따라 모바일 보안에 대한 관심이 증대될 것이다.

• 스팸의 지속적인 진화: 전통적인 차단 시스템을 피하고 사용자들을 속이기 위한 스팸이 지속적으로 진화될 전망이다.

• 가상화된 머신(virtualized machine) 공격에 대한 집중: 2007 보안 회고에서 지적한 바와 같이 올해에도 가상 머신에 대한 공격이 증대될 전망이다.

• 미국 대선의 관심을 끌기 위한 공격: 선거 전략에 인터넷 이용이 증가됨에 따라, 관련 보안 위험도 증가될

것으로 전망하고 있다. 이러한 예로는 후보자 공약 및 행동에 대한 잘못된 정보 분배, 피싱, 비밀성 침해 위협 등이 있다.

McAfee에 의하면 IM(Instant Messaging), 가상화, VoIP 소프트웨어에 대한 공격과 함께 웹 2.0 사이트, 윈도우 비스타 및 온라인 게임에 대한 위협이 증가될 것으로 보고 있다[1]. 윈도우 비스타 설치가 증가됨에 따라 공격도 증가될 것으로 예상하고 있다. 온 라인 게임에서 교환되는 가상 계정 등 가상 객체들이 금전적인 가치가 있기 때문에 더 많은 공격의 대상이 될 것으로 예상하고 있다. McAfee는 특히 Storm botnet가 악성 소프트웨어를 지속적으로 확산시켜 더욱 많은 PC들을 침해할 것으로 예상하고 있다. Storm botnet은 다른 botnet들이 감소되는 경향을 보여주는 반면 크기가 혼자 커지고 있는 경향이다. 이것은 정교한 코딩 기술 때문이며 암호화 채널 상으로 통신이 되며 시간이 지남에 따라 공격 방법이 바뀌기 때문이다.

기생 크라임웨어(parasitic crimeware)에 대한 증가도 예측되고 있다. 이 바이러스는 독립적인 파일을 설치하는 대신에 기존 파일에 데이터를 작성하여, 제거하는 것을 더욱 어렵게 만든다. 이 기법은 오래된 기술로써 최근 항-바이러스 프로그램들이 이런 전술에 잘 대처할 수 없는 점이 지적되고 있다. 또한 McAfee사는 VoIP 공격이 작년에 비하여 50% 증가될 것으로 예상하고 있다. 또한 가상화 소프트웨어에 대한 공격도 해커들의 관심이 될 것으로 예상하고 있다.

위의 전망을 통하여 다소 차이는 있겠으나 국내에서의 보안 기술 동향에 대하여도 자연스런 전망이 나올 것으로 판단된다.

Ⅳ. 맺음말

국내에서는 광대역통합망(BcN: Broadband Convergence Network)의 설치와 홈 네트워크의 보급으로 인하여 각 가정 가입자의 보안 의식에 대한 중요성이 증대되고 있다. 기업과 공공기관에서는 보안전문가를 통한 보안관리가 가능하기 때문에 보안 정책의 수립 및 시행이 상대적으로 쉬울 것이나, 그에 비하여 각 가정에서는 개인들이 자신이 보유한 컴퓨터의 보안을 대부분 책임져야 한다.

참고로 사이버범죄에 대항하기 위한 일반적인 원칙을 다음과 같이 소개한다[4].

- 의심스러운 이메일로 전송된 링크를 클릭하지 않는다. URL 창에 알고 있는 URL을 직접 입력한다.
- 모르는 송신자로부터의 이메일 부착물을 열지 않는다.
- 신용 카드 사용에 대한 정기적인 조사
- 온 라인 쇼핑에서 secure-HTTP 사용
- 항 바이러스, 항스파이웨어, 방화벽, 신원정보보호를 포함하는 인터넷보안 도구 유지. 운영체제, 브라우저 및 다른 응용들에 대한 최근 보안 패치 설치
- 디지털 상식-"온라인상에서 뭔가 이상하면, 진행하지 말라"의 이용

진정한 u-Society로 가기 위해서는 국내 정보보안 수준이 획기적으로 향상되어야 하고, 이를 위하여 정부, 학계, 기업 모두가 다 같이 노력해야 할 것이다. 또한 선진 보안 기술의 연구개발도 지속되어야 할 것이다.

참고문헌

[1] Thomas Claburn, McAfee Sees Cybercriminals Targeting Web 2.0, Window Vista, and Online Games, Information Week, Nov. 15, 2007.

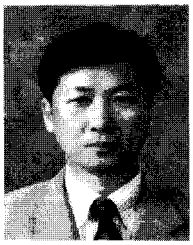
[2] Thomas Claburn, Symantec's Top 10 Internet Security Trends, Information Week, Nov. 16, 2007.

[3] Symantec, Cybercrime: Security Threat Trends for 2008, Overview, Symantec Security Response, http://enterprise.symantec.com,

[4] Symantec: trends van 2007 & 2008, Dec. 19, 2007. http://www.computertaal.info/

[5] 정보보호 21c, 2007 정보보호 Hot Issue 10, 2007년 12월호.

〈著者紹介〉



전 용 희 (Yong-Hee Jeon)
1971. 3 ~ 1978. 2 : 고려대학교 전기전자전파공학부
1985. 8 ~ 1987. 8 : 미국 플로리다공대 대학원 컴퓨터공학과
1987. 8 ~ 1992. 12 : 미국 노스캐롤라이나주립대 대학원 Elec. and Comp. Eng. 석사, 박사
1978. 1 ~ 1978. 11 : 삼성중공업(주)
1978. 11 ~ 1985. 7 : 한국전력기술(주)
1979. 6 ~ 1980. 6 : 벨기에 벨가톰사 연수
1989. 1 ~ 1989. 6 : 미국 노스캐롤라이나주립대 Dept of Elec. and Comp. Eng. TA
1989. 7 ~ 1992. 9 : 미국 노스캐롤라이나주립대 부설 CCSP (Center For Comm. & Signal Processing) RA
1992. 10 ~ 1994. 2 : 한국전자통신연구원 광대역통신망연구부 선임연구원
1994. 3 ~ 현재 : 대구가톨릭대학교 컴퓨터·정보통신공학부 교수
2001. 3 ~ 2003. 2 : 대구가톨릭대학교 공과대학장 역임
2004. 2 ~ 2005. 2 : 한국전자통신연구원 정보보호연구단 초빙연구원
2007. 1 ~ 2007. 12 : 한국정보보호학회 학회지 편집위원장
2008. 1 ~ 현재 : 한국정보보호학회 부회장
관심분야 : 네트워크 보안, 웜 모델링 및 대응 기술, 통신망 성능분석