침해사고 대응지원 데이터에 기반한 과학기술계 사이버위협 동향 분석

김미경*, 이윤수*

요약

급변하는 사이버 해킹에 능동적으로 대응하기 위해서는 사이버위협 상황에 대한 최신의 분석 데이터가 반드시 필요하다. 본 논문에서는 과학기술사이버안전센터(S&T-SEC)가 처리한 과학기술계 출연연구기관 및 첨단연구망에 대한 침해사고 대응 지원 데이터를 수집·분석하여 제공함으로써 정보보안 분야 연구자와 실무자들이 침해대응 기술연구 및 보안정책 수립을 위한 유용한 기초자료로 활용될 수 있을 것으로 기대된다.

Cyber Threat Trend Analysis Dedicated to Science and Technology Field Based on Incident Response Dataset

Mi-Kyoung Kim*, Youn-Su Lee*

ABSTRACT

Accurately analyzed data about cyber threat situation is required to research and develop of incident response technique and information security system actively, because hacking techniques are becoming more intelligent and diverse. In this paper, we analyzed cyber threat trend dedicated to S&T filed by using large amounts of actual incident response dataset collected by S&T-SEC. Analyzed results are useful to researchers and security officer who develop and enhance the incident response technique or establish a security policy as a basic dataset.

Key Words : Statistical Analysis of Cyber Threat Trend, Science and Technology Security Center, Information Security Events, Attack Port, Attack Nation

* 한국과학기술정보연구원(✉kimmik@kisti.re.kr)
· 제1저자(First Author) : 김미경 · 교신저자(Correspondent Author) : 이윤수
· 접수일(2012년 2월 18일), 수정일(1차 : 2012년 3월 16일), 게재확정일(2012년 3월 19일)

Ⅰ. 서 론

지난 2009년(7월 7일)과 2011년(3월 4일)에 발생된 DDoS 공격으로 사이버 해킹 공격은 단순한 해커의 실력과시를 벗어나 정치·경제·사회적인 문제로 인식하게 되었다. 특히, 금전탈취 위하여 민간 웹포털을 대상으로 빈번히 발생되던 DDoS 공격이 국가·공공 부문 웹사이트에 대한 공격으로 확장되면서 정치적이고 사회적인 이슈들이 빈번히 발생되는 현대사회의 특성으로 향후에도 지속적으로 발생될 것으로 예측된다.

이와 같이 급변하는 사이버위협 상황에 대한 체계적이고 효율적인 대응을 위해서는 사이버위협 동향에 대한 주기적이고 정밀한 수집·분석을 통해 변화하는 해킹기법과 대상에 대하여 능동적으로 침해대응기술을 연구·개발하고 적절한 보안정책을 수립·적용하는 것이 매우 중요하다. 따라서, 국내외 연구자들과 정보보안 전문기관에서는 자체적인 침해위협 데이터 수집 체계를 활용하여 위협동향을 분석하고 있으며, 이러한 통계분석 결과들은 학계와 산업계에서 정보보안기술 연구·개발을 위한 기초자료로 유용하게 활용되고 있다[1, 2, 3, 4, 5].

본 논문에서는 학계와 산업계에 종사하는 정보보안 관련 연구자·개발자 및 개별기관의 보안담당자들이 침해대응기술 개발 및 보안정책 수립 시에 참조할 수 있도록 최신의 사이버위협 동향 분석 정보를 제공하고자 한다. 특히, 본 논문에서 사용된 침해사고 대응지원 데이터들은 국내 국가·공공 부문 주요 부문관제센터 중에서 과학기술 분야 출연연구기관 및 첨단연구망에 대한 실시간 보안관제 및 침해대응 기술지원을 담당하고 있는 한국과학기술정보연구원(KISTI) 과학기술사이버안전센터(S&T-SEC)를 통해 수집·처리된 정보이다[6]. 따라서, 본 논문에서 제시한 사이버위협 동향 분석 결과는 국내 과학기술계에 특화된 해킹 경향을 제공하며 국내 타 부문관제센터(NCSC, KrCERT 등)에서 제공하는 정보와는 차별성을 확보하였다. 본 논문을 통해 분석된 과학기술계 사이버위협 동향 분석 결과는 정보보안 분야 연구자 및 실무자들에게 최신 해킹 동향에 대한 정보 습득과 차세대 보안기술 연구·개발에 유용하게 활용될 수 있을 것으로 기대된다.

본 논문의 2장에서는 과학기술계의 사이버위협 동향 분석을 위하여 과학기술 분야 주요 연구기관에 대한 보안관제를 담당하는 과학기술사이버안전센터를 소개하고, 3장에서는 과학기술사이버안전센터를 통해 최근 3년간 처리된 침해사고 대응지원 데이터를 기반으로 침해위협 유형, 침해위협 이벤트, 공격대상 포트 및 공격 국가의 4개 분야에 대한 통계적 기법을 적용하여 사이버위협 동향을 분석한 결과를 제시하며, 4장에서 결론을 맺는다.

Ⅱ. 과학기술사이버안전센터 소개

본 논문에서는 과학기술계의 사이버위협 동향을 분석하기 위하여 과학기술사이버안전센터에서 3년간 (2009년 1월 ~ 2011년 12월) 처리된 약 6천건의 침해사고 대응지원 데이터를 활용하였다.

우리나라는 사이버 침해사고에 대한 체계적이고 효과적인 탐지-분석-대응을 위하여 국가 차원에서 보안관제센터를 설치·운영하고 있으며 2011년 기준으로 약 20여개의 분야별 보안관제센터가 운영되고 있다[4]. 특히, 교육과학기술부 주관으로 과학기술 분야 정부출연연구소에 대한 실시간 보안관제, 침해대응 기술지원 및 침해사고 예방활동 등을 수행하기 위하여 2005년 한국과학기술정보연구원(KISTI)에 과학기술사이버안전센터(S&T-SEC)를 설치하여 운용 중에 있다[6].

과학기술사이버안전센터의 주요 역할은 <그림 1>에서 보이며, 2011년 현재 과학기술 분야 출연연구기관과 지역분·지원, 첨단연구망 이용기관 등 총 200여개 기관에 대한 전주기적 정보보호 활동을 수행하고 있다.

그림 1. 과학기술사이버안전센터 역할
Fig. 1 Major Roles of S&T-SEC

III. 사이버 침해사고 대응지원 동향 분석

본 장에서는 <그림 1>에서 소개한 과학기술사이버안전센터의 주요 역할 중에서 실시간 보안관제 및 침해사고 대응지원 수행 결과 수집된 최근 3년간(2009년 1월 ~ 2011년 12월) 정보를 기반으로 4개 유형(침해위협 유형, 침해위협 이벤트, 공격 포트 및 공격 국가)에 대한 동향분석 결과를 제시한다.

3.1 "사이버 침해위협 유형" 분석

최근 3년간 과학기술사이버안전센터에서는 <표 1>과 같이 총 6,286건의 실시간 침해위협 시도를 탐지·분석하고 대응지원 활동을 수행하였다.

표 1. 침해사고 대응지원 결과
Table 1. Incident Response Results by S&T-SEC

구분	웜·바이러스	경유지 악용	자료훼손·유출	홈페이지 위·변조	서비스 거부공격	단순침입 시도	합계
'09년	1,563	47	46	44	15	836	2,551
'10년	1,845	44	11	14	1	0	1,915
'11년	1,758	36	10	16	0	0	1,820
합계	**5,166**	**127**	**67**	**74**	**16**	**836**	**6,286**

특히, 과학기술사이버안전센터에서는 사이버 침해위협 시도를 "웜·바이러스", "경유지 악용", "자료훼손 및 유출" 등 총 6개의 유형으로 분류하고 있다.

침해위협 유형별 분포를 살펴보면 <그림 2>와 같이 "웜·바이러스" 유형이 전체의 82.2%를 차지하고 있었다. 이는 지난 "7·7 DDoS 대란"을 기점으로 다수의 웜·바이러스에 의한 좀비PC 감염 및 악성행위가 증가하여 이에 대한 집중적인 탐지·대응이 수행되었기 때문으로 분석되었다.

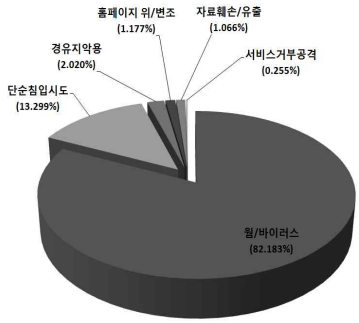

그림 2. 침해위협 유형별 분포
Fig. 2 Distributions of Incident Response Type

침해위협 유형별 월간 발생 추이는 <그림 3>에서 보이며, "웜·바이러스" 유형은 지난 2009년 DDoS 사건을 기점으로 크게 증가하여 지속적으로 발생하고 있는 것으로 나타났다. 또한, "단순침입시도" 유형은 스캔공격 등으로 대부분 개별기관의 방화벽 장비에서 차단되는 경향을 보임에 따라 2009년 말부터 대응지원 활동에서 제외되었다.

3.2 "침해위협 이벤트" 분석

지난 3년 동안 과학기술사이버안전센터를 통한 침해사고 대응지원 활동에는 총 5,922건의 침해위협 이벤트가 활용(이 중에서 364건의 침해사고 대응지원 활

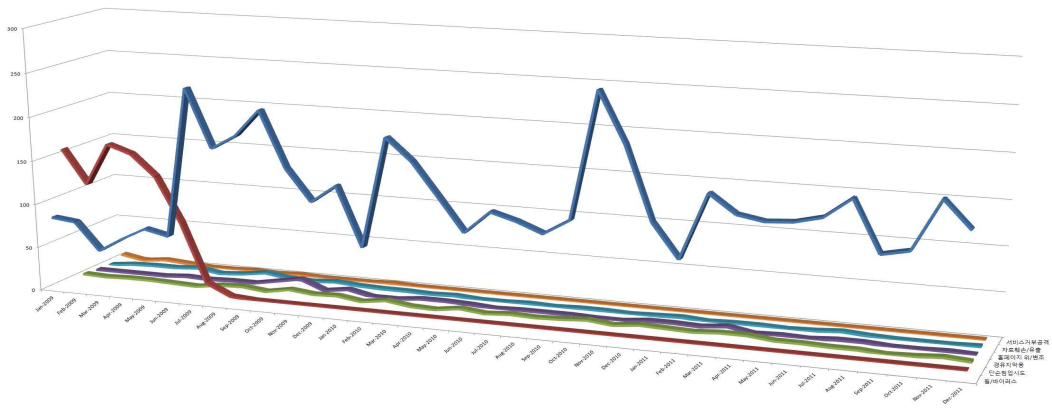

그림 3. 침해위협 유형별 발생 추이
Fig. 3 Statistics of Incident Response Type

동은 실시간 보안관제 이외의 사고신고·접수 등에 의한 것으로 상세 분석에서는 제외)되었다. 특히, 월간 평균 165건이 탐지되었으며 최대 272건(2010년 11월), 최소 63건(2009년 3월)이 탐지된 것으로 분석되었다.

또한, 총 300종의 침해위협 이벤트가 탐지되었으며, 이는 월간 평균 33종, 최대 53종(2010년 12월), 최소 16종(2009년 6월)이 탐지되었다.

침해위협 이벤트의 분포를 살펴보면 <그림 4>와 같이 "virus-trojan-conficker", "malware-downloader(fosniw)", "virus-trojan-agent(RookIE)" 등의 순으로 발생하였으며, 상위 10개 이벤트가 전체의 57.1%를 차지하고 있었다.

특히, 침해위협 이벤트 발생 빈도가 높은 상위 14종의 이벤트에 대한 월간 발생 추이를 살펴보면 <그림 5> ~ <그림 6>과 같다.

<그림 5>에서는 "virus-trojan-conficker"와 "virus-trojan-agent(RookIE)"가 비슷한 추세로 발생하는 경향을 보이고 있으며, 이는 이들 이벤트 사이에 연관성이 존재함을 추정할 수 있다. 또한, "malware-downloader(fonsiw)"는 2010년 11월에 관련 패턴 적용에 따라 지속적으로 발생하는 것을 확인할 수 있었다.

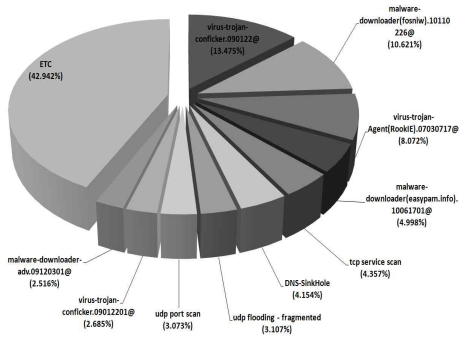

그림 4. 보안이벤트 분포
Fig. 4 Distributions of Security Events

기타 침해위협 이벤트 분석을 통해 발견된 특징으로는 <표 2>와 같이 다수의 침해위협 이벤트는 특정 월을 기점으로 더 이상 탐지되고 있지 않다는 것이다. 이는 특정 기간동안 유행하는 침해위협상황의 특성으로 인해 최초 유행시 지속적으로 탐지되다가 유행이

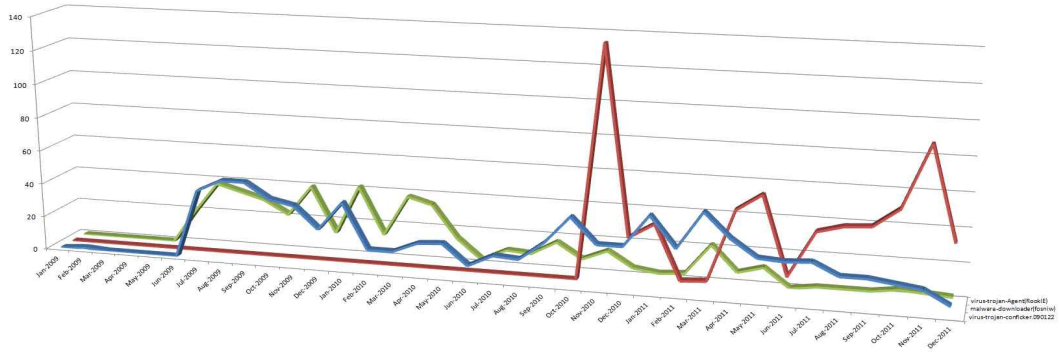

그림 5. Top-3 보안이벤트 발생 추이
Fig. 5 Statistics of Top-3 Security Events

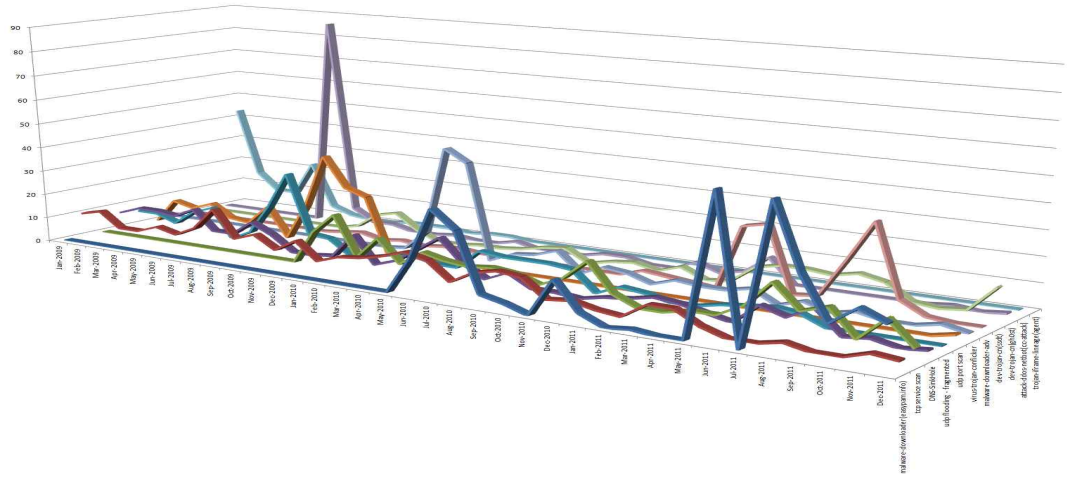

그림 6. Top-14 보안이벤트 발생 추이
Fig. 6 Statistics of Top-14 Security Events

지난 시점에서는 더 이상 사용되지 않기 때문인 것으로 분석되었다. 향후, 추가적인 분석을 통해 침해위협 탐지패턴에서 제거할 필요가 있다.

<표 2> 특이동향-1
<Table 2> Interesting Trend-1

순위	침해위협 탐지 이벤트명	미탐지기간
14	trojan-iframe-lineage(agent)	21개월
16	email subject - *Customer* (swen worm)	6개월
32	attack-ddos-relay-ip(**.**.**.**)	14개월
34	attack-web-webshell-cn(idpw)	8개월
46	malware-mac-info-ptrn	16개월

3.3 공격대상 포트 분석

지난 3년 동안 과학기술사이버안전센터를 통해 처리된 침해사고 대응지원의 공격대상 포트 정보를 분석한 결과 총 530종의 포트가 활용된 것으로 나타났다. 특히, 월간 평균 25종, 최대 51종(2011년 7월), 최소 8종(2009년 6월)이 탐지되었다.

공격에 활용된 프로토콜을 살펴보면 <그림 7>과 같이 TCP → UDP → ICMP 순으로 분석되었다. 특히, TCP는 487종, UDP는 42종이 공격에 사용되었다.

공격 프로토콜에 대한 월간 발생 추이를 도식화 하면 <그림 8>과 같다. UDP와 ICMP는 전체적으로 발생 빈도가 유사한 편이지만 TCP는 상대적으로 발생 빈도가 크고 특정 기간에 집중적으로 발생한 것을 알 수 있다.

공격대상 포트의 분포를 살펴보면 <그림 9>와 같이 "TCP/80", "UDP/ANY", "TCP/25" 등의 순으로 발생하였으며, 상위 5개 포트가 전체의 82.1%를 차지하고 있었다

특히, 발생 빈도가 높은 상위 18종의 공격대상 포트에 대한 월간 발생 추이를 살펴보면 <그림 10> ~ <그림 11>과 같다.

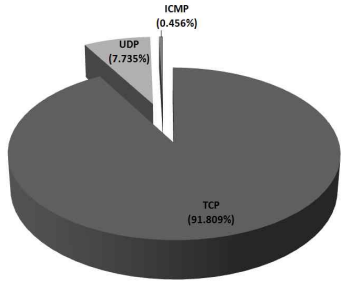

그림 7. 공격 프로토콜 분포
Fig. 7 Distributions of Network Protocol

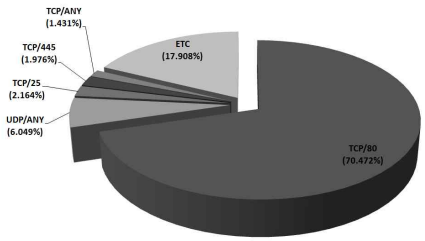

그림 9. 공격대상 포트 분포
Fig. 9 Distributions of Attack Port

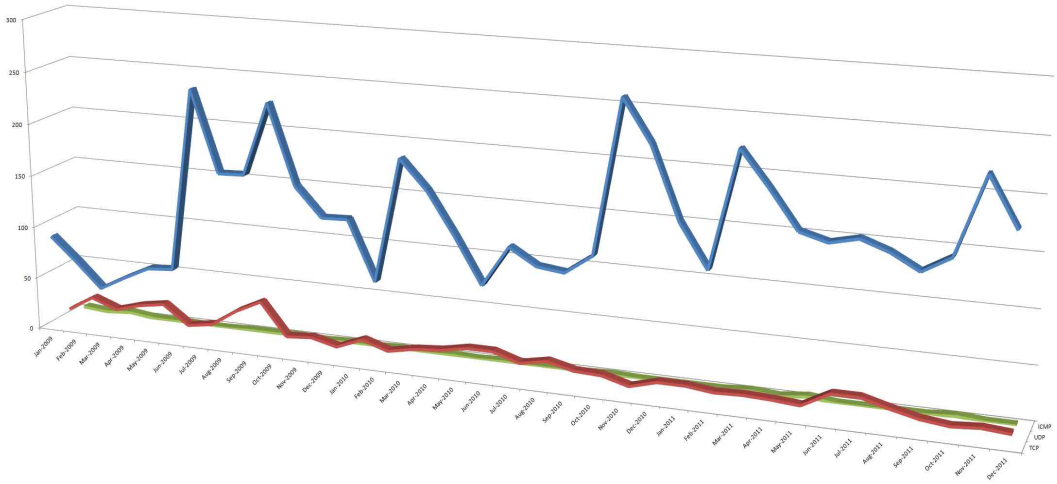

그림 8. 프로토콜별 발생 추이
Fig. 8 Statistics of Network Protocol

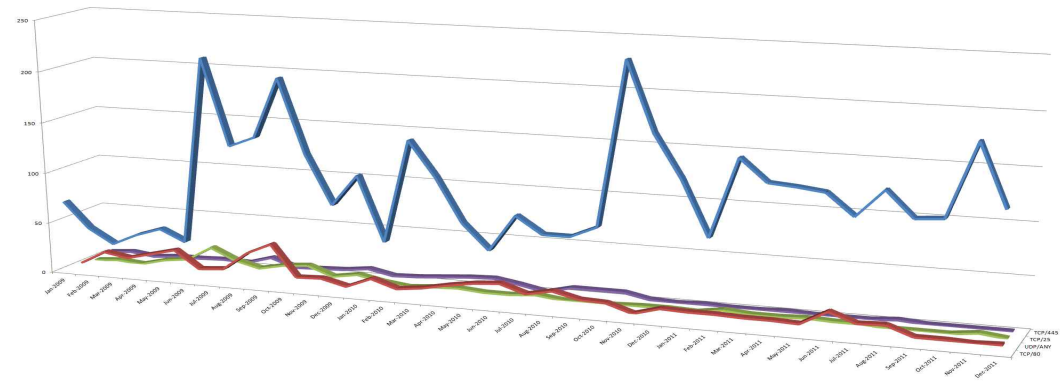

그림 10. Top-4 공격대상 포트 발생 추이
Fig. 10 Statistics of Top-4 Attack Port

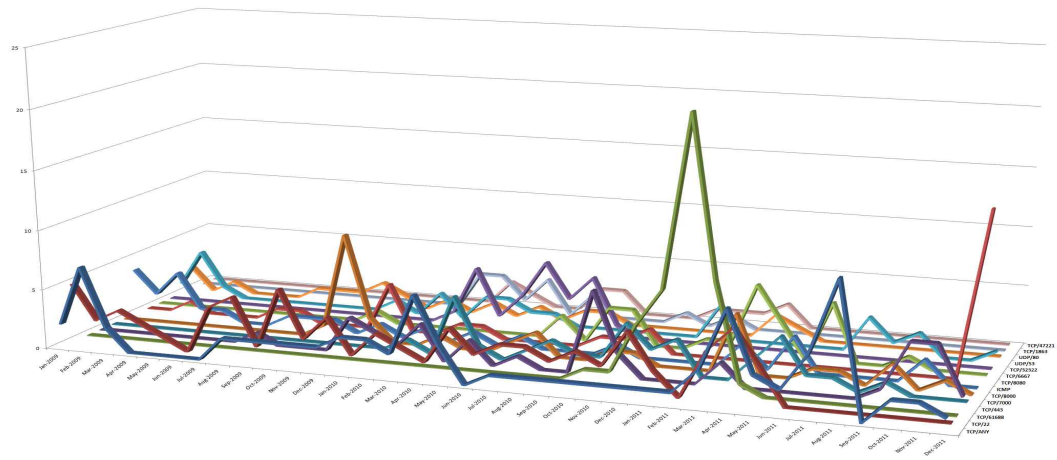

그림 11. Top-18 공격대상 포트 발생 추이
Fig. 11 Statistics of Top-18 Attack Port

<그림 10>에서는 "TCP/80"이 압도적으로 많은 것을 확인할 수 있었다. 이는 전체의 70.5%를 차지할 정도로 웹(홈페이지) 관련 해킹시도가 빈번히 발생하고 있으며 향후에도 집중적으로 보안관제를 수행해야 함을 의미한다.

<그림 11>에서는 "TCP/61688"과 "TCP/8080"이 상대적으로 많이 발생되고 있으며 특히 특정 기간에 급증하는 것을 확인할 수 있다. 이는 대규모 DDoS 공격에 활용된 좀비PC 제어와 관련되어 3월과 12월에 집중적으로 처리된 것으로 분석되었다.

기타 공격대상 포트 분석을 통해 발견된 특징들은 다음과 같다.

첫째, TOP-4에 해당하는 "TCP/80", "UDP/ANY",

"TCP/25", "TCP/445"는 전체 기간동안 발생되고 있는 반면 나머지 포트들은 특정 기간에만 발생되고 있는 것으로 나타났다. 이는 취약점 확인을 위한 스캔공격 및 웹 공격은 상시적으로 발생되는 반면 특정 포트들은 해당되는 취약점 발표 및 웜·바이러스 활동 시기와 맞물려 일시적으로 발생되기 때문인 것으로 분석되었다.

둘째, <표 3>과 같이 2종의 포트는 특정 기간에만 탐지되고 나머지 기간에는 전무한 것으로 확인되었다. 이는 특정 시점에 유행하였던 웜·바이러스의 특성 때문으로 "TCP/32322"는 "Back Oriffice"와 "TCP/61688"은 지난 DDoS 공격에 활용된 좀비PC와 관련된 것으로 분석되었다.

표. 3 특이동향-2
Table. 3 Interesting Trend-2

순위	공격대상 포트	집중탐지기간
7	TCP/61688	2010-10 ~ 2011-04
14	TCP/32322	2010-02 ~ 2010-09

3.4 공격 국가 분석

지난 3년 동안 과학기술사이버안전센터를 통해 처리된 침해사고 대응지원의 공격국가 정보를 분석한 결과 총 34개 국가에서 해킹공격 시도가 발생한 것으로 나타났으며, 공격 국가의 분포를 살펴보면 <그림 12>와 같이 "대한민국", "중국", "미국" 등의 순으로 발생하였다. 특히, 상위 3개 국가가 전체 공격의 98.4%를 차지하고 있으며, "대한민국"은 95.6%로 매우 큰 비중을 차지하고 있었다.

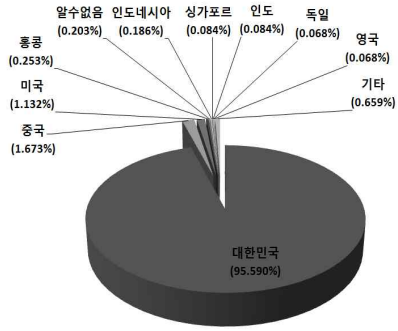

그림 12. 공격 국가 분포
Fig. 12 Distributions of Attack Nation

특히, 발생 빈도가 높은 상위 6개 국가의 월간 발생 추이를 살펴보면 <그림 13> ~ <그림 14>와 같다.

<그림 13>에서는 "대한민국"에서 발생한 해킹시도는 지속적으로 증가하는 추세이며, 2009년 7·7 및 2011년 3·4 DDoS 공격 시점에서 집중되고 있는 경향을 확인할 수 있다.

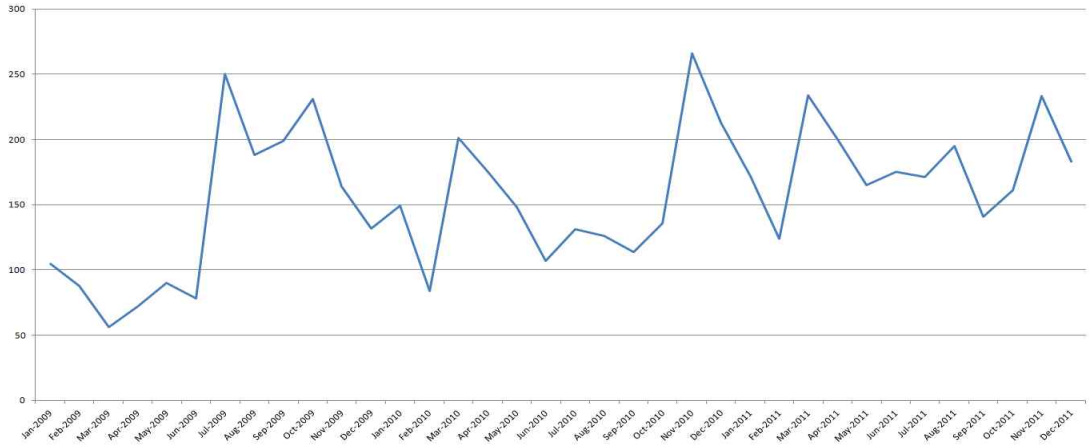

그림 13. Top-1 공격국가 발생 추이
Fig. 13 Statistics of Top-1 Attack Nation

<그림 14>에서는 "중국"과 "홍콩"이 유사한 시기에 공격시도가 급증한 것을 확인할 수 있다. 이는 1차적으로 확보된 경유지에 의해 동일 취약점에 대한 해킹시도가 증가하였기 때문인 것으로 추정된다.

기타 공격국가 분석을 통해 발견된 특징들은 다음과 같다.

첫째, "대한민국"과 "중국"은 지속적으로 공격시도가 발생하고 있음을 확인할 수 있다. 이는 정보통신 인프라가 급속히 발전한 한국의 IT 환경을 이용하여 개인정보 및 중요자료 탈취를 목적으로 하는 직접공격과 좀비PC 확보 및 경유지 확보 등의 간접공격이 활발히 시도되고 있기 때문인 것으로 분석되었다.

둘째, <표 4>와 같이 "인도네시아" 및 "공격자 미상(알수없음)"의 경우 특정 월에만 발생한 것으로 확인되었다. 이는 해당 국가에서 직접적인 해킹공격을 시도한 것이 아니라 악성코드에 감염된 좀비PC에 의한 공격시도가 발생한 것으로 분석되었다.

TOP-3 공격국가에서 발생한 침해위협 이벤트 유형을 살펴보면 다음과 같다.

표. 4 특이동향-3
Table. 4 Interesting Trend-3

순위	공격 국가	집중탐지기간
5	알수없음(공격자 미상)	2009-10
6	싱가포르	2009-10

TOP-1인 "대한민국"에서는 <그림 15>와 같이 총 266종의 보안이벤트가 발생하였으며, 상위 5개 보안이벤트(virus-trojan-conficker, malware-downloader(fosniw), virus-trojan-agent(RookIE), malware-downloader(easwpam.info), tcp service scan)가 전체의46.3%를 차지하였다.

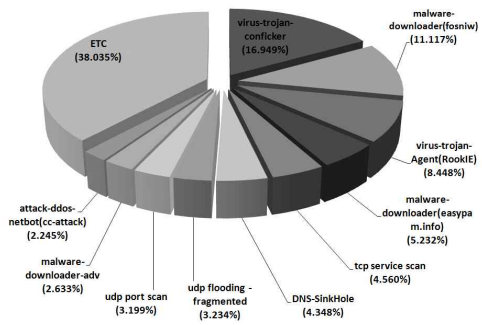

그림 15. 보안이벤트 분포(대한민국)
Fig. 15 Distributions of Security Event(Korea)

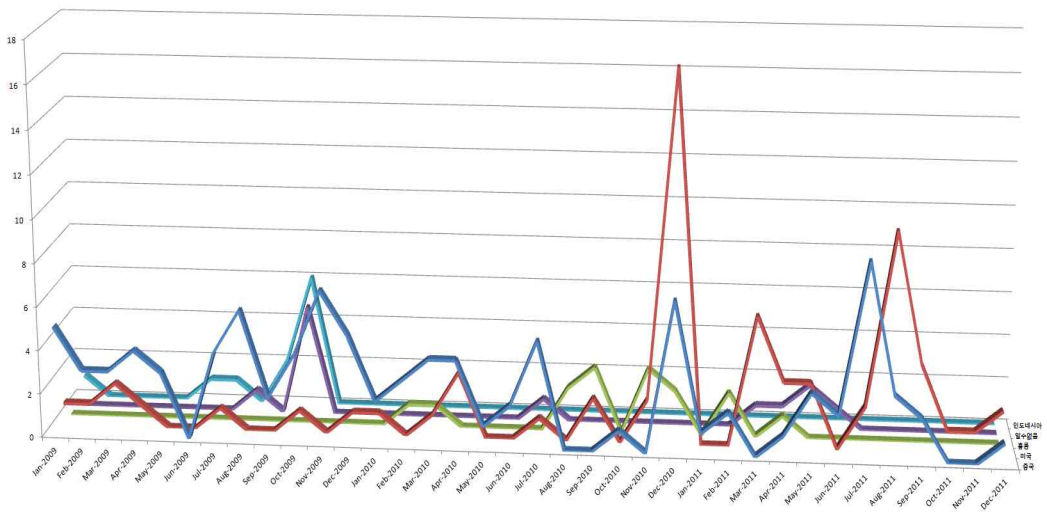

그림 14. Top-6 공격국가 발생 추이
Fig. 14 Statistics of Top-6 Attack Nation

TOP-2인 "중국"에서는 <그림 16>과 같이 총 21종의 보안이벤트가 발생하였으며, 상위 5개 보안이벤트(http sql injection attack, dev-trojan-cn(gh0st), attack-web-webshell-cn(idpw), dev-trojan-cn(baijin), virus-trojan-email(cn-gongji))가 전체의 75.8%를 차지하였다.

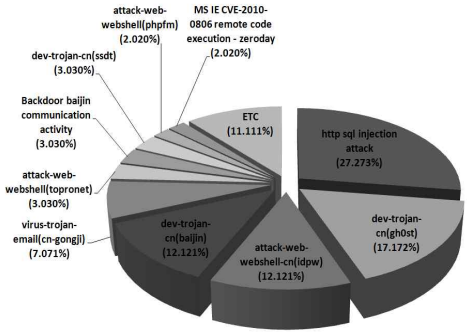

그림 16. 보안이벤트 분포(중국)
Fig. 16 Distributions of Security Event(China)

TOP-3인 "미국"에서는 <그림 17>과 같이 총 15종의 보안이벤트가 발생하였으며, 상위 3개 보안이벤트(dev-trojan-cn(ssdt), MS IE CVE-2010-0806 remote code execution - zeroday, dev-trojan-cn(gh0st))가 전체의 73.1%를 차지하였다.

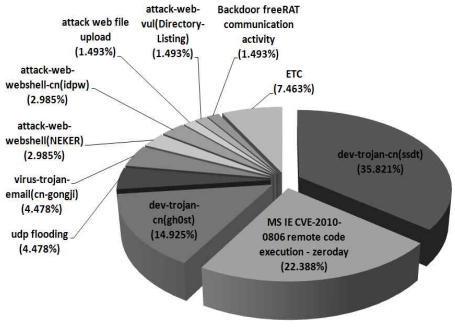

그림 17. 보안이벤트 분포(미국)
Fig. 17 Distributions of Security Event(USA)

Ⅳ. 결 론

본 논문에서는 과학기술계 주요 연구기간에 대한 실시간 보안관제 업무를 담당하는 과학기술사이버안전센터(S&T-SEC)에서 처리된 실제 침해사고 대응지원 데이터를 기반으로 "침해위협 유형", "보안이벤트", "공격대상 포트", "공격 국가" 등 총 4개 부문에 대한 사이버위협 동향을 분석한 결과를 제시하였다. 특히, 본 논문을 통해 분석된 과학기술계 사이버위협 동향은 다음과 같이 정리·요약할 수 있다.

① "침해위협 유형" 동향 : 2009년 7월 7일에 발생된 대규모 분산서비스거부공격(DDoS) 사건으로 인해 기존에는 홈페이지 위·변조 및 자료훼손·유출 등에 비교하여 상대적으로 위험도/중요도가 낮은 것으로 판단되던 웜·바이러스 유형이 급격히 증가하고 있으며, 향후에도 지속적으로 증가할 것으로 예측된다. 이는 웜·바이러스 유형의 해킹공격이 2차 공격(타겟형 공격) 시에 매우 유용하게 활용할 수 있는 좀비PC 확보에 매우 효과적이기 때문이며 최근 좀비군단 확보에 열을 올리고 있는 해커 트렌드와도 일맥상통하다고 볼 수 있다.

② "침해위협 이벤트" 동향 : 웜·바이러스와 관련된 이벤트가 상위에 랭크되었으며 전체의 약 50% 이상을 차지하고 있었다. 특히, 트로이목마/백도어 기능이 포함된 이벤트(conficker, fonsiw, RookIE 등)가 집중적으로 발생되고 있으며 향후에도 지속적으로 증가할 것으로 예측된다. 그러나, 일부 이벤트들은 유행에 매우 민감하여 특정 시점동안만 발생되다가 더 이상 사용되지 않는 경향을 보이기 때문에 각급 사이버안전센터들은 이와 관련된 체계적이고 효율적인 침해위협 탐지패턴 관리가 필요할 것으로 보인다.

③ "공격대상 포트" 동향 : 공격에 사용된 네트워크 프로토콜은 TCP → UDP → ICMP 순으로 발생하였으며 TCP/80이 전체의 70.5%를 차지하고 있었다. 이는 일반 사용자가 의심스러운 웹사이트에 접속하였을 경우 백그라운드에서 쉘코드 등 악성코드가 설치되거나

좀비PC가 정보유출 등을 목적으로 특정 웹페이지에 접속을 시도하기 때문인 것으로 분석되었으며, 향후에도 지속적으로 발생할 것으로 예측된다. 또한, 보안이벤트와 유사하게 일부 포트들도 유행에 민감하여 특정 기간 동안에만 집중적으로 발생하는 경향을 보였다.

④ "공격 국가" 동향 : 국내 과학기술계에 대한 해킹 시도는 대한민국 → 중국 → 미국 등의 순으로 발생하였으며 대한민국이 전체의 95.6%를 차지하고 있었다. 이는 세계 최고 수준의 인터넷 사용 인프라를 보유하고 있는 우리나라의 특성 때문으로 국내외로부터 웜·바이러스가 유입되어 좀비PC화 되어 이들에 의한 추가 공격이 발생되기 때문이며 향후 지속적으로 증가할 것으로 예측된다.

본 논문에서 제시한 과학기술계 사이버위협 동향 분석 결과는 다양한 정보보안 분야 연구자, 개발자 및 실무담당자들이 침해대응기술 연구·개발 또는 보안정책 수립 등 보안활동 수행 시에 유용한 참고자료로 활용할 수 있을 것으로 기대된다.

참고문헌

[1] 시만텍, http://www.symantec.com/
[2] 안철수연구소, http://www.ahnlab.com/
[3] 인터넷침해대응센터, http://www.krcert.or.kr/
[4] "2011년 국가정보보호백서", 방송통신위원회, 2011.5.
[5] Jungsuk Song, Hiroki Takakura, et al., "Statistical Analysis of Honeypot Data and Building of Kyoto 2006+ Dataset for NIDS Evaluation," Proceedings of the 1st Workshop on BADGERS, pp.29-36, 2011.
[6] 과학기술사이버안전센터, http://www.sntsec.or.kr/

저자소개

김미경 (Mi-Kyoung Kim)

2002년 한남대학교 컴퓨터공학과 (공학사)
2008년 충남대학교 대학원 컴퓨터공학과 (공학석사)
2010년~현재 한국과학기술정보연구원 과학기술사이버안전센터 연구원
※ 관심분야 : 데이터베이스, 분산컴퓨팅, 침해대응기술연구

이윤수 (Youn-Su Lee)

2007년 전남대학교 산업공학과 (공학사)
2010년 충남대학교 대학원 컴퓨터공학과 (공학석사)
2007년~현재 한국과학기술정보연구원 과학기술사이버안전센터 연구원
※ 관심분야 : 정보시스템 보안취약점 점검·분석, 침해대응시스템 연구·적용