통계적 보안이벤트 분석 기반의 글로벌 사이버위협 동향 분석

이윤수*, 김미경*

요 약

사이버 해킹 공격이 지속적으로 지능화·다양화 되는 경향을 보임에 따라 효과적인 침해대응 기술 및 정보보호시스템 연구·개발을 위해서는 정확한 사이버위협 상황에 대한 분석 데이터가 반드시 필요하다. 본 논문에서는 보안관제센터를 통해 실제 네트워크 상에서 수집된 대량의 보안이벤트 정보를 활용하여 최신 글로벌 사이버위협 동향을 분석한 결과를 제시하였다. 제시한 결과는 정보보안 분야 연구자, 개발자 및 개별기관 보안담당자들이 침해대응기술 연구·개발 및 보안정책 수립 등을 위한 기초자료로 유용하게 활용될 수 있을 것이다.

Global Cyber Threat Trend Analysis Based on Statistics of Information Security Events

Youn-Su Lee*, Mi-Kyoung Kim*

ABSTRACT

Accurately analyzed data about cyber threat situation are required to research and develop of effective incident response technique and information security system, because hacking attacks are becoming more intelligent and diverse. In this paper, we analyzed global cyber threat trend by using large amounts of information security events which are collected by actual cyber security center. Analyzed results are useful to researchers, developer and security officer who develop and enhance the incident response technique or establish a security policy as a basic dataset.

Key Words : Global Cyber Threat Trend, Statistical Analysis, Information Security Events, Attack Port, Attack Nation

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

Ⅰ. 서 론

정보화 사회는 컴퓨터와 인터넷의 발전을 토대로 급격한 성장을 거듭하였고 경제·문화·사회 등 우리 삶 곳곳에 필수불가결한 존재로 자리 잡으며 지대한 영향을 미치고 있다. 그러나 최근 언론을 통해 빈번히 접하게 되는 해킹사고 소식들은 정보화의 역기능 역시 증대되고 있음을 깨닫게 한다. 개인정보 유출·중요정보 탈취·주요 서비스 및 전산망 마비 등 해킹사고를 미연에 방지하고 건전한 정보화 사회를 조성하기 위해, 정보보호 활동은 이제 "선택"이 아닌 "필수"사항이라 할 수 있겠다.

체계적이고 효율적인 정보보호 활동을 위한 노력은 다양한 분야에서 있어왔다. 산업계에서는 침해위협 유형별 특성에 적합한 각종 정보보호시스템(침입차단시스템, 침입탐지시스템, 침입방지시스템, 통합보안관리시스템 등)을 연구·개발하여 제공하고 있으며, 연구자들은 침해위협 동향 분석을 기반으로 신종 침해대응시스템 연구 및 정보보호시스템의 성능 최적화, 효율적 사용방법론 등에 대한 연구를 활발히 수행하고 있다.

그러나 최근 사이버 해킹 공격은 그 목적과 방법이 지능화·다양화 되는 경향을 보이고 있으며, 신종·변종 공격이 지속적으로 증가하면서 기존에 연구·개발된 정보보호 시스템과 침해대응 기술에만 의존해서는 효율적인 대응이 현실적으로 불가능한 실정이다. 새로운 대안제시를 위해 , 사이버 위협상황에 대한 실시간 모니터링을 수행한 결과를 기반으로 글로벌 위협동향을 분석하고 그 결과를 피드백 하여 침해위협 탐지패턴 및 정보보호시스템 고도화에 활용하는 것이 매우 중요한 연구 분야라 할 수 있다.

이러한 시대적 요구에 발맞춰 글로벌 정보보안 기업들과 정보보안 관련 연구자들, 그리고 정보보안 관련 국가·공공기관들이 사이버 침해위협 데이터를 수집, 정기적인 분석 결과 발표를 수행하고 있으며, 이러한 데이터들은 산업계와 학계에서 보다 효율적인 정보보안 메커니즘 연구·개발을 위한 기초자료로 유용하게 활용되고 있다[1, 2, 3, 4, 5].

이러한 배경에서, 본 논문에서는 침해대응 기술 연구자 및 정보보호시스템 개발자들이 신종·변종 해킹공격 대응기술 및 시스템 개발에 활용할 수 있는 글로벌 보안이벤트를 자체적으로 수집하고, 통계적 기법을 적용하여 분석한 글로벌 사이버위협 동향 분석 결과를 제시하고자 한다. 특히, 과학기술 분야 연구기관에 대한 실시간 보안관제 및 침해대응 기술지원을 담당하고 있는 과학기술사이버안전센터(S&T-SEC)에서 최근 18개월간 수집된 데이터를 활용하여 사이버위협 동향을 분석하였다[6]. 본 논문에서 제시한 글로벌 사이버위협 동향 분석 결과는 과학기술 분야에 집중된 침해위협 데이터를 기반으로 한다. 이는 국내 타 부문관제센터(KISA/KrCERT 등)가 수집·분석한 데이터와는 차별화 되어 특정 분야만의 사이버위협을 파악하는데 효과적인 정보를 제공할 수 있다. 또한 글로벌 정보보호 업체 및 타 부문 동향분석 결과와의 비교·분석에도 연구자 및 개발자들이 매우 유용하게 활용할 수 있을 것으로 기대된다.

본 논문의 2장에서는 글로벌 사이버위협 동향 분석을 위한 보안이벤트 수집 체계를 소개하고, 3장에서는 수집체계를 통해 국내에 유입된 18개월 간의 데이터를 기반으로 침해위협 이벤트, 공격대상 포트 및 공격 국가의 3개 부분에 대한 통계적 기법을 적용하여 글로벌 사이버위협 동향을 분석한 결과를 제시하며, 4장에서 결론을 맺는다.

Ⅱ. 보안이벤트 수집 체계

본 논문에서는 글로벌 사이버위협 동향을 분석하기 위하여 과학기술사이버안전센터에서 18개월(2010년 7월 ~ 2011년 12월) 동안 수집한 약 2억 5천만건의 보안이벤트 데이터를 활용하였다.

과학기술사이버안전센터는 과학기술 분야 연구기관에 대한 실시간 보안관제·분석 및 대응기술지원을 목적으로 2005년 설립된 국내 주요 부문보안관제센터 중 한곳이다[4, 6]. 특히, 과학기술사이버안전센터는

실시간 위협상황 모니터링을 수행하기 위하여 <그림 1>과 같은 보안이벤트 수집 체계를 구축하여 운용하고 있으며, 2011년 기준으로 총 37개 연구기관 네트워크 백본에서 침해위협 이벤트를 수집하여 실시간 보안관제 업무를 수행하고 있다.

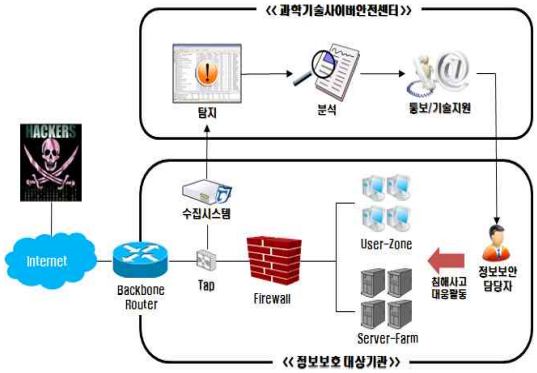

그림 1. 보안이벤트 수집 체계
Fig. 1. Collection Scheme of the Security Event

침해위협 이벤트의 분포를 살펴보면 <그림 2>와 같이 "udp flooding", "tcp service scan", "udp port scan" 등의 순으로 발생하였으며, 상위 5개 이벤트가 전체의 84.4%를 차지하고 있었다.

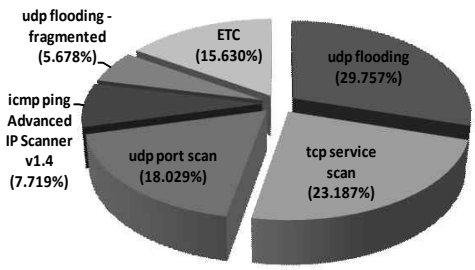

그림 2. 보안이벤트 분포
Fig. 2. Distributions of Detected Security Events

III. 사이버위협 동향 분석

본 장에서는 <그림 1>에서 제시한 보안이벤트 수집 체계를 통해 획득한 정보를 기반으로 3개 유형(침해위협 이벤트, 공격 포트 및 공격 국가)에 대한 동향분석 결과를 제시한다.

3.1 침해위협 이벤트 부문

지난 18개월 동안 과학기술사이버안전센터에서는 총 254,179,797건의 침해위협 이벤트가 탐지되었다. 특히, 월간 평균 14,121,100건이 탐지되었으며 최대 25,686,432건(2011년 6월), 최소 7,252,667건(2010년 9월)이 탐지된 것으로 분석되었다.

또한, 총 847종의 침해위협 이벤트가 탐지되었으며, 이는 월간 평균 329종, 최대 408종(2011년 10월), 최소 262종(2010년 9월, 2010년 10월)이 탐지되었다.

특히, 침해위협 이벤트 발생 빈도가 높은 상위 10종의 이벤트에 대한 월간 발생 추이를 살펴보면 <그림 3> ~ <그림 4>와 같다.

<그림 3>에서는 "udp flooding"이 발생하기 전월에 "udp port scan"이 급증하는 것을 확인할 수 있다. 따라서, 향후 보안이벤트 탐지 시에 "udp port scan"과 "udp flooding" 이벤트의 상관관계 분석을 통해 분산 서비스거부공격(DDoS)의 조기 예경보에 활용할 수 있을 것이다.

<그림 4>에서는 "mstream attacker prompt3"와 "mstream attacker promt"가 동일한 기간에 급증하였으며, "udp flooding - same ip"와 "IPSwitch WS_FTP Logging Server Daemon Denial of Service" 이벤트가 유사한 기간에 발생하였음을 확인할 수 있다. 따라서, 이들 보안이벤트 간에 연관성이 존재함을 추측할 수 있다.

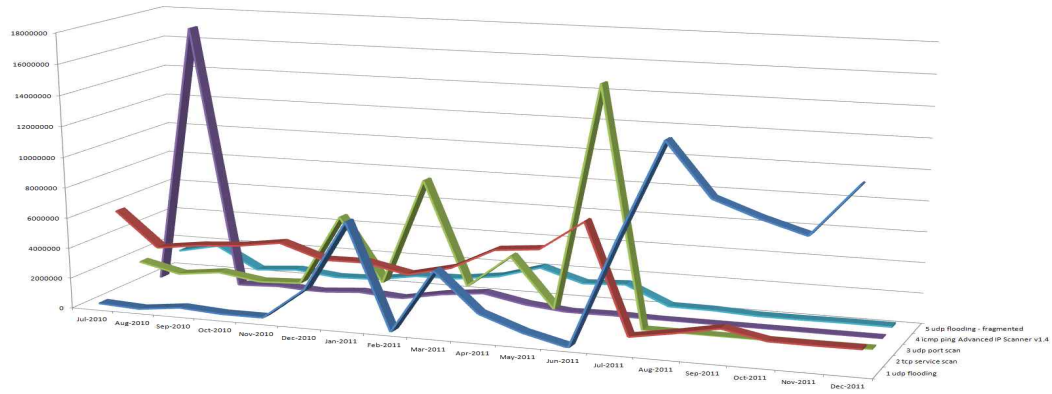

그림 3. Top-5 보안이벤트 발생 추이
Fig. 3. Statistics of Top-5 Security Events

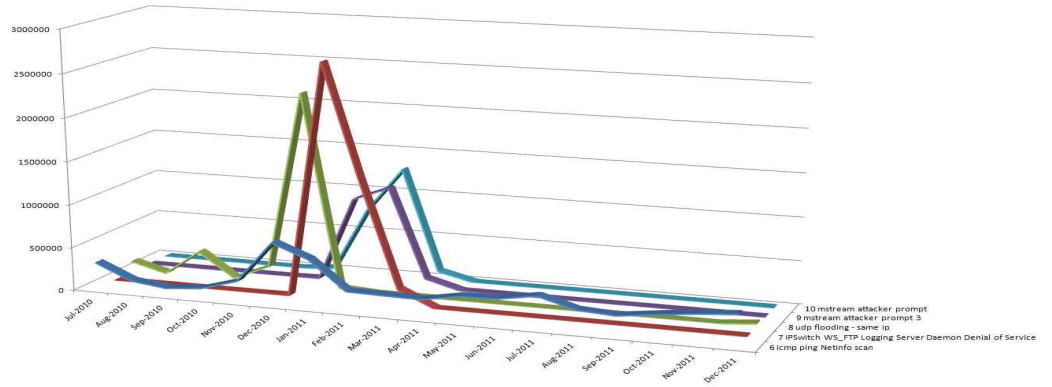

그림 4. Top-10 보안이벤트 발생 추이
Fig. 4. Statistics of Top-10 Security Events

기타 침해위협 이벤트 분석을 통해 발견된 특징들은 다음과 같다.

첫째, <표 1>에서 보인 14종의 침해위협 이벤트는 2011년 6월을 기점으로 더 이상 탐지되지 않았다. 이는, 관련 보안취약점에 대한 해킹 성공률 감소에 따라 해킹시도가 감소한 것으로 추측된다.

둘째, <표 2>와 같이 특정 침해위협 이벤트들은 특정 기간에만 집중적으로 탐지되었다. 이는, 특정 기간에만 활동하도록 조작된 웜/바이러스의 특성에 따른 것으로 보인다.

표 1. 특이동향-1
Table 1. Interesting Trend-1

순위	침해위협 탐지 이벤트명
4	icmp ping Advanced IP Scanner v1.4
20	http directory traversal
40	email subject - *Customer* (swen worm)
46	virus-trojan-irc-upload(upfile)
65	http sql injection expression union select
83	rpc dcom interface overflow exploit
88	ping of death/jolt/jolt2
97	tfn client command be
109	malware-signal-infection
115	email subject - *Near* (neroma worm)
121	http frontpage
125	http sql injection keyword (124)%2b
127	tftp parent directory
128	http sql injection expression and 1=1

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

순위	침해위협 탐지 이벤트명	집중탐지기간
33	malware-zbot-download(bin-ru)	2010년 10월
50	attack-DDoS-darkness-bot	2011년 9월
61	snmp show rmon	2010년 9월, 11월
81	attack-ddos-relay-ip(**.**.**.**)	2011년 7월, 8월
95	virus-trojan-conficker	2010년 10월
106	http Nessus scan user-agent header	2011년 10월, 11일
107	IIS web server vulnerability 2	2011년 12월
108	snmp trap handling agentx/tcp request	2010년 8월, 11월

3.2 공격대상 포트 부문

지난 18개월 동안 과학기술사이버안전센터에서 탐지된 침해위협 이벤트의 공격대상 포트 정보를 분석한 결과 총 128,517종의 포트가 활용된 것으로 나타났다. 특히, 월간 평균 40,542종, 최대 87,269종(2011년 8월), 최소 7,529종(2011년 2월)이 탐지되었다.

공격에 활용된 프로토콜을 살펴보면 <그림 5>와 같이 UDP → TCP → ICMP 순으로 분석되었다. 특히, UDP는 65,490종, TCP는 63,026종이 공격에 사용되었다.

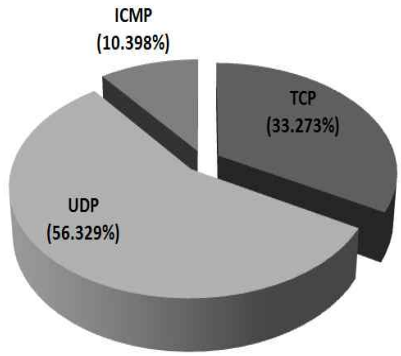

그림 5. 공격 프로토콜 분포
Fig. 5. Distributions of Cyber-attack Protocol

공격 프로토콜에 대한 월간 발생 추이를 도식화 하면 <그림 6>과 같다. UDP와 TCP는 전체적으로 발생 빈도가 유사한 편이지만 ICMP는 특정 기간에만 집중적으로 발생한 것을 알 수 있다.

공격대상 포트의 분포를 살펴보면 <그림 7>과 같이 "UDP-0", "ICMP", "TCP-1433" 등의 순으로 발생하였으며, 상위 5개 포트가 전체의 52.3%를 차지하였다.

특히, 발생 빈도가 높은 상위 10종의 공격대상 포트에 대한 월간 발생 추이를 살펴보면 <그림 8> ~ <그림 9>와 같다.

<그림 8>에서는 "UDP-0", "UDP-53(DNS 관련)" 및 "ICMP"가 특정 기간에 집중되고 있다는 것을 확인할 수 있다. 이는 특정 보안취약점 발표와 맞물려 해당 취약점을 이용한 해킹공격시도가 급증하기 때문인 것으로 분석되었다.

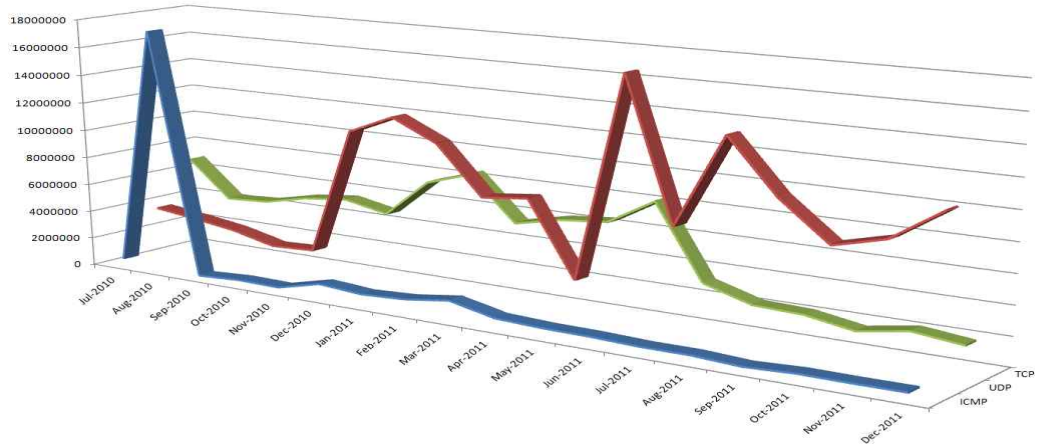

그림 6. 프로토콜별 발생 추이
Fig. 6. Statistics of Network Protocol

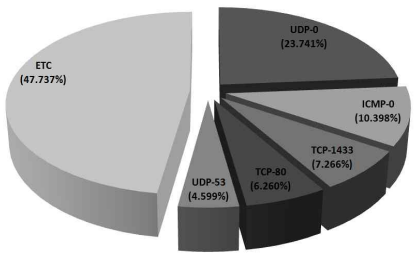

그림 7. 공격대상 포트 분포
Fig. 7. Distributions of Attack Port

<그림 9>에서는 "UDP-80"과 "UDP-5151"가 특정 기간에 집중되고 있으며, "TCP-3306"은 지속적으로 증가 및 감소를 반복하다가 특정 시점에서 공격이 사라진 것을 확인할 수 있다. 이는 MySQL과 WS_FTP 관리자 로그인 상의 취약점을 이용한 공격이 유행하다가 보안패치 적용 시점에서 사라진 것으로 분석되었다.

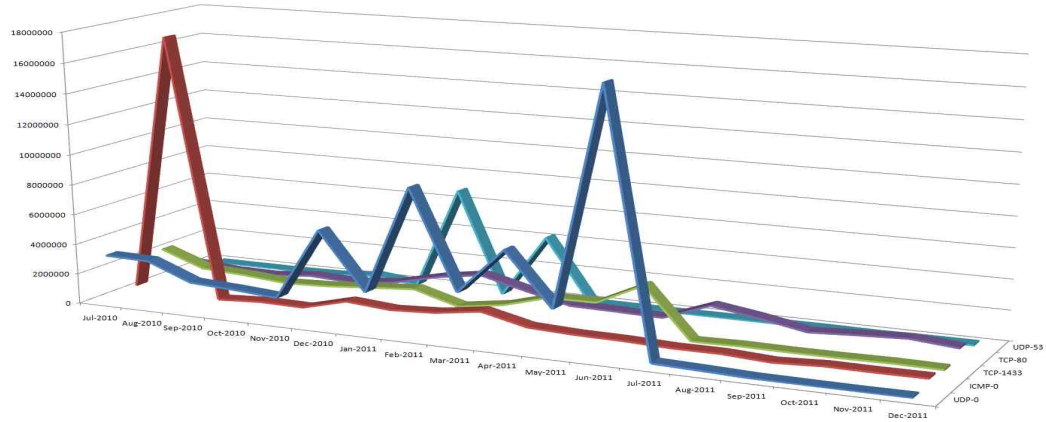

그림 8. Top-5 공격대상 포트 발생 추이
Fig. 8. Statistics of Top-5 Attack Port

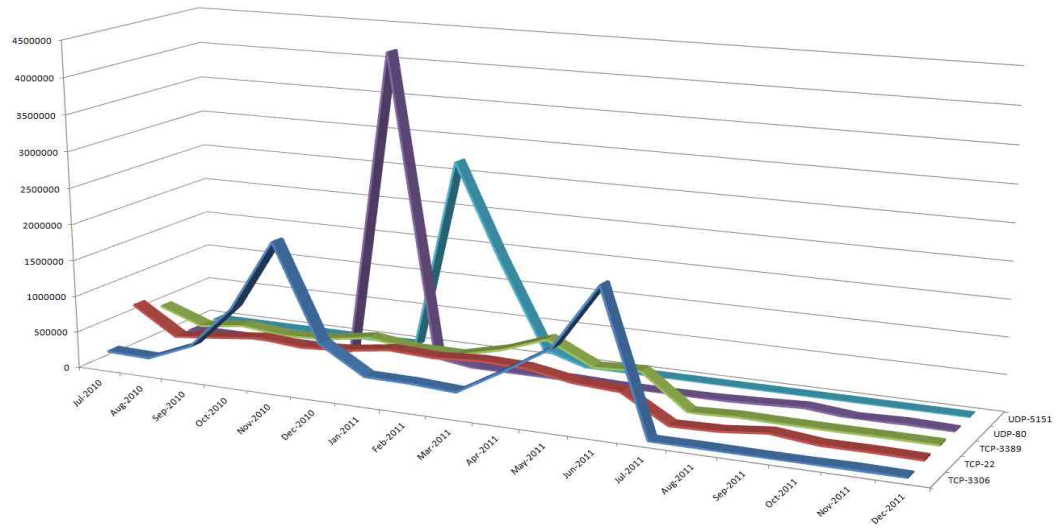

그림 9. Top-10 공격대상 포트 발생 추이
Fig. 9. Statistics of Top-10 Attack Port

기타 공격대상 포트 분석을 통해 발견된 특징들은 다음과 같다.

첫째, <표 3>에서 보인 5종의 포트들은 2011년 1월에 집중적으로 공격대상으로 활용되었다. 이는, 상호 연관된 보안취약점을 이용한 일련의 해킹(취약점 스캔 → 1차 해킹시도 → 관리자 권한 획득 시도 → 2차 자료유출 및 훼손)시도에 따라 발생된 것으로 추정된다.

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

순위	공격대상 포트
37	TCP-16776
61	TCP-6341
68	TCP-9769
75	TCP-7043
90	TCP-4536

둘째, <표 4>와 같이 특정 공격대상 포트들은 특정 기간에만 집중적으로 탐지되었다.

이는, 특정 기간에만 활동하도록 조작된 웜·바이러스의 특성과 특정 기간에 발표된 취약점의 집중적인 공격시도에 따른 것으로 보인다.

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

순위	공격대상 포트	집중탐지기간
14	UDP-123	2011-12
16	UDP-51304	2011-04
46	TCP-3984	2011-07
58	UDP-14392	2011-08
85	UDP-38209	2010-09
93	TCP-2499	2011-03

3.3 공격 국가 부문

지난 18개월 동안 과학기술사이버안전센터에서 탐지된 침해위협 이벤트의 공격 국가 정보를 분석한 결과 총 205개 국가에서 해킹공격 시도가 발생한 것으로 나타났으며, 공격 국가의 분포를 살펴보면 <그림 10>과

같이 “대한민국”, “중국”, “미국” 등의 순으로 발생하였으며, 상위 2개 국가가 전체 공격의 75.2%를 차지하고 있었다.

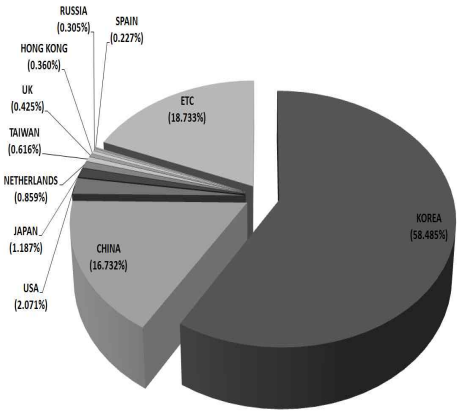

그림 10. 공격 국가 분포
Fig. 10. Distributions of Attack Nation

특히, 발생 빈도가 높은 상위 7개 국가의 월간 발생 추이를 살펴보면 <그림 11> ~ <그림 12>와 같다.

<그림 11>에서는 “대한민국”과 “중국” 간의 해킹 공격의 상호 연관성은 다소 미흡하며 특정 기간에 집중되는 경향을 확인할 수 있다. 이는 특정 공개형 해킹 툴 및 보안취약점을 이용한 해킹공격시도가 급증하기 때문인 것으로 분석되었다.

<그림 12>에서는 “미국”과 “네덜란드”가 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, <표 5>에서 보인 일부 국가들은 특정 기간에만 해킹시도가 급증하는 경향을 보였다. 이는 특정 취약점에 대한 집중공격 및 사전에 확보된 좀비군단에 의한 2차 해킹시도에 따른 것으로 분석되었다.

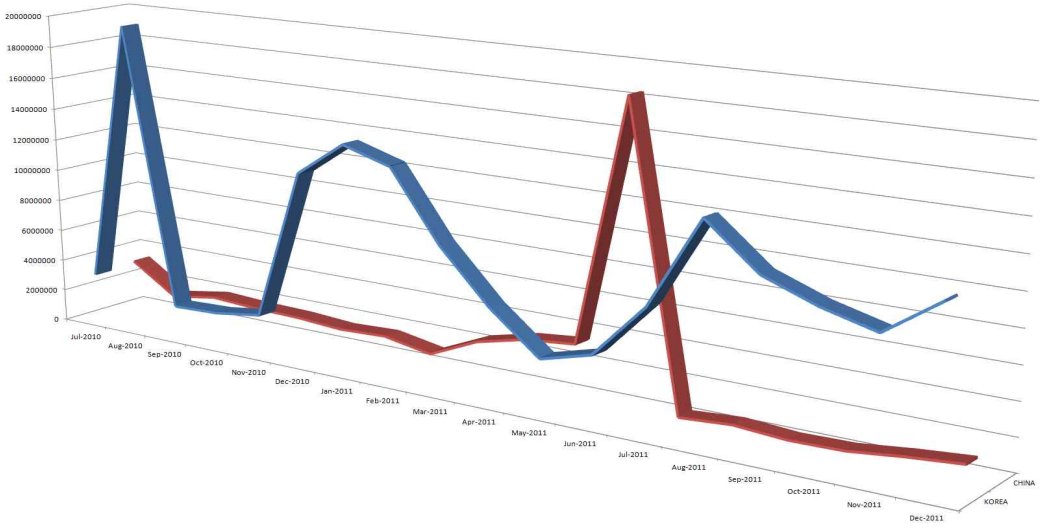

그림 11. Top-2 공격국가 발생 추이
Fig. 11. Statistics of Top-2 Attack Nation

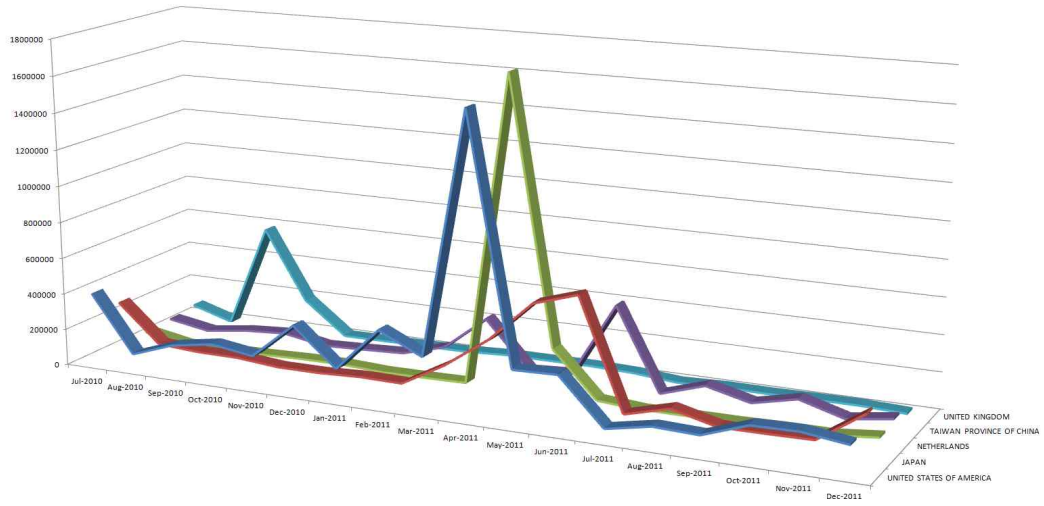

그림 12. Top-7 공격국가 발생 추이
Fig. 12. Statistics of Top-7 Attack Nation

표 5. 특이동향-5
Table 5. Interesting Trend-5

순위	공격 국가	집중탐지기간
10	SPAIN	2011-04
15	AUSTRIA	2011-05
17	NEW ZEALAND	2011-04
22	SINGAPORE	2011-02
24	ROMANIA	2011-11

둘째, <표 6>에서 보인 하위권의 일부 국가들은 특정 월에만 해킹시도가 발생하였고 다른 기간에는 전문한 것으로 확인되었다. 이는 해당 국가에서 직접적인 해킹공격을 시도한 것이 아니라 악성코드에 감염된 좀비PC에 의한 공격시도가 발생한 것으로 분석되었다.

표 6. 특이동향-6
Table 6. Interesting Trend-6

순위	공격 국가	탐지 월
129	TUVALU	2011-09
189	CHAD	2011-05
194	NIGER	2011-03
195	MICRONESIA FEDERATED STATES OF	2011-11
197	ERITREA	2011-11
198	ST. PIERRE AND MIQUELON	2011-09
200	REUNION	2011-03
201	PALAU	2011-07
202	COOK ISLANDS	2010-09
203	AMERICAN SAMOA	2011-01
204	GUINEA	2011-07
205	ANTARCTICA	2011-04

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

TOP-1인 "대한민국"에서는 <그림 13>과 같이 총 778종의 보안이벤트가 발생하였으며, 상위 3개 보안이벤트(udp flooding, udp port scan, icmp ping advanced IP scanner v1.4)가 전체의 70.4%를 차지하였다.

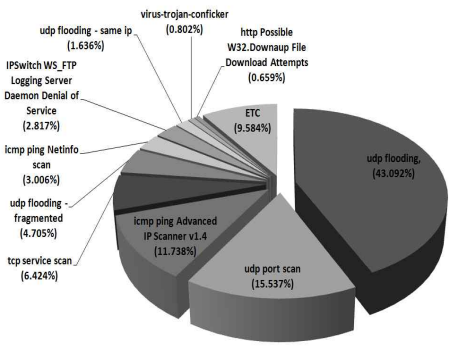

그림 13. 보안이벤트 분포(대한민국)
Fig. 13. Distributions of Security Event(Korea)

TOP-2인 "중국"에서는 <그림 14>와 같이 총 237종의 보안이벤트가 발생하였으며, 상위 2개 보안이벤트(udp flooding, udp port scan)가 전체의 94.4%를 차지하였다.

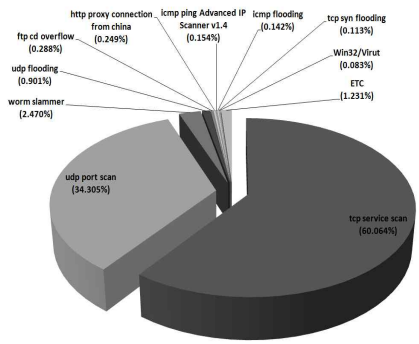

그림 14. 보안이벤트 분포(중국)
Fig. 14. Distributions of Security Event(China)

TOP-3인 "미국"에서는 <그림 15>와 같이 총 359종의 보안이벤트가 발생하였으며, 상위 2개 보안이벤트(udp port scan, tcp service scan)가 전체의 75.4%를 차지하였다.

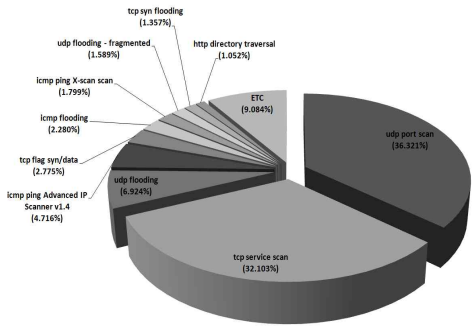

그림 15. 보안이벤트 분포(미국)
Fig. 15. Distributions of Security Event(USA)

Ⅳ. 결 론

본 논문에서는 과학기술사이버안전센터(S&T-SEC)를 통해 국내 주요 연구기관에서 발생된 실제 침해위협 이벤트 데이터를 수집한 결과를 기반으로 "보안이벤트", "공격대상 포트", "공격 국가" 등 총 3개 부문에 대한 글로벌 사이버위협 동향을 분석한 결과를 제시하였다. 특히, 본 논문을 통해 분석된 글로벌 사이버위협 동향은 다음과 같이 요약할 수 있다.

① "침해위협 이벤트" 부문 : 스캐닝 공격 및 서비스 거부공격(DoS)과 관련된 이벤트가 상위에 랭크되었으며 전체의 84.4%를 차지(TOP-5 기준)하고 있었다. 실질적인 해킹 공격 수행 이전에 공격 대상을 탐색하기 위해서는 반드시 선행되어야 하므로 앞으로도 지속적으로 발생할 것으로 예측된다. 또한, 특정 보안이벤트들은 집중적으로 발생하는 기간이 존재하였다. 이는 웜·바이러스와 봇 계열로써 감염된 시스템에 잠복해

있다가 특정 시점에 공격을 수행하는 고유한 특성 때문인 것으로 분석되어진다. 지난 2009년 발생된 7·7 DDoS 테러 시점 이후부터 지속적으로 증가하고 있는 추세이며 향후 점점 더 증가하고 탐지가 어렵도록 지능화·다양화 될 것으로 예측된다.

② "공격대상 포트" 부문 : 공격에 사용된 네트워크 프로토콜은 UDP → TCP → ICMP 순으로 발생하였으며 UDP-0이 전체의 23.7%를 차지하고 있었다. 이는 공격 대상 탐지를 위해 UDP-ANY(무작위) 형태로 포트 스캔을 수행하고 있기 때문이며 향후에도 스캐닝 공격과 함께 지속적으로 발생할 것으로 예측된다. 또한, 침해위협 이벤트 부문과 유사하게 특정 공격대상 포트들은 집중적으로 발생하는 기간이 존재하였다. 이는 보안 취약점 발표 시점에 맞물려 제로데이 공격 형태로 해당 취약점을 이용한 공격 시도가 급증하기 때문이며, 포트 번호는 달라지더라도 유사한 형태로 취약점 관련 포트에 대한 집중 공격시도가 발생할 것으로 예측된다.

③ "공격 국가" 부문 : 대한민국 → 중국 → 미국 등의 순으로 발생하였으며 대한민국이 전체의 58.5%를 차지하고 있었다. 이는 국내의 다수의 시스템들이 웜·바이러스 감염 등에 따른 좀비PC화로 인해 2차 공격을 국내 공격 대상에 시도하였기 때문이며 향후에도 국내 인터넷 사용수준 등을 감안하면 지속적으로 증가할 것으로 예상된다. 또한, 국가별로 발생한 침해위협 이벤트 유형이 매우 상이하였으며 상위에 랭크된 국가들에서는 점점 더 심화될 것으로 예측된다.

본 논문에서 제시한 글로벌 사이버위협 동향 분석 결과는 침해대응기술 연구자, 정보보호시스템 개발자 및 개별기관 정보보안 담당자들에게 현재의 위협상황을 인지하고 대응기술 및 보안정책 수립 등의 정보보안 활동 수행을 위한 기초자료로 활용할 수 있을 것이다.

참고문헌

[1] 시만텍, http://www.symantec.com/
[2] 안철수연구소, http://www.ahnlab.com/
[3] 인터넷침해대응센터, http://www.krcert.or.kr/
[4] 방송통신위원회, "2011년 국가정보보호백서," 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

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

김미경 (Mi-Kyoung Kim)

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