Regular paper http://dx.doi.org/10.13067/JKIECS.2013.8.12.1841

다크넷 트래픽을 활용한 보안관제 체계 구축에 관한 연구

박시장* · 김철원**

A Study on Constructing of Security Monitoring Schema based on Darknet Traffic

Si-Jang Park* · Chul-Won Kim**

요 약

본 논문에서는 매우 국한된 사이버공격에만 대응할 수 있는 기존 정형화 탐지패턴 기반의 보안관제를 극복하기 위하여 대규모 네트워크상에서 유출입 되는 이상행위 정보에 대한 종합적·체계적 수집·분석을 통해 실시간 보안관제 정확도 향상 및 관제영역 확대 방안에 대하여 연구하였다. 다크넷 네트워크상에 유입되는 다양한 침해위협 정보들을 수집·저장·분석하기 위한 이상 징후 관측 체계를 구축하고 통계 기반의 해킹동향 분석을 통해 알려진 사이버위협, 알려지지 않은 이상징후 및 고위험 이상행위 정보 분류 체계를 제시하였다. 본 연구에서 제시한 다크넷 트래픽을 활용한 보안관제 체계를 적용할 경우, 전체 침해위협 탐지가 기존 대비 12.6% 증가하였으며, 기존에는 감지할 수 없었던 신종·변종 공격을 120여종 감지하는 것으로 나타났다.

ABSTRACT

In this paper, the plans for improvement of real-time security monitoring accuracy and expansion of control region were investigated through comprehensive and systematic collection and analysis of the anomalous activities that inflow and outflow in the network on a large scale in order to overcome the existing security monitoring system based on stylized detection patterns which could correspond to only very limited cyber attacks. This study established an anomaly observation system to collect, store and analyze a diverse infringement threat information flowing into the darknet network, and presented the information classification system of cyber threats, unknown anomalies and high-risk anomalous activities through the statistics based trend analysis of hacking. If this security monitoring system utilizing darknet traffic as presented in the study is applied, it was indicated that detection of all infringement threats was increased by 12.6 percent compared with conventional case and 120 kinds of new type and varietal attacks that could not be detected in the past were detected.

키워드

Darknet, Honeynet, Honeypot, IDS, Anomaly Detection, Behavior Detection
다크넷, 허니넷, 허니팟, 침입탐지시스템, 이상탐지, 행위기반탐지

* 호남대학교 컴퓨터공학과(sijan.park@kt.com)
** 교신저자(corresponding author) : 호남대학교 컴퓨터공학과 교수(cwkim@honam.ac.kr)
접수일자 : 2013. 10. 15 심사(수정)일자 : 2013. 11. 25 게재확정일자 : 2012. 12. 16

Ⅰ. 서 론

인터넷의 급격한 발전은 국가 경제・사회 전반을 지탱하는 하나의 중요한 인프라로 자리매김 함과 동시에 국민생활에 대한 편리성과 효율성, 국부 창출에도 지대한 공헌을 하고 있다. 인터넷의 발전은 편리함으로 대변되는 긍정적 효과와 더불어 사이버범죄와 같은 부정적 효과를 동반한다[6]. 사이버 공간의 활용・의존도가 기하급수적으로 증가하는 현실 속에서 지능화・첨예화 되어가는 사이버 공격에 대한 효과적인 대응방안 마련은 언제나 중요한 이슈이다. 단순과시를 목적으로 시도되던 사이버 공격은 정치・금전적 목적을 가지고 시도되면서 다양해지고 교묘해 졌기 때문에 보안활동 역시 초기 기술적 보안 중심에서 전사적 보안 중심으로 무게중심이 이동하고 있으며, 수동적 대응방안보다 능동적 대응방안이 선호되고 있다. 대한민국의 경우, 국가정보원을 중심으로 국내 주요 국가기반시설 유형별 사이버 보안을 담당하는 부문 보안관제센터를 설치・운영하는 보안관제 중심의 사이버공격 대응체계를 갖추고 있으며, 이중 대부분은 패턴기반[7] 보안관제 방식을 채용하고 있다[1]. 상기 방식은 침입자로부터의 공격을 탐지/차단하기 위해 미리 정의된 침입규칙에 의거해 정형화된 단순 침입시도(알려진 공격 : 스캐닝, 웜・바이러스 등)로부터 내부 시스템과 네트워크등의 자원을 비교적 안전하게 보호할 수 있으나[8], 분석 작업이 선행되어야 하는 특징 때문에 첨예화・지능화 되어가는 해킹(알려지지 않은 공격: 신종・변종 사이버공격, 제로데이공격 등)에 신속한 대응이 어려운 문제를 안고 있어, 능동형 관제기술에 관한 관심과 연구가 증가하는 추세이다.[2,3,4] 본 논문에서는 매우 국한된 사이버공격에만 대응할 수 있는 기존 정형화 탐지패턴 기반의 보안관제를 극복하기 위하여 대규모 네트워크 상에서 유출입 되는 이상행위 정보에 대한 종합적・체계적 수집・분석을 통해 실시간 보안관제 정확도 향상 및 관제영역 확대 기반을 제시하고자 한다[7].

Ⅱ. 관련 연구

본 연구의 관련 연구로 다크넷을 통한 대규모 네트워크 이상징후 관측 체계를 구성하기 위한 시스템 구축 및 관제시스템 구성방안에 대해 기술한다.

1) 다크넷(darknet) 주소공간

다크넷(Darknet)이란 할당(사용)되지 않은 IP주소 공간으로 일반적으로 해당 IP대역에서 발생하는 네트워크 트래픽을 모니터링 하는 인터넷 시스템이라는 의미로도 쓰인다.[5] 이를 위해 유휴 IP 주소자원 중 C클래스 주소 8개를 확보하여 연구망 백본 라우터 상에 그림 1과 같이 설정한다.

```
HR-Router#sh run | inc ***.***.***.***
ip route ***.***.***.*** 255.255.255.0 XXX.XXX.XXX.XXX

※ ***.***.***.*** : unassigned C Class address resource
※ XXX.XXX.XXX.XXX : unused VLAN IP address
```

그림 1. 백본 라우터 상에 다크넷 주소공간 설정 방법
Fig. 1 A method of darknet address space setting on backbone router

2) 침해위협 탐지센서 시스템

이상탐지와 오용탐지의 비교・분석을 원활하게 수행하기 위하여 시그니처 기반의 침해위협 탐지센서(IDS)를 다크넷 주소공간에 설정한다[9,10].

3) 이상행위 수집서버 시스템

다크넷 주소공간으로 유입된 이상징후 발생 IP에 대하여 실제 네트워크 상에서 어떤 악성행위를 시도하고 있는지를 추적・분석하기 위하여 이상행위 수집서버를 추가적으로 다크넷 주소공간에 설정한다.

4) 이상행위 데이터 수집・관리 시스템

다크넷 주소공간에 대한 이상행위 정보를 침해위협 탐지센서 및 이상행위 수집서버로부터 실시간으로 수집・관리하기 위해 이상행위 데이터 수집・관리 시스템을 구축한다.

5) 사이버위협 동향 수집・분석 시스템

이상행위 데이터 수집・관리 시스템으로부터 수집된 다양한 정보들에 대한 통계 분석을 수행하기 위하여 별도의 동향 수집・분석 시스템을 구축한다.

6) 차세대 보안관제 시스템

대규모 네트워크 상에서 발생되는 다양한 이상행위 정보들을 체계적・효율적으로 분석하여 침해대응 활

동에 접목시키기 위한 실시간 모니터링 및 분석용 보안관제 시스템을 구축한다.

III. 다크넷 트래픽을 활용한 보안관제 체계 구성

3.1 시스템 구성도 및 흐름도

구축된 관측체계를 활용해 다크넷 네트워크 상에 유입되는 이상징후를 관측하는 구성 및 동작과정은 그림 2와 같다.

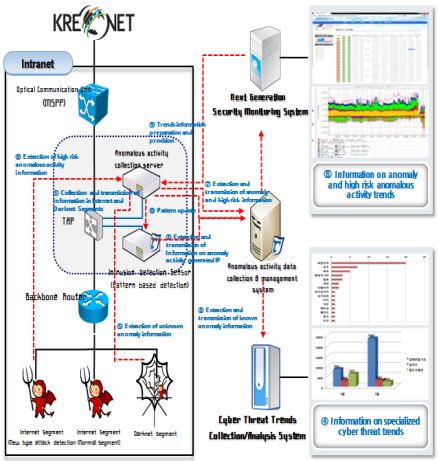


그림 2. 다크넷 네트워크 이상징후 관측 절차
Fig. 2 Observation procedure for anomaly detection on darknet network

(1) 다크넷 주소공간으로 유입되는 트래픽을 TAP을 통해 '이상행위 수집서버'와 '침해위협 탐지센서'로 전송

(2) 수집된 트래픽 중 '침해위협 탐지센서'에서 감지 가능 및 불가능 패킷을 구분하여 '이상행위 데이터 수집·관리 시스템'에 전송

(3) '이상행위 데이터 수집·관리 시스템'에 수집된 트래픽 중 침해위협 탐지센서에서 감지 가능한 이상행위 발생 IP목록을 추출하여 '사이버위협 동향 수집/분석 시스템'으로 전송 및 DB화

(4) 수집된 DB를 기반으로 알려진 사이버위협 정보 실시간 제공

(5) '침해위협 탐지센서'에서 감지 불가한 정보를 알려지지 않은 이상징후 정보로 규정하고 '이상행위 수집 서버'를 통해 해당 공격자로부터 오는 모든 트래픽을 수집

(6) '이상행위 수집서버'에서 수집된 공격자 트래픽 중 목적지 IP주소가 정상 시스템일 경우 이를 고위험 이상행위 정보로 규정

(7) 관련 정보를 '이상행위 데이터 수집·관리 시스템'으로 전송

(8) '이상행위 데이터 수집·관리 시스템'에 수집된 정보 중 알려지지 않은 이상징후 및 고위험 이상행위 정보 목록을 '차세대 보안관제 시스템'으로 전송 및 DB화

(9) 수집·분석된 정보를 기반으로 신규 패턴을 제작하여 차세대 보안관제 시스템을 통해 과학기술 분야에 알려지지 않은 이상징후 및 고위험 이상행위 정보 실시간 제공

(10) 생성된 신규패턴을 '침해위협 탐지센터'에 전송하여 업데이트 수행

그림 3은 구축된 다크넷 네트워크 상에 발생하는 알려진 사이버위협, 알려지지 않은 이상징후, 고위험 이상행위를 검출하기 위한 개념도를 의미한다.

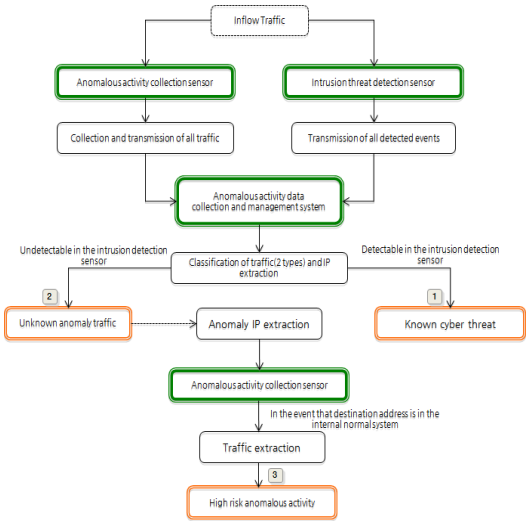


그림 3. 다크넷 네트워크상의 이상징후 관측 개념도
Fig. 3 Conceptual diagram for observing anomaly on darknet network

3.2 알려진 사이버위협 분석

알려진 사이버위협은 트래픽의 목적지 주소가 다크넷 공간인 트래픽 중에서 침해위협 탐지센서에서 탐지 가능한 이벤트들을 의미하며, 침해위협탐지센서에서 탐지된 침해위협 정보를 '사이버위협 동향 수집/분석 시스템'에서 수집 및 분석하여 대규모 네트워크 상에 유출입되는 알려진 사이버위협 분석을 수행한 상세한 내역은 다음과 같다.

① 입력 : 지역센터에서 수집된 침해위협 탐지 정보

② 결과 : 4개 부문 (이벤트, 공격자IP, 공격포트, 공격국가)

- 2개월 간 수집된 데이터를 기준으로 통계 분석

실제 구축된 화면은 그림 4, 그림 5와 같다.

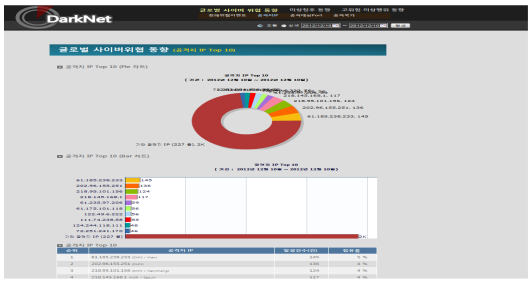


그림 4. 공격자 IP 분석 화면
Fig. 4 Analytical screen of attacker IP

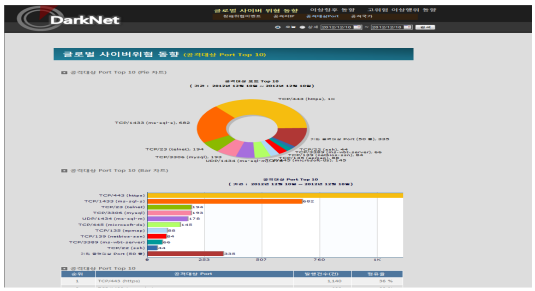


그림 5. 공격대상 포트 분석 화면
Fig. 5 Analytical screen of attack target port

3.3 알려지지 않은 이상징후 분석

알려지지 않은 이상징후 정보는 그림 6과 같이 다크넷 구간으로부터 '침해위협 탐지센서'에서 수집된 알려진 공격 정보를 제외한 나머지를 가리키는 것이며, 알려지지 않은 이상징후에는 고위험 이상행위 정보를 모두 포함한다. 정보 수집을 위해 알려지지 않은 이상징후 정보와 알려진 공격 정보 패킷에서 추출한 IP목록의 여집합을 '이상행위 발생 IP'로 정의하고 알려지지 않은 이상징후 정보 중 해당 IP와 연관된 정보로 지칭한다. 다크넷 네트워크 이상징후 관측체계를 활용해 알려지지 않은 이상징후 정보를 수집하는 골격은 그림 7과 같다.

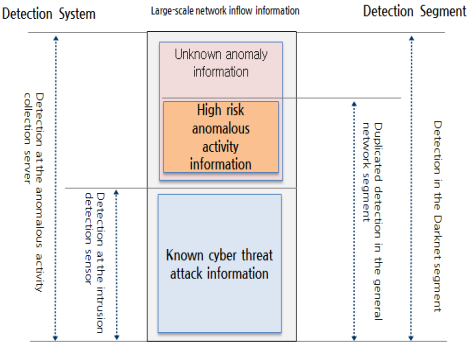


그림 6. 다크넷 구간에서 수집한 알려지지 않은 이상징후 정보의 유형
Fig. 6 Types of unknown information with anomaly collected in the darknet segment

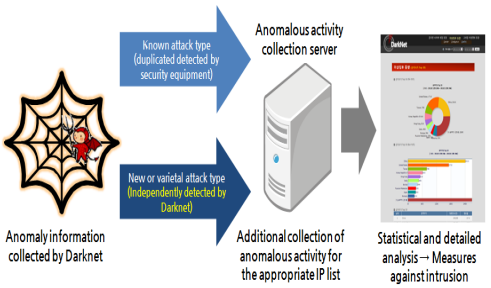


그림 7. 알려지지 않은 이상징후 수집 방법론의 골격
Fig. 7 Methodology frame for collecting unknown anomaly collection

알려지지 않은 이상징후 정보를 수집하기 위해 '이상징후 수집서버'를 구축하여 이상행위 발생 IP주소 목록을 차세대 보안관제 시스템으로부터 실시간으로 수신받아 이를 기반으로 알려지지 않은 공격에 대한 패킷 필터링을 수행한다.

이를 기반으로 차세대 보안관제 시스템에서 수집 및 분석된 대규모 네트워크 상에 유출입되는 알려지지 않은 이상징후 분석을 수행한 상세 내역은 다음과 같다.

① 입력 : 지역센터에서 수집된 다크넷 트래픽 정보

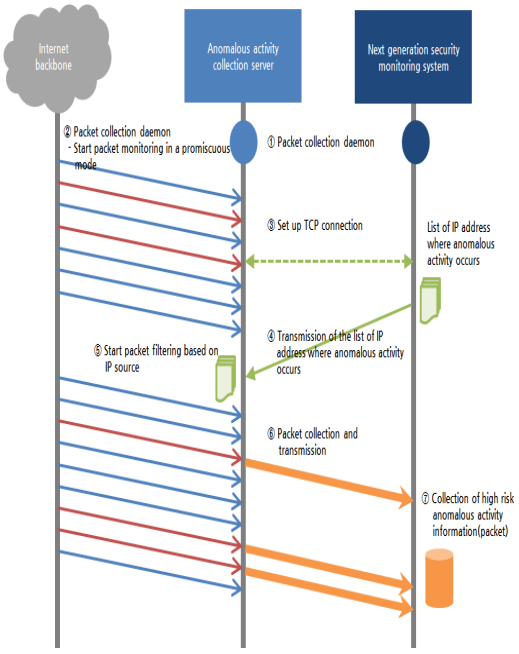
② 결과 : 3개 부문 (공격자IP, 공격포트, 공격국가) - 2개월 간 수집된 데이터를 기준으로 통계 분석

알려지지 않은 이상징후는 알려진 사이버 위협 분석에서 탐지된 총 477,687건 대비 약 3배 정도 많은 132,604,323건이 탐지된 것으로 확인되었다.

특히 알려지지 않은 이상징후에서 탐지된 IP들은 알려진 사이버위협 탐지된 IP와 달리 실제 공격에 활용되었을 확률이 매우 높아 위험 IP로 바로 활용이 가능할 것으로 예상되며, 탐지 포트의 경우 알려진 사이버위협에서는 공격 포트가 대부분 웹 서비스인 것과 달리 telnet이나 icmp등 다양한 포트 공격이 탐지되었다.

3.4 고위험 이상행위 분석

고위험 이상행위 정보는 '이상행위 수집서버'에서 '이상행위 발생 IP'를 활용해 일반 네트워크 구간에서 수집된 정보를 일컫는다. 고위험 이상행위 정보라 명명한 이유는 이 정보들이 기존 보안관제 체계에서 탐지되지 않지만 일반 네트워크에서 행해지고 있는 공격일 위험이 매우 높기 때문이다. 그림 8은 고위험 이상행위 정보 수집 프로세스를 나타내며, '이상행위 수집서버'의 패킷 필터링 및 DB 수집 구동화면은 그림 9, 그림 10과 같다.



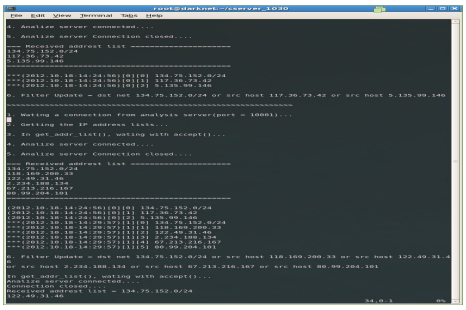


그림 9. 이상행위 수집서버의 패킷필터링 화면
Fig. 9 Packet filtering screen of anomalous activity collection server

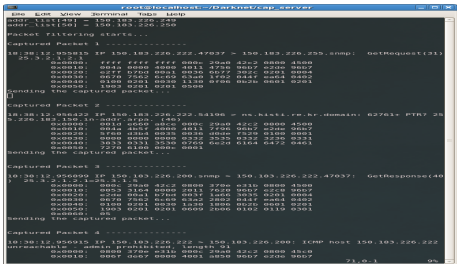


그림 10. 이상행위 수집서버의 DB 수집・저장 화면
Fig. 10 DB collection saving screen of anomalous activity collection server

이상행위 수집서버의 동작 프로세스는 그림 11과 같다.

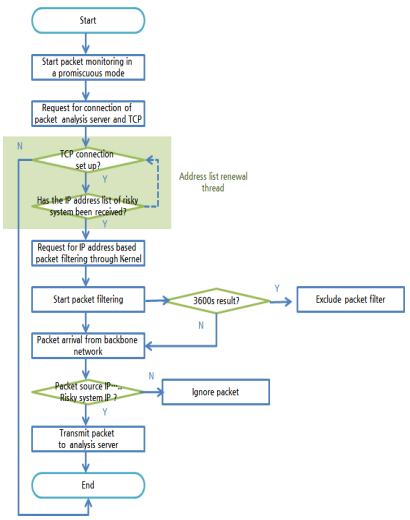


그림 11. 이상행위 수집서버의 동작 프로세스
Fig. 11 Operation process of anomalous activity collection server

'이상행위 수집서버'를 통해 수집된 고위험 이상행위 정보를 실시간으로 모니터링하고 상세분석하기 위해 개발한 '차세대 보안관제 시스템' 운용 화면은 그림 12, 그림 13과 같다.

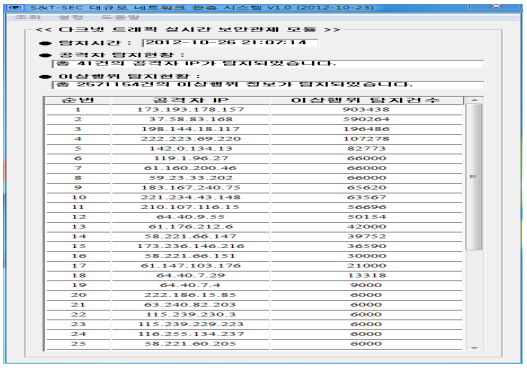


그림 12. 고위험 이상행위 보안관제 시스템 메인 화면
Fig. 12 Main screen for security and monitoring of high risk anomalous activities

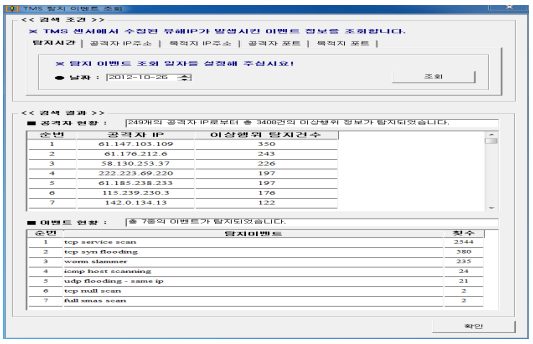


그림 13. 고위험 보안관제 시스템의 보안이벤트 분석 화면
Fig. 13 Analytical screen of security events in high risk security and monitoring system

이상행위 수집서버에서 탐지된 공격자 IP(다크넷 트래픽 유발)의 실제 이상행위 추적·탐지 정보를 수집하여 고위험 이상행위 분석을 수행한 상세 내역은 다음과 같다.

① 입력 : 지역센터에서 수집된 고위험 이상행위 정보
② 결과 : 3개 부문 (공격자IP, 공격포트, 공격국가)
- 2개월 간 수집된 데이터를 기준으로 통계 분석

고위험 이상행위는 총 105,990,386건이 탐지된 것으로 확인되었으며, 탐지된 포트는 알려지지 않은 이상징후와 같이 다양한 포트 공격이 탐지되었다. 공격자IP와 공격국가의 경우 알려지지 않은 이상징후에서 가장 많이 탐지된 국가인 중국과 달리 미국에서 가장 많은 발생하는 것으로 탐지되었다.

Ⅳ. 연구결과 분석

본 연구를 통해 대규모 네트워크 이상징후 분석과 전용 웹페이지를 활용하여 최근 2개월간(2012년 10월 1일~2012년 11월 30일) 과학기술 분야에 발생된 다크넷 구간 이상징후를 수집·분석한 통계는 표 1과 같다.

표 1. 다크넷 구간 이상징후 통계 목록(최근 2개월)
Table 1. Statistical summary of anomalies in the darknet segment(during recent 2 months)

Division	No. of detection	Attack IP	No. of attacked countries
Known cyber threat	477,687	14,068	126
Unknown anomalies	132,604,324	21,055	140
Anomalous activities with high risk	105,990,386	2,103	69

먼저, 알려진 사이버위협 총 477,687건 중 DDoS공격 등에 활용되는 "tcp syn flooding" 공격 이벤트가 전체의 50.67%(242,024건)으로 가장 많이 탐지되었으며, 알려지지 않은 이상징후는 "TCP/445 (microsoft-ds)" 공격 이벤트가 전체의 16.31%(21,624,421)건으로 가장 많이 탐지되었다. 고위험 이상행위는 "TCP/1433(ms-sql-s)" 공격 이벤트가 전체의 15.50%(16,425,197)건으로 가장 많이 탐지 되었다.

제안된 시스템을 통해 그림 14과 같이 기존의 정형화된 탐지패턴 기반 보안관제체계 대비 12.5%의 추가적인 신규 영역 탐지가 이루어졌으며, 표 2와 같이 기존 보안관제에서 감지하지 못했던 다양한 신종·변종 및 대규모 사이버공격에 대한 조기 탐지를 확인 할 수 있었다.

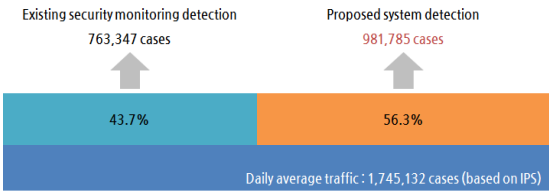


그림 14. 제안 연구를 통한 신규 탐지영역 발생
Fig 16. Occurrence of new detection coverage through research

표 2. 제안 연구를 통한 신종·변종 공격 조기 탐지
Table 2. Early detection of new type and varietal attacks through research

No.	Types of new type and varietal attacks	Existing security and monitoring	Darknet security and monitoring
1	Denial of service attack (DoS detection)	-	48
2	Detection of malware infection signal transmission	-	14
3	Detection of DBMS vulnerability attack trials	-	7
4	Detection of vulnerability scanning trials	-	34
5	Detection of web vulnerability attack trials	-	12
6	Detection of DoS attack trials based on IP forgery	-	5
	Total 6 types	-	120

V. 결 론

본 논문에서는 다크넷에 유입되는 대규모 네트워크 이상징후 관측 체계를 근간으로 알려진 사이버위협과 알려지지 않은 이상징후 및 고위험 이상행위 분석 방법론을 활용한 신·변종 및 대규모 해킹공격 조기 탐지기술 방법을 제안하였다.

제안된 시스템을 통해 기존 보안관제와 개선된 다크넷 보안관제와의 효율적인 연계로 오탐을 줄이고, 정탐을 늘려 분석대상을 줄임과 동시에 고위험 이상행위 정보 잠재적인 해커의 행위를 추적하여 실제 해킹공격 및 피해 발생 이전에 능동적으로 보안관제 및 침해예방을 수행하기 위한 좋은 데이터로 활용 가능할 것으로 판단된다. 그러나 첨예해져가는 사이버 공격에 효과적으로 대응하기 위해서는 탐지·수집·분석 프로세스 상의 신속성, 정확성 향상과 침해위협정보의 실시간 가시화를 통한 대규모 사이버공격 탐지능력을 향상 시키고, 제안된 보안관제체계 활용을 통해 국가 보안관제체계 수립의 실효성을 검증하는 것이 추후의 연구과제이다.

참고 문헌

[1] Seok-Soo Kim, “A Research on Intrusion Prevention System and Security Monitoring System”, Security Engineering Research Paper Journal, Vol 1, No. 1, pp. 2-5, 2005.

[2] Jeong-Nyo Kim, Jong-soo Jang, Sung-Won Son, “Integrated Security Technology for Intrusion Prevention for I&C System Infrastructure”, Information and Communications Magazine in Korea, Vol 21, No. 9, pp. 75-90, 2004.

[3] Woo-Seok Seo, Jae-Pyo Seo, Mun-Seok Jeon, “A Research on Platform Design Methodology Standardized for Network Security Infrastructure Constitution”, The Journal of the Korea Institute of Electronic Communication Sciences, Vol 7, No. 1, pp. 204-206, 2012.

[4] Jung-Suk Jang, Yong-Hee Jeon, Jong-soo Jang, Sung-Won Son, “A Distributed Communication Model and Performance Evaluation for Information Transfer in a Security Policy-based Intrusion Detection System”, Korea Communication Academic Association Journal, Vol 29, No. 12, pp. 1707-1712, 2004.

[5] Tao Ban, Lei Zhu, Jumpei Shimamura, Shaoning Pang, Daisuke Inoue, Koji Nakao, “Behavior Analysis of Long-term Cyber Attacks in the Darknet”, ICONIP (5) pp. 620-628, 2012.

[6] Cjha-in Hwan, “A study on the Development of Personal Security Management for Protection against Insider threat”, The Journal of the Korea Institute of Electronic Communication Sciences, Vol 3, No. 4, pp. 210-211, 2008.

[7] Taek-Yong Nam, Suk-Yeon Kim, Sung-Min Lee, Jeong-Hun Ji, Sung-Won Son, “Reliable Next Generation Network Security System”, Korea Information Protection Academic Association Journal, Vol 6, No. 5, pp. 1-12, 2003.

[8] Woo-Seok Seo, Moon-Seog Jun, "A Study on the Realization of Diskless and Stateless Security Policy Based High-speed Synchronous Network Infrastructure", The Journal of the Korea Institute of Electronic Communication Sciences, Vol 6, No. 5, pp. 676-679, 2011.
[9] Soo-Hyeong Jo, Jeong-Nyo Kim, "Policy-based Security Management for Intrusion Detection", Korea Information Science Academic Association Journal, Vol 29, No. 2, pp. 574-576, 2002.
[10] J. Song, H. Takakura, and Y. Kwon, "A Generalized Feature Extraction Scheme to Detect 0-Day Attacks via IDS Alerts", The 2008 International Symposium on Applications and the Internet(SAINT2008)", The IEEE CS Press, pp. 51-56, 28 July-1 Aug. 2008.

저자 소개

박시장(Si-Jang Park)

2007년 호남대학교 인터넷소프트웨어학과 졸업(공학사)
2009년 호남대학교 소프트웨어공학과 졸업(공학석사)
2013년 호남대학교 컴퓨터공학과 졸업(박사수료)
1994년 한국전기통신공사 입사
2008년~현재 KT전남고객본부 SMB컨설팅 팀장
※ 관심분야 : U-City 설계, VoIP, 정보보안

김철원(Chul-Won Kim)

1997년 광운대학교(공학박사)
1998년~현재 호남대학교 컴퓨터공학과 교수
※ 관심분야 : XML 응용, 멀티미디어 정보검색