Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.30, NO.3, Jun. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.3.465

IP 주소 기반 사이버공격 실시간 및 통계적 가시화 방법*

문 형 우,[1,4†] 권 태 웅,[1] 이 준,[2] 류 재 철,[5] 송 중 석[3,6‡]
[1,2,3]한국과학기술정보연구원 (연구원, 선임연구원, 책임연구원), [4,5]충남대학교 (대학원생, 교수),
[6]과학기술연합대학원대학교(교수)

A Real-Time and Statistical Visualization Methodology of Cyber Threats Based on IP Addresses*

Hyeongwoo Moon,[1,4†] Taewoong Kwon,[1] Jun Lee,[2]
Jaecheol Ryou,[5] Jungsuk Song[3,6‡]
[1,2,3]Korea Institute of Science and Technology Information(KISTI)
(Researcher, Senior Researcher, Chief Researcher),
[4,5]Chungnam National University (Graduate Student, Professor)
[6]University of Science and Technology (Professor)

요 약

국내·외 기업 및 기관들은 사이버위협으로부터 자신들의 IT 인프라를 안전하게 보호하기 위해 24시간/365일 모니터링 및 대응할 수 있는 보안관제센터를 활용하고 있다. 하지만, 현재 대부분의 보안관제센터는 전문 인력에 의한 수동분석과 텍스트 기반의 보안관제체계에 의존하는 태생적인 한계점을 안고 있다. 이러한 보안관제체계의 문제점들을 극복하기 위해 가시화 기술을 활용한 사이버위협 탐지·분석 연구가 활발하게 진행되고 있지만 이들 연구의 대부분은 보안관제 분야에 최적화되어 있지 않고, 많은 경우에 개별 기관에서만 활용할 수 있다는 제한이 따랐다. 따라서 본 논문에서는 보안관제 분야의 최종 목표인 실제 공격자 IP를 탐지할 수 있을 뿐만 아니라, 보안관제센터에서도 활용할 수 있는 새로운 가시화 방법론을 제안한다. 본 논문에서 제안하는 가시화 방법론의 핵심은 보안이벤트를 발생시킨 공격자(IP)의 행위정보를 실시간 및 추적(통계) 분석을 가능하게 하는 것이다. 제안된 가시화 방법론을 기반으로 개발된 시스템을 실제 보안관제센터에 성공적으로 적용하였으며, 실제 운영을 통해 다양한 공격자 IP를 탐지 및 분석하는데 성공함으로써 본 논문에서 제안한 가시화 방법론의 실용성 및 유효성을 검증했다.

ABSTRACT

Regardless of the domestic and foreign governments/companies, SOC (Security Operation Center) has operated 24 hours a day for the entire year to ensure the security for their IT infrastructures. However, almost all SOCs have a critical limitation by nature, caused from heavily depending on the manual analysis of human agents with the text-based monitoring architecture. Even though, in order to overcome the drawback, technologies for a comprehensive visualization against complex cyber threats have been studying, most of them are inappropriate for the security monitoring in large-scale networks. In this paper, to solve the problem, we propose a novel visual approach for intuitive threats monitoring by

Received(04. 08. 2020), Modified(05. 25. 2020), Accepted(05. 25. 2020)
* 본 연구는 한국과학정보기술연구원(KISTI) 지원으로 수행하였습니다.
† 주저자, hwmoon@kisti.re.kr
‡ 교신저자, song@kisti.re.kr(Corresponding author)

detecting suspicious IP address, which is an ultimate challenge in cyber security monitoring. The approach particularly makes it possible to detect, trace and analysis of suspicious IPs statistically in real-time manner. As a result, the system implemented by the proposed method is suitably applied and utilized to the real-would environment. Moreover, the usability of the approach is verified by successful detecting and analyzing various attack IPs.

Keywords: Cybersecurity, Visualization, Real-time Monitoring, Statistical Analysis, SOC

I. 서 론

랜섬웨어, 지능형 지속 위협(APT), 분산서비스 거부(DDoS), 멀웨어(malware)등의 사이버위협은 해마다 지능화·고도화되고 있으며, 이로 인한 실제 피해대상 및 규모 또한 광범위하게 확대되고 있다. 국내·외 기업 및 기관들은 사이버위협으로부터 자신들의 IT 인프라를 안전하게 보호하기 위해 24시간/365일 모니터링 및 대응할 수 있는 보안관제센터를 자체적으로 운영 하거나 전문기업을 통한 아웃소싱(outsourcing)을 이용하고 있다. 그 결과 국내 보안관제 서비스의 규모는 매년 약 10% 이상 급격히 성장 중이며[1][2], 뿐 만 아니라 캐나다, 독일, 영국, 미국 등의 해외 주요국가에서도 기업의 84%, 대기업 중 약 91%가 보안관제센터를 구축 및 운영하고 있다[3].

이와 같이 보안관제센터의 중요성은 해마다 강조되고 있지만, 현재 대부분의 보안관제센터는 전문 인력에 의한 수동분석과 텍스트 기반의 보안관제체계에 의존하는 태생적인 한계로 인해 폭발적으로 증가하는 사이버위협에 대한 신속·정확한 탐지 및 대응에 많은 어려움을 겪고 있다.

특히 네트워크의 규모와 속도가 급격하게 발전함에 따라 이를 효율적으로 모니터링 할 수 있는 방법과 도구들이 요구되었지만 여전히 전통적인 텍스트기반의 보안관제체계가 유지되고 있으며, 이로 인해 급증하는 보안이벤트에 효과적으로 대응하지 못 하고 있다. 보안관제요원들 또한 가시성 부족 및 과중한 업무 등을 보안관제의 효율성 저해의 요인으로 지적하였다[4][5].

이러한 보안관제체계의 문제점들을 극복하기 위해 다양한 연구들이 활발히 진행되어 왔으며, 그 중에서 가장 주목할 분야가 대규모 보안이벤트에 대한 가시화를 통한 사이버위협 탐지·분석 연구이다. 기존의 가시화 연구가 대규모 보안정보를 직관적으로 분석할 수 있는 장점을 제공하였지만, 이들 대부분은 보안관제 분야에 최적화되어 있지 않고, 많은 경우에 개별 기관에서만 활용할 수 있다는 제한이 따랐다.

따라서 본 논문에서는 보안관제 분야의 최종 목표인 대규모 사이버위협정보를 분석하여 실제 공격자 IP를 탐지할 수 있을 뿐만 아니라, 중앙 집중 방식으로 분석업무를 수행하는 보안관제센터에서도 활용할 수 있는 새로운 가시화 방법론을 제안한다.

본 논문에서 제안하는 가시화 방법론의 핵심은 보안이벤트를 발생시킨 공격자(IP)의 행위정보를 실시간은 물론 추적(통계) 분석을 가능하게 하는 것이다. 이를 위해, 모든 공격자 IP에 대해 1분마다 10개 종류의 행위정보를 추출하고 이를 최대 24시간 동안 누적해서 모니터링 할 수 있도록 가시화한다.

본 논문에서 제안하는 가시화 방법론을 활용하여 공격자의 공격행위에 대한 순간적인 변화, 규칙/불규칙적인 패턴 변화, 공격행위의 빈도(빠름/느림 등) 변화, 공격행위의 양(감소/증가/일정 등)의 변화, 이들 공격 패턴의 조합 등 사이버공간에서 발생할 수 있는 다양한 공격 시나리오에 대해 탐지 및 대응할 수 있다.

제안된 가시화 방법론을 기반으로 개발된 시스템을 국내 공공분야 부문보안관제센터 중 하나인 과학기술사이버안전센터(S&T-CSC: Science & Technology Cyber Security Center)의 실환경에 성공적으로 적용하였으며, 실제 운영을 통해 다양한 공격자 IP를 탐지 및 분석하는데 성공함으로써 본 논문에서 제안한 가시화 방법론의 실용성 및 유효성을 검증했다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 보안관제 체계의 한계, 보안이벤트 가시화방법 및 한계점에 대해 설명한다. 3장과 4장에서는 제안하는 방법론과 구현방법에 대해 각각 서술한다. 5장에서는 제안하는 방법론을 활용한 실탐지 사례를 보임으로써 제안하는 방법론의 효용성을 증명하며, 6장에서는 결론 및 향후 연구 방향에 대해 서술한다.

II. 관련연구

본 장에서는 고도화 되고 있는 사이버공격에 대응하기 위한 보안관제 현황과 최근 발생하는 한계점들

을 함께 살펴보고, 보안관리자의 탐지, 분석 및 대응 업무의 효율성 제고를 위해 연구된 다양한 보안이벤트 가시화 기법을 소개한다. 또한 가시화를 통한 탐지 사례를 통해 그 유효성을 확인한다.

2.1 보안관제 현황 및 한계점

대부분의 국가, 공공기관은 물론 기업에서도 운영중인 보안관제센터는 대규모/고도화 되고 있는 보안위협에 대응하기 위한 필수 조직으로 고려되고 있다. 국내의 경우, 국가사이버안전센터(NCSC, National Cyber Security Center)를 중심으로 모든 국가·공공기관에서 각급 보안관제센터를 중심으로 보안관제를 수행하고 있으며, 상업조직 및 대기업도 보안관제 전문기업(MSSP, Managed Security Service Providers)의 전문 서비스를 통해 사이버 위협에 대응하고 있다.

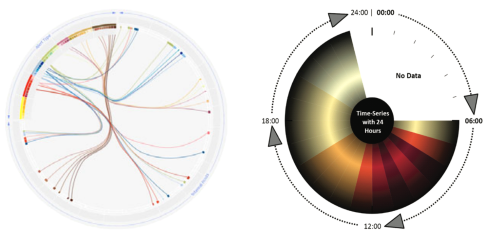
하지만 통신기술의 발달로 인하여 급격하게 증가하는 트래픽과 보안이벤트는 실제 보안관제 업무에 있어서 많은 어려움을 초래하고 있다. 임퍼바(imperva)가 2018년 RSA컨퍼런스에서 수행한 설문[6]에 의하면, 보안관리자의 27%가 매일 100만 건 이상의 보안이벤트를 처리하고 있다고 답변하였으며, SOAR 보고서(the state of SOAR report, 2018)[7]에 따르면 대부분의 보안관리자는 매주 약 15만 건 이상의 공격 경보를 받고 매일 평균12,000건을 처리하고 있다고 밝혔다. 특히, 급격하게 증가하는 보안이벤트로 인하여 보안위협 대응의 핵심평가지표인 평균대응시간(MTTR, Mean Time to Respond)은 4.35일에 달하는 것으로 나타났다[8]. 즉, 보안관제센터를 운영함에도 불구하고, 적시에 적절한 대응이 어려워 치명적인 보안위협에 노출되는 문제점이 발생하고 있는 실정이다. 따라서 이와 같은 문제점을 해결하고 보안관리자의 직관적인 위협탐지 및 대응을 돕기 위해, 대용량 보안이벤트의 효율적인 가시화 기법에 대한 연구가 활발히 진행되고 있다.

2.2 보안이벤트 가시화 기법

네트워크 트래픽에 대한 가시성 부족은 보안관제 업무에 비효율성을 초래하는 가장 큰 요소로 지적되고 있다[4][5]. 이와 같이 대량으로 발생하는 보안이벤트의 효율적인 관제 및 대응을 위해 다양한 방식의 가시화 방법들이 제안 되어져왔다[9][10][11]. 특히 모든 송수신 네트워크 트래픽을 감시하는 네트워크 침입 탐지 시스템(NIDS, Network Intrusion Detection System) 으로부터 발생하는 대량의 보안이벤트(즉, 로그 및 경보)는 보안관제를 돕기 위한 주요 가시화 대상이다[12][13][14].

대표적인 NIDS인 SNORT[15]의 로그를 이용하여 각 보안이벤트들을 매트릭스 형태로 표현한 SnortView[16]는 2차원 공간에 IP주소와 프로토콜 정보를 바탕으로 보안 경보 종류 및 우선순위에 따라 아이콘과 색상에 효과를 줌으로써 보안상황을 보다 효과적으로 식별하는 것에 초점을 맞췄다. 다만 단기간(약4시간) 동안의 공격만을 누적하여 가시화함으로써 긴 주기를 갖는 사이버공격을 식별하는데 어려움이 있고, 가시화 가능한 IP 주소 개수의 한계 때문에 대규모 네트워크를 관찰하기에 부적합한 면이 존재한다. 반면, Rainstorm[17]은 B클래스 IP주소 블록전체를 24시간 동안 누적하여 2차원 단일 화면에 가시화함으로써 네트워크 전체의 경보발생 상황을 한눈에 볼 수 있게 하였다. 또한 연속적인 IP주소 세트를 단일 행의 픽셀에 할당함으로써 보안관리자의 가시성을 향상시켰다. 하지만, 대용량 트래픽이 발생하는 경우 너무 많은 경보가 단일 화면에 발생하며, 비록 확대 시각화 기능을 제공하지만 중요한 경고를 적시에 식별하기가 어렵다.

이와 같은 초기 시각화 기법들은 주로 픽셀 단위의 IP주소 표현을 통해 많은 양의 IP 주소를 단일 화면에 가시화를 시도하였으나, 경고 발생 시 픽셀에 해당하는 각 주소를 확인하기 위한 사용자 인터랙션의 비효율성과 더불어 경고가 발생하지 않는 IP주소를 전부 가시화함으로써 공간의 활용도가 비효율적이다. 이와 같은 문제점을 해결하고자 Avisa[18]는 방사형(radical) 구조를 갖는 시각화를 통해 공간



(a) Initial design of Avisa[18] (b)Circular clock glyph[19]

Fig. 1. Examples of Visualization for Security Events

활용의 극대화를 추구하였다. 특히 경보의 단계와 유형을 각각 색상과 명암의 차이로 표현하여 경보 발생 상황을 쉽게 식별하도록 하였다(Fig.1.(a)). BANKSAFE[19]는 시간기준 보안이벤트 시각화를 위한 원형차트(Fig.1.(b))와 IP 주소기준 세부 경보 상황 파악을 위한 트리맵(treemap) 시각화를 함께 제공함으로써 보안관리자의 가시성 향상 및 보안이벤트의 주기성 분석 향상을 도모하였다.

2.3 가시화 기법 활용 탐지 사례

직관적인 보안관제 및 대응을 위해 다양한 가시화 기법이 연구·개발 되어왔지만, 실제 보안관제 환경에서 활용하기 위해서는 다양한 요소들이 고려되어야 한다. 특히 대용량의 보안이벤트를 실시간으로 처리하여, 위협도가 높은 주요 이벤트를 추출하고 이를 직관적으로 가시화 하는 것이 중요하다. Itoh 등[20]은 공격의심 송수신 IP들을 계층적으로 구성하여 각각 중첩되지 않도록 가시화를 시도하였으며, 위협정도를 함께 고려하여 시각화함으로써 보안관리자의 직관적인 정보습득을 추구하였다. 또한 2.5차원 평면상에 계층화된 IP들을 표현함으로써 동시에 수천 개 이상의 대상을 표현하여 종합적인 가시화를 구현하였고, 특히 침해 발생 빈도수에 따라 색상 및 그래프 크기를 다르게 시각화함으로써 가시성 향상에 주력하였다. 다만, 약 4천개의 IP를 분석하여 약 2분 안에 가시화 하는 성능에도 불구하고, 로그(log) 파일 기반의 가시화 방법을 취함으로써 실시간으로 가시화가 불가능한 문제점과 더불어 다대다(many-to-many) 트래픽에 대한 분석과 가시화를 제공하지 않음으로써 실제 보안관제환경에는 사용하기 부적합한 단점이 있다.

반면, DAEDALUS-VIZ[21]는 실시간 분석환경을 지원하는 다크넷 보안관제를 위한 가시화 시스템이다. 특히 내/외부 다기관에 걸친 트래픽을 모두 감시하고 침해위협 행위를 검출하는 알고리즘을 설계함으로써 범용성 있는 보안관제 환경을 구축 가능하게 하였다. 또한 Fig.2.과 같이 직관적인 정보를 제공하기 위하여 가시성 높은 3차원(3D) 그래픽 인터페이스를 채용함으로써 시각적 공간 활용과 직관성 향상의 극대화를 추구하였다.

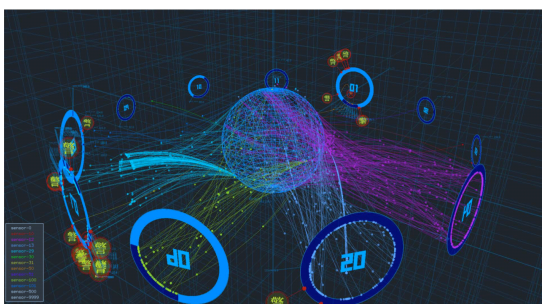


Fig. 2. Visualization example from DAEDALUS-VIZ[21]

다만, 모든 침해의심 트래픽에 대하여 IP간 선(line)으로 표현하는 가시화 기법으로 인하여, 대규모 네트워크에 적용 시 화면상에 너무 많은 선이 표현되어 오히려 보안관리자의 직관성을 저해하는 경우가 발생한다. 또한 세부 침해 정보나 현황을 확인 시에, 각각의 대상 IP를 확대하여 클릭한 후 드릴다운(drill-down) 형태로 단계별 검색을 수행해야하는 불편함이 존재한다.

본 연구에서는 실제 보안관제 환경을 지원하기 위한 가시화를 수행하기 위해서, 실시간기반 분석 및 가시화 환경을 지원하고, 대규모 네트워크의 침해위협 발생 상황을 직관적으로 파악할 수 있는 통합 가시화 방법론을 제시한다. 또한 침해위협 가능성이 높은 주요 IP들과 각 세부내용을 효율적으로 추출 및 제공 가능한 가시화의 방법론을 제안하고 이를 실제로 구현 및 현장에 적용하고 그 결과를 제시한다.

III. 가시화 방법론

본 논문에서 제안하는 가시화 방법론의 가장 큰 장점은 공격자(IP)의 행위정보를 실시간은 물론 추적(통계) 분석할 수 있다는 점이다. 따라서 제안하는 가시화 방법론은 사용자(분석가)에게 이러한 장점이 보장된 분석환경을 제공함으로써, 보안관제 등 사이버위협정보 분석 업무의 최종 목표인 공격자(IP)를 특정(탐지)할 수 있는데 많은 기여를 할 수 있다. 이를 위해 본 논문에서는 보안이벤트 등 사이버위협 정보에서 추출한 송신자(공격자) IP를 중심으로 해당 IP의 공격행위를 사전에 정의한 통계(추적)정보를 활용하여 시간 흐름(실시간)에 따라 가시화하기 위한 새로운 방법론을 제안한다.

3.1 가시화 방법론 전체 구조

Fig.3.은 본 논문에서 제안하는 실시간 및 통계적 가시화 방법론의 전체 개념도를 나타낸다. 제안하는

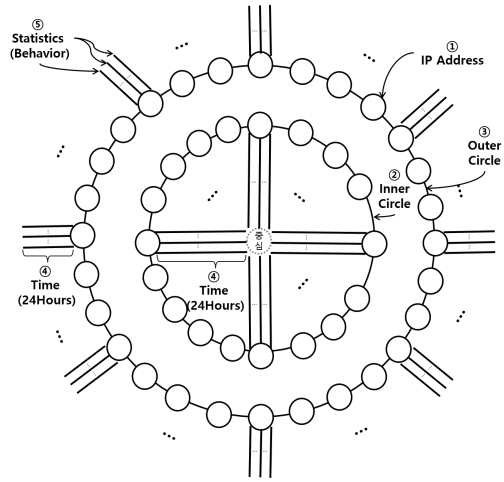


Fig. 3. Conceptual image of the proposed visualization methodology

가시화 방법론은 아래와 같이 크게 5개 부분으로 구성되어 있다.

① IP주소 : 보안이벤트에서 추출한 송신자(공격자)를 나타낸다. 각 IP주소는 다른 IP주소와 중복되지 않고 서로 다른 공격자를 의미한다. 한 화면에 표시할 수 있는 전체 IP 주소의 개수에 제한이 있기 때문에, 본 논문에서는 500개의 IP 주소를 동시에 가시화할 수 있는 시스템을 제안한다. 실제로 500개 이상의 IP주소를 동시에 가시화하는 것도 가능은 하지만, 4장에서 설명하는 실제 시스템 구현 및 활용 측면에서 볼 때, 사용자(분석가)에 대한 가독성 및 실용성을 보장할 수 있는 최대 개수가 500개 수준인 것을 경험적으로 발견했다. 또한, 실제 보안장비가 탐지한 보안이벤트의 신규 송신자(공격자)는 지속적으로 발생(증가)하기 때문에, 본 논문에서는 500개의 IP 주소를 유지(추가 및 삭제)하기 위한 방법도 제시하며 상세한 내용은 3.6에서 설명한다.

② 내원 : ①에서 설명한 500개의 IP 주소를 효율적으로 표현하기 위해 본 논문에서는 크게 2개의 원(내원 및 외원)을 제안한다. 내원은 안쪽에 있는 작은 원을 의미하며, 본 논문에서는 내원에 최대 150개의 IP주소를 표현하는 방법을 제안한다.

③ 외원 : ①에서 설명한 IP 주소를 표현하기 위한 원을 의미하며, 외원은 내원의 바깥쪽에 있는 큰 원을 의미하며, 본 논문에서는 외원에 최대 350개의 IP주소를 표현하는 방법을 제안한다.

④ 시간 정보 : 각 IP의 공격행위를 보여주기 위한 시간을 의미하며, 사용자 정의에 의해 변경이 가능하다. 다만 본 논문에서는 보안이벤트의 탐지, 분석, 통계정보 생성 등의 처리시간을 고려하여 경험적인 기준으로 최소 단위를 1분(실시간 가시화), 최대 시간을 24시간(통계적/추적 가시화)으로 제안한다. 최소단위를 단축(예: 30초 등) 또는 연장(예: 2분, 5분 등)하는 경우, 전자의 경우는 스캐닝, DDoS공격, 플루딩 등 실시간성이 중요한 사이버공격 탐지에 효과적이며, 후자의 경우는 APT 등 장기간에 걸쳐 발생하는 공격의 탐지에 효과적일 수 있다. 각 IP주소의 시간정보는 ①에서 설명한 IP주소에서 멀어지는 방향으로 시간이 증가(1분 단위)하는 것을 나타낸다. 내원에 위치하고 있는 IP주소의 시간정보는 내원의 안쪽(중심) 방향으로 증가하고, 외원에 위치하고 있는 IP주소의 시간정보는 외원의 바깥쪽 방향(내원의 반대 방향)으로 증가한다.

⑤ 통계(행위) 정보 : 각 IP의 공격행위에 대한 심각성 정도(수치)를 선으로 표현한 정보를 의미하며, ④에서 설명한 시간 정보 상에 수직으로 표시한다.(3.2 참고) 공격의 위험도가 증가할수록 통계 정보의 심각성 정도를 나타내는 선의 길이도 길어진다. 이러한 통계 정보의 종류는 공격패턴이 다양하게 나타날 수 있는 현실을 고려하여, 단순히 1개의 통계정보를 정의하는 것이 아니라 여러 다른 종류의 통계정보를 표현할 수 있다. 본 논문에서는 10개의 서로 다른 행위정보를 정의하고, 이에 대한 상세내용은 3.4에서 설명한다.

3.2 IP별 공격행위 가시화 방법론

Fig.4.는 각각의 IP에 대해 공격행위(통계정보)를 표시하는 방법을 보여준다. 3.1에서 설명한 바와 같이, 각 IP는 여러 종류의 통계정보를 표시할 수 있으며, Fig.4.는 특정 IP에 대한 1개의 통계정보를 시간 순서에 따라 가시화 하는 개념도를 나타낸다.

Fig.4.에서 알 수 있듯이, 각 IP에 대한 공격행위는 1분 단위로 그 심각성 정도(수치)를 시간정보와 수직으로 표현한다. 예를 들면, '특정 IP가 1분 동안 발생시킨 보안이벤트의 개수'로 통계정보를 정의한 경우, 특정 IP가 발생시킨 이벤트의 개수가 많을수록 선의 길이가 길어진다. 각 IP에 대한 공격행위 가시화는 3.4에서 정의한대로 10개의 서로 다른

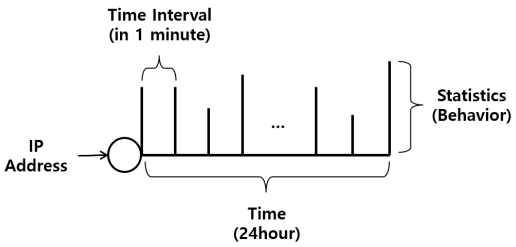


Fig. 4. Conceptual image of attack behavior (statistics) on IP

통계정보를 표현할 수 있다. 시간정보는 1분 단위로 최대 24시간(최대 1,440개의 수직선)까지 표현할 수 있다.

3.3 시간흐름에 따른 가시화 방법

Fig.5.는 3.2에서 설명한 각 IP의 공격행위(통계정보)가 시간 흐름(1분 단위)에 따라 가시화 되는 개념도를 보여준다. 특정 IP가 최초로 출현했을 경우, 해당 IP에 대한 공격행위의 심각성 정도(수치)는 Fig.5.의 (a)와 같이 가시화 된다. 예를 들면, '특정 IP가 1분 동안 발생시킨 보안이벤트의 개수'로 통계정보를 정의한 경우, 최초 1분 동안 해당 IP가 10개의 보안이벤트를 발생시킨 것을 의미한다. Fig.5.의 (b)와 (c)는 해당 IP가 2분 째 및 K분 째 발생시킨 공격행위 정보를 나타내며, 시간이 지남에 따라 1분 단위로 해당 IP의 시간정보의 길이도 점차 늘어나게 된다. Fig.5.의 예제에서는 2분 째 및 K분 째도 동일하게 10개의 보안이벤트를 발생시킨 것을 의미한다. 마지막으로, Fig.5.의 (d)는 해당 IP가 1,440분 째(24시간) 발생시킨 공격행위 정보를 나타내며, 이 때 시간정보의 길이는 최대가 된다. Fig.5.의 예제에서는 해당 IP가 총 12개의 보안이벤트를 발생시킨 것을 의미한다. 이와 같은 보안이벤트 가시화 방법론을 활용하여 실제로 분석할 수 있는 공격행위의 대표적인 사례는 3.5에서 상세하게 설명한다.

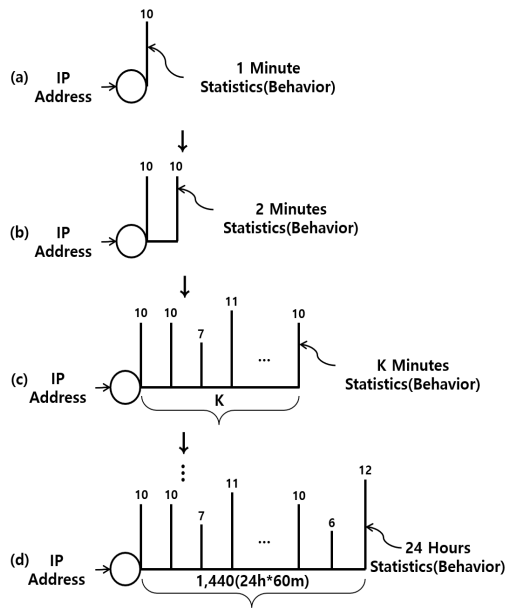


Fig. 5. Conceptual image for attack behavior of IP according to the change of time (in 1-minute increments)

3.4 IP에 대한 공격행위(통계정보) 정의

Table 1.은 각 IP의 공격행위를 정의하기 위한 10개 종류의 통계정보를 보여준다. 1번부터 8번까지의 공격행위 정보는 1분 내에서의 수치(심각성 정도)를 실시간으로 산출하는 것을 의미하고, 9번과 10번 통계정보는 24시간 내에서 1분 단위의 수치(심각성 정도)를 누적하여 통계정보를 산출하는 것을 의미한다. 따라서 3.1, 3.2 및 3.3에서 설명한 본 논문의 가시화 방법론은 그 자체로 실시간성과 추적성(통계성)을 모두 보유하고 있을 뿐만 아니라, 본 논문에서 정의한 공격행위 측면에서도 두 가지 장점을 모두 확보하고 있다. Table 1.의 10개 종류의 공격행위에 대한 의미는 아래와 같다.

1. # of security events : 각 IP가 1분 동안 발생시킨 보안이벤트의 총 개수. 예를 들면, 특정 IP가 1분 동안 총 10개의 보안이벤트를 발생시켰다면, 통계정보는 '10'이 된다.
2. Type # of security events : 각 IP가 1분 동안 발생시킨 전체 보안이벤트에 포함된 서로 다른 보안이벤트 종류의 개수. 예를 들면, 특정 IP가 발생시킨 10개의 보안이벤트가 'SQL injection' 및 'Webshell upload'라는 2개 종류로 구성되어 있다면, 통계정보는 '2'가 된다.
3. # of unique destination IP addresses : 각 IP가 1분 동안 발생시킨 전체 보안이벤트에 포함된 서로 다른 목적지 IP의 개수. 예를 들면, 특정 IP가 발생시킨 10개의 보안이벤트 내에, 서로 다른 목적지 IP가 '1.1.1.1', '2.2.2.2', 및

Table 1. Description of 10 Attack Behaviors

No	Attack Behavior	Remarks
1	# of security events	Real-time (in 1 minute)
2	Type # of security events	
3	# of unique destination IP addresses	
4	# of unique destination Port numbers	
5	# of unique source Port numbers	
6	Difference in # of security events	
7	# of destination Blacklist IP addresses	
8	# of destination Whitelist IP addresses	
9	Average of time interval	Statistics (during 24 hours)
10	Standard deviation of time interval	

'3.3.3.3'이라는 3개로 구성되어 있다면, 통계정보는 '3'이 된다.

4. # of unique destination Port numbers : 각 IP가 1분 동안 발생시킨 전체 보안이벤트에 포함된 서로 다른 목적지 포트의 개수. 예를 들면, 특정 IP가 발생시킨 10개의 보안이벤트 내에, 서로 다른 목적지 포트가 '22', '80', 및 '143'이라는 3개로 구성되어 있다면, 통계정보는 '3'이 된다.
5. # of unique source Port numbers : 각 IP가 1분 동안 발생시킨 전체 보안이벤트에 포함된 서로 다른 송신지 포트의 개수. 예를 들면, 특정 IP가 발생시킨 10개의 보안이벤트 내에, 서로 다른 송신지 포트가 '10,000' 및 '20,000'이라는 2개로 구성되어 있다면, 통계정보는 '2'가 된다.
6. Difference in # of security events : 각 IP가 이전 1분 및 현재 1분 동안 각각 발생시킨 전체 보안이벤트 개수의 차이. 예를 들면, 특정 IP가 이전 1분 동안 10개의 보안이벤트를 발생시켰고, 현재 1분 동안 20개의 보안이벤트를 발생시켰다면, 통계정보는 '10'이 된다.
7. # of destination Blacklist IP : 각 IP가 1분 동안 발생시킨 전체 보안이벤트에 포함된 서로 다른 목적지 IP 중에서 블랙IP에 해당되는 개수. 예를 들면, 특정 IP가 발생시킨 10개의 보안이벤트 내에, 서로 다른 목적지 IP가 '1.1.1.1', '2.2.2.2', 및 '4.4.4.4'이고, 이 중에서 '4.4.4.4'가 블랙IP에 해당 된다면, 통계정보는 '1'이 된다.
8. # of destination Whitelist IP : 각 IP가 1분 동안 발생시킨 전체 보안이벤트에 포함된 서로 다른 목적지 IP 중에서 화이트IP에 해당되는 개수. 예를 들면, 특정 IP가 발생시킨 10개의 보안이벤트 내에, 서로 다른 목적지 IP가 '1.1.1.1', '2.2.2.2', 및 '4.4.4.4'이고, 이 중에서 '1.1.1.1' 및 '2.2.2.2'가 화이트IP에 해당 된다면, 통계정보는 '2'가 된다.
9. Average of time interval : 각 IP가 보안이벤트를 최초로 발생시킨 시점부터 현재 시점까지 중에서, 보안이벤트를 발생시킨 시점 간의 간격(1분 단위)을 평균한 값. 예를 들면, 특정 IP가 보안이벤트를 최초로 발생시킨 시점부터 2분 간격으로 총 5회 연속으로 보안이벤트를 발생시켰다면, 통계정보는 '2'가 된다.
10. Standard deviation of time interval : 각 IP가 보안이벤트를 최초로 발생시킨 시점부터 현재 시점까지 중에서, 보안이벤트를 발생시킨 시점 간의 간격(1분 단위)에 대한 표준편차. 예를 들면, 특정 IP가 보안이벤트를 최초로 발생시킨 시점부터 2분 및 3분 간격으로 총 10회 연속으로 보안이벤트를 발생시켰다면, 통계정보는 '표준편차(2,3,2,3,2,3,2,3,2,3)' = '0.5'가 된다.

3.5 IP 공격행위의 대표적 사례

3.4에서 설명한 10개 종류의 공격행위(통계정보)에 대해 본 논문에서 제안한 가시화 방법론(3.1 ~ 3.3)을 적용하는 경우의 대표적인 사례를 Fig.6.에서 보여준다. 본 논문에서 제안하는 가시화 시스템은 실시간 및 통계분석이 가능하기 때문에, 각 IP(공격자)의 공격행위에 대한 순간적인 변화뿐만 아니라, 규칙/불규칙적인 패턴 변화 등을 직관적으로 인지 및 분석할 수 있다.

예를 들면, 특정 IP의 공격행위의 빈도/양 등이 지속적으로 증가, 일정하게 유지, 감소하는 경우, Fig.6.의 (a), (b), (c)와 같은 형태로 가시화될 수

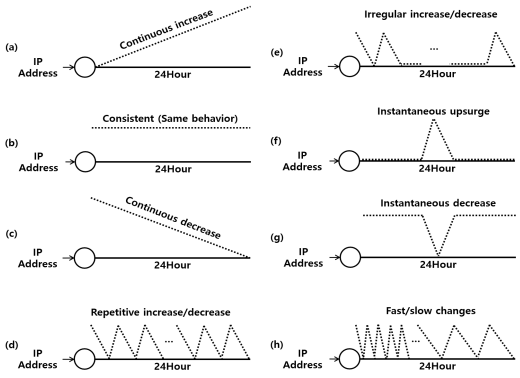


Fig. 6. Representative cases of attack behavior

있다. 또한, 특정 IP의 공격행위가 규칙적으로 증가/감소 반복, 불규칙적으로 증가/감소 반복, 특정 시점에서 급격하게 증가 또는 감소, 공격빈도의 빠름/느림 변화 등에 대해서도 Fig.6.의 (d), (e), (f), (g), (h)와 같은 형태로 가시화될 수 있다. 이와 같은 대표적인 8가지 사례 외에도, 이러한 공격행위가 조합된 형태로 복합적으로 발생하는 경우에도 본 논문에서 제안한 가시화 시스템을 통해 사용자(분석가)는 직관적으로 인지할 수 있다.

3.6 IP별 위험도 산출 방법(스코어링 알고리즘)

3.1에서 설명한 바와 같이, 본 논문에서 제안하는 가시화 방법론은 최대 500개의 IP 주소에 대한 공격행위를 실시간 및 통계적으로 가시화할 수 있다. 비록 본 논문에서 제안하는 가시화 방법론이 전체 IP 주소 또는 보안이벤트를 동시에 가시화하는 것은 현실적으로 불가능하지만, 가시화 시스템 자체는 기존 텍스트 기반 분석체계를 완전히 대체할 수 있는 것이 아니라, 상호보완적인 관계로 서로 병행해서 운영·발전할 필요가 있다. 따라서 가시화 시스템은 모든 보안이벤트 또는 모든 공격자 IP를 모니터링하고 분석하는데 활용하는 것 보다는, 위험도가 높은 IP를 우선적으로 선별·분석하여 신속·정확하게 실제 해킹공격을 탐지하는 것이 보다 실효성이 있을 것이다. 이러한 측면에서 볼 때, 본 논문에서 제안하는 IP주소 기반 가시화 방법론은 현실적으로 유효하고 활용가능성이 높아 보인다.

본 논문에서는 대규모 보안이벤트에 포함된 송신자(공격자) IP 중에서 500개를 선별 및 유지하기 위해 아래와 같은 IP별 스코어링 알고리즘(위험도 산출 방법)을 제안한다. 제안하는 스코어링 알고리즘은 Table 2.에서 나타내는 모두 5개의 통계정보를 활용하여 산출한다. 제안하는 스코어링 알고리즘은, 3.4에서 제안한 10개 종류의 공격행위 정보와 유사하게, A, B, C 통계정보는 1분 내에서의 수치(심각성 정도)를 실시간으로 산출하는 것을 의미하고, D와 E 통계정보는 24시간 내에서 1분 단위의 수치(심각성 정도)를 누적하여 통계정보를 산출하는 것을 의미한다. 따라서 각 IP의 위험도를 실시간 특징과 장기간(통계성) 특징을 모두 고려하기 때문에 보다 정확한 위험도 산출이 가능하다. Table 2.의 5개 종류의 공격행위 중, A, B, C 및 D는 3.4의 1, 3, 4, 9와 의미가 동일하다. E(Appearance count)의 경우는, 각 IP가 보안이벤트를 최초로 발생시킨 시점부터 현재 시점까지 중에서, 보안이벤트를 발생시킨 시점(1분 단위)의 개수(출현 빈도)를 의미한다. 예를 들어, 특정 IP가 보안이벤트를 최초로 발생시킨 시점부터 현재 시점까지 총 5번 발생(출현)했다면, 통계정보는 '5'가 된다.

본 논문에서 제안하는 스코어링 알고리즘은 Table 2.에서 나타낸 5개 종류의 통계정보를 활용하여 각 IP에 대해 아래와 같이 위험도(R)를 도출한다. 여기서 $Max.$는 전체 IP에 대한 각 통계정보의 최댓값을 의미한다.

$$R = \frac{A}{Max.} + \frac{B}{Max.} + \frac{C}{Max.} + \frac{D}{Max.} + \frac{E}{Max.}$$

예를 들어, 특정 IP에 대해 $A=10$, $B=5$, $C=20$, $D=2$, $E=30$의 값을 갖는다고 하자. 이는, 해당 IP가 현재 시점(1분 단위)에 총 10개

Table 2. Five statistical information

	Meaning	Remarks
A	# of security events	Real-time (in 1 minute)
B	# of unique destination IP addresses	
C	# of unique destination Port numbers	
D	Average of time interval	Statistics (during 24hour)
E	Appearance count	

($A=10$)의 보안이벤트를 발생시켰고, 여기에는 총 5개($B=5$)의 서로 다른 목적지 IP와 20개($C=20$)의 서로 다른 목적지 포트가 있는 것을 의미한다. 또한, 해당 IP가 최초로 보안이벤트를 발생시킨 시점 이후부터, 1분 단위로 총 30번($E=30$) 출현했으며, 출현 시점의 평균 간격은 2분($D=2$)인 것을 의미한다. 이 경우에, 전체 IP에 대한 A, B, C, D, E의 최댓값($Max.$)이 각각 20, 10, 100, 10, 30이라고 하면, 해당 IP의 위험도(R)는 다음과 같다.

$$R = \frac{10}{20} + \frac{5}{10} + \frac{20}{100} + \frac{2}{10} + \frac{30}{30}$$

$$= 0.5 + 0.5 + 0.2 + 0.2 + 1 = 2.4$$

위와 같은 스코어링 알고리즘에 따라, 각 IP에 대해 산출한 점수가 높은 순서부터 500위까지의 IP주소가 3.1에서 설명한 가시화 시스템 상에 표시된다. 다시 말해, 현재 1분 동안 신규로 발생한 송신자(공격자) IP주소가 20개라고 하면, 기존에 가시화되어 있는 500개의 IP 주소 중에서 스코어링 점수가 가장 낮은 20개의 IP가 가시화 시스템에서 삭제되고, 해당 자리에 신규로 추가된 IP가 가시화 되는 방식이다.

IV. 가시화 시스템 구현

4.1 시스템 개발 및 구동 환경

Table 3.은 3장에서 제안한 실시간 및 통계적 가시화 방법론을 실제로 구현 및 구동하기 위한 주요사양을 보여준다. 먼저 소프트웨어(S/W)의 경우에는, 가시화 엔진은 Unity 3D를 활용했으며, 가시화에 필요한 보안이벤트 수집 및 통계처리를 위해서는 Python, 사용자 편의를 위한 웹 화면은 Tomcat을 활용했다. 개발한 시스템을 구동하기 위한 하드웨어는 현재의 일반적인 서버사양 수준으로 구성했다.

개발한 가시화 시스템을 국내 부문보안관제센터인 과학기술사이버안전센터(S&T-CSC: Science & Technology Cyber Security Center)에 실제로 적용하여 성공적으로 구동이 되는 것을 확인했다. 과학기술사이버안전센터는 한국과학기술정보연구원(KISTI), 한국전자통신연구원(ETRI), 한국과학기술원(KAIST) 등 국내 과학기술 분야 61개 국가·공공 기관에 대한 실시간 보안관제 업무를 수행하고 있으며, 일평균 2,000만 건, 1분당 평균 1만 건/최대 10만 건의 보안이벤트를 실시간으로 수집·분석하고 있다. 개발한 가시화 시스템이 이러한 대규모 보안이벤트를 실시간으로 처리할 수 있다는 것은 대부분의 보안관제 센터에서도 활용될 수 있는 실용성 또한 갖추고 있다는 것을 의미한다.

Table 3. Main Software and Hardware specifications for Development and Execution of the proposed Visualization System

Type		Specification
Engine	Visualization	Unity 3D
	Data Collection & Statistical Processing	Python
	Web Interface	Tomcat
Database		Maria DB
CPU		Intel i7-3770K@3.50Ghz
Memory		32GB
HDD		2TB

4.2 가시화 시스템 전체 화면

Fig.7.는 본 논문에서 제안한 실시간 및 통계적 가시화 시스템을 실제로 구현한 화면(이하 '가시화 시스템')을 보여준다. 3장에서 설명한 방법론과 마찬가지로, 가시화 시스템은 크게 내원 및 외원으로 구성되어 있으며, 내원과 외원에는 각각 150개 및 300개의 IP 주소(작은 원)를 가시화 한 것을 알 수 있다. 또한 내원과 외원에 위치한 500개 IP주소의

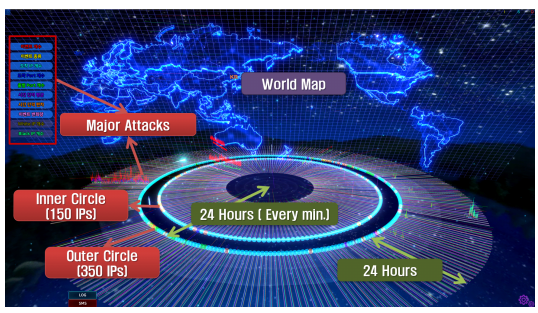


Fig. 7. Overall screen of visualization system

공격행위를 1분 단위로 24시간 동안 가시화하였고, 각 IP에 대해 3.4에서 정의한 10개의 통계정보를 가시화한 것을 알 수 있다. 또한, 본 논문의 가시화 시스템은 실제 공격현황 등을 보다 효율적으로 분석하기 위해, 각 IP의 공격이 어느 국가/도시를 향해 발생하는지를 실시간으로 가시화하도록 세계지도를 추가로 구현했다.

4.3 IP 주소 가시화 화면

Fig.8.은 가시화 시스템의 내원 및 외원 상에 위치하는 각 IP주소를 보여준다. IP 주소는 하나의 작은 원으로 표시되어 있으며, 내원의 IP에 대한 공격행위는 시간이 흐름에 따라 중심방향으로 표시되고 외원의 IP에 대한 공격행위는 가시화 시스템 바깥쪽으로 증가하는 방향으로 표시된다. 또한, 본 논문의 가시화 시스템은 각 IP주소의 유형을 표시할 수 있도록 개발했다. IP 주소가 보안관제 대상기관 내의 시스템이고 해당 시스템에 대한 유형정보를 확보하고 있다면 PC, 서버, 네트워크 장비 등에 대한 정보를 동시에 가시화하는 것은 보다 효율적인 관제업무를 수행하는데 많은 도움이 될 것이다.

Fig. 8. Display of IP address

4.4 10개 종류의 공격행위(통계정보) 가시화 화면

Fig.9.은 가시화 시스템의 내원 및 외원 상에 위치하는 각 IP주소의 공격행위를 나타내기 위한 10개의 통계정보를 보여준다. 각 IP별로 최대 10개의 통계정보를 1분단위로 24시간 동안 가시화할 수 있으며, 사용자의 선택에 따라 가시화하기 위한 통계정보의 개수를 최소 1개에서 최대 10개까지 변경할 수 있다. 가시화하기 위한 통계정보의 선택은 화면 좌상단에 표시한 통계정보 버튼을 클릭 또는 해제하는 형태로 개발했다.

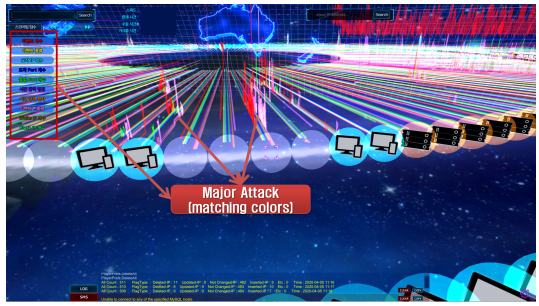


Fig. 9. 10 kinds of statistical information

4.5 스코어링 알고리즘 및 IP주소 추가/삭제 화면

Fig.10.은 현재 가시화 시스템에서 표시하고 있는 전체 500개 IP에 대한 위험도를 계산한 스코어링 점수를 보여주는 화면이다. Fig.10.에서는 상위 20개 IP에 대해 3.6절에서 설명한 스코어링 알고리즘에 따라 산출한 점수를 내림차순으로 표시하고 있다.

예를 들어, 1위 스코어링 점수는 3.2점, 20위는 1.92점을 나타내고 있다. 이와 같은 스코어링 점수

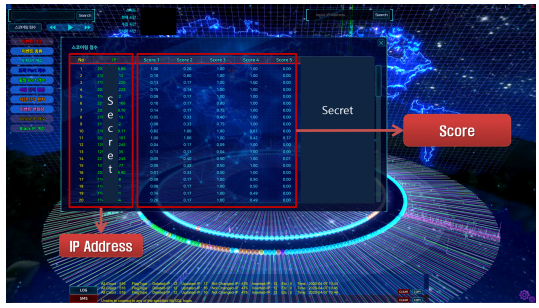


Fig. 10. Risk scores of all 500 IP addresses (Top 20)

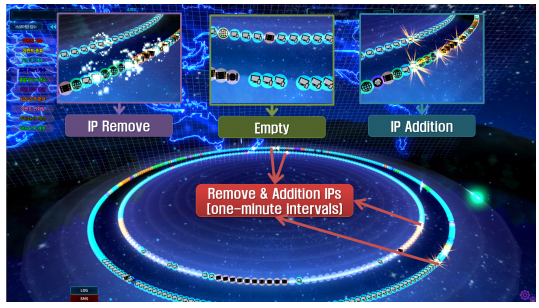


Fig. 11. Remove and Addition of IP addresses

에 따라서 500개 IP 중에서 하위에 있는 IP들은 삭제되고 신규로 출현한 IP가 삭제된 IP의 위치로 추가된다. IP의 추가 및 삭제 화면은 Fig.11.에서 보여준다.

4.6 공격행위 장기간 분석 화면

Fig.12.은 각 IP 주소에 대한 공격행위를 최소 1일부터 최대 1년까지 장기간 분석할 수 있는 화면을 보여준다. 가시화 시스템의 내원 및 외원 상의 IP주소를 클릭하면 해당 IP에 대한 기본정보 및 최대 1년간의 10개 통계정보에 대한 공격행위를 분석할 수 있다. 분석가는 이러한 장기간 분석 기능을 활용하여 보다 효율적인 공격 탐지 및 분석업무를 수행할 수 있다.

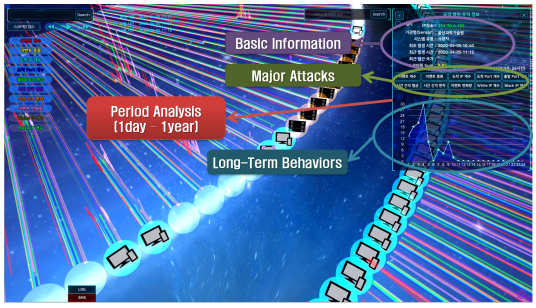


Fig. 12. Attack behaviors of each IP address in the long term(1day ~ 1year)

V. 유효성 검증 및 활용 사례

본 논문에서 제안된 방법론의 유효성을 검증하기 위하여, 가시화 시스템을 활용한 악성코드 감염으로 인한 호스트 악용 검출 및 비인가 암호화폐 채굴 행위의 트래픽 탐지 사례에 대하여 살펴본다. 특히, Fig.6.의 IP 공격행위의 특정 패턴 가시화 정보를 바탕으로 텍스트 형태의 로그에서 발견하기 어려운 침해사고를 효과적으로 발견하고 대응함으로써 실제 보안관제 환경에 활용 가능성을 확인하였다.

Fig.13.과 Fig.14.은 악성코드 감염을 통한 호스트 악용으로 인하여 C2 서버로 일정한 간격마다 지속적인 접근 시도 및 활성화 여부를 확인(health check) 하는 침해사고의 예로써, 본 논문에서 제안된 가시화 방법(Fig.13.)과 기존 텍스트 기반 시스템의 분석 결과(Fig.14.)를 나타낸다. Fig.13.은

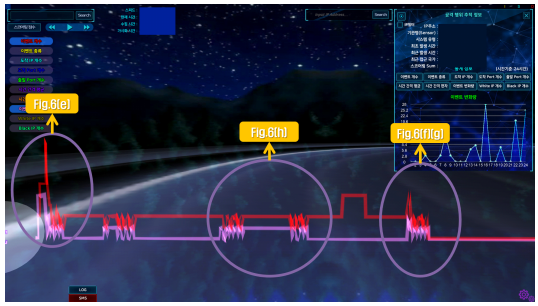


Fig. 13. Example of visualization for suspicious threats (malware)

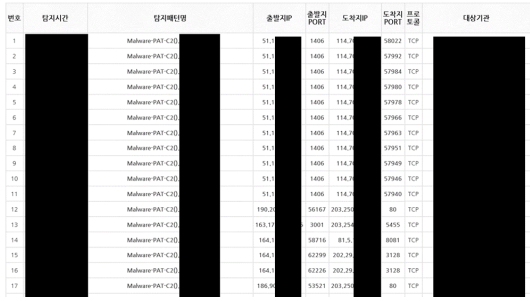


Fig. 14. Monitoring result from traditional text-based alert system

3.4절에서 정의한 IP 공격행위의 대표적 패턴 중 Fig.6.(e), Fig.6.(f), Fig.6.(g), 그리고 Fig.6.(h)이 복합적으로 가시화되어 표현된 것을 쉽게 확인할 수 있다. 즉, 가시화 결과로 부터 사용자는 즉각적으로 패턴을 확인하여 해당 IP에 대해 침해위협 정도가 높은 것으로 파악하고 적시에 분석 및 대응 과정을 수행할 수 있다 (실제 침해사고 대응 수행완료).

반면, Fig.14.는 기존 텍스트 기반 침해위협 탐지 시스템의 예로써, 단순 텍스트 형태의 로그를 테이블 형태로 사용자에게 제공 하는 관계로 사용자의 비효율적인 악성행위의 판단과 탐지 과정을 초래한다.

한편, 비인가 암호화폐 채굴행위의 경우 Fig.15.와 같이 이벤트 변화량(빨간색 라인)과 출발지 Port 개수(녹색 라인)의 통계정보가 지속적으로 높고 일정한 패턴(Fig.6.(b) 패턴)을 나타내는 가시화 결과를 통해 출발지 포트가 많이 발생하고, 보안이벤트가 다량으로 발생하는 것을 쉽게 식별할 수 있다. 다시 말하면, 암호화폐 채굴은 주로 출발지 포트는 동일하지 않으나 채굴결과 수신 도착지 포트는 동일하며, 암호

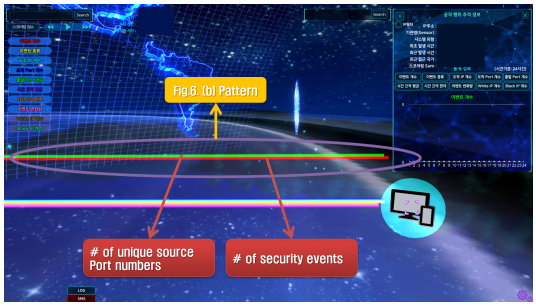


Fig. 15. Example of visualization for suspicious threats (cryptocurrency miner)

화폐 채굴결과를 지속적으로 송신해야 하므로 동일한 행위를 나타내는 패턴이 발생하기 쉽다. 따라서 Fig.15.의 가시화 결과로부터 해당 악성 의심행위를 쉽게 판단 가능하다. 이 경우, 악성코드 감염의 경우와 같이 Fig.15. 형태의 정보를 사용자에게 제공한다면, 해당 침해행위의 판단이 매우 어려운 것을 쉽게 확인할 수 있다.

뿐 만 아니라, Fig.6.(b)과 동일한 패턴이 발생하더라도 Fig.16.과 같이 색상(즉, 도착, 출발 IP 및 포트 등) 으로 구분되는 가시화 결과로부터 타 침해행위 또한 탐지가 가능하다. 예를 들어, Fig.15. 와 Fig.16.의 경우 동일한 행위가 반복되는 같은 패턴을 보이지만, 가시화 대상 (즉, 도착 및 출발 port) 그래프의 상대적 위치관계를 통해 서로 다른 침해 행위의 탐지가 가능하다.

실제 탐지 사례에서 살펴본 결과로부터, 네트워크 상에 발생하는 다양한 공격들이 본 연구에서 제안된 방법을 통한 가시화를 통해 특정 패턴으로 발생함을 확인 할 수 있었고, 이를 통해 사용자의 직관적인 탐지를 가능하게 함과 동시에 실제 보안관제 환경에 사용 가능함을 확인 하였다.

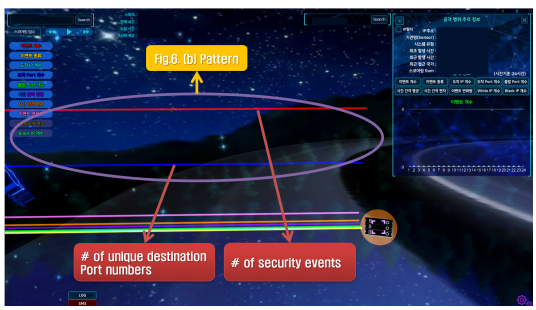


Fig. 16. Example of visualization for suspicious threats (port scanning)

VI. 결 론

본 논문에서는 기존의 보안관제체계의 한계점을 극복하기 위해 대규모 보안이벤트를 실시간 및 통계적으로 가시화할 수 있는 방법론을 새롭게 제안했다. 제안한 가시화 시스템은 각 IP에 대한 10개의 공격행위를 정의하고, 최대 500개의 IP에 대한 공격행위를 1분 단위로 최대 24시간 동안 실시간 및 추적해서 모니터링이 가능하다. 또한, 각 IP에 대한 위험도를 산출하는 스코어링 알고리즘을 활용하여 가장 위험도가 높은 500개의 IP만을 선별하여 집중관제가 가능하도록 하였다.

제안한 가시화 시스템을 구현하여 실제 보안관제 업무를 수행하고 있는 과학기술사이버안전센터에 적용 및 운영하는데 성공하였으며, 다양한 공격자 IP를 탐지 및 분석하는데 성공함으로써 본 논문에서 제안한 가시화 방법론의 실용성 및 유효성을 검증했다.

기존 가시화 방법의 프로그램, 데이터출처(소스) 등이 공개되어 있지 않으며, 기존 연구에서도 타 연구와의 정성적 또는 정량적 비교·평가를 수행하지 않고 실제 탐지 사례를 활용하였기에, 본 논문에서도 3건의 실제 사이버공격 탐지 사례를 통해 제안한 가시화 방법론의 우수성을 증명하였다. 또한, 본 논문의 가시화 방법론은 공격자(IP)의 행위정보를 실시간 및 추적(통계) 분석하는 것으로, 방법론적 측면에서도 기존 가시화 방법들과 차이점이 확실히 존재하며 한계점 또한 극복하였다고 할 수 있다.

본 논문에서는 IP의 공격행위를 10개 종류만 제안을 하였지만, 향후에는 보다 다양한 공격행위를 정의하고 이를 가시화하기 위한 고도화 연구를 수행해야 할 것이다. 또한, 가시화 가능한 최대 IP 개수(500개), 가시화 가능한 최대 시간(24시간) 등 현실적인 제약사항을 극복하기 위한 연구가 필요할 것이다.

References

[1] Korea Information Security Industry Association (KISIA), Annual report for 2019: Survey for information security industry in korea, 2019.

[2] Korea Information Security Industry Association (KISIA), The First Annual report for 2019: Industry trend of information security report,

2019.
[3] McAfee Labs, Quarterly Threat Report for 2016: McAfee labs threats report, Dec. 2016.
[4] Ponemon Institute Research, Analyst Research Report for 2019: Improving the effectiveness of the SOC, June. 2019.
[5] Endance, Research Report for 2019: Challenges of managing and securing the network, 2019.
[6] Imperva, Survey for 2108: 27 Percent of IT professionals receive more than 1 million security alerts daily, May. 2018.
[7] Demisto, The second annual state of incident response report for 2018: The state of SOAR report, 2018.
[8] Enterprise Management Associates (EMA), White Paper for 2017: InfoBrief: a day in the life of a cyber security pro, May. 2017.
[9] Lee Dong-Gun , Kim, Huy Kang, and Kim, Eunjin, "Study on security log visualization and security threat detection using RGB palette," The Journal of the Korea Institute of Information Security & Cryptology, 25(1), pp. 61-73, Feb. 2015
[10] Park, Jae-Beom, Kim, Huy Kang, and Kim, Eunjin, "Design and implementation of the honeycomb structure visualization system for the effective security situational awareness of large-scale networks," The Journal of the Korea Institute of Information Security & Cryptology, 24(6), pp. 1197-1213, Dec. 2014
[11] Koo Bon-Hyun, Cho kyu-Hyung, Cho Sang-Hyun, and Moon Jong-Sub, "Real-time web attack detection visualization tool design and implementation using HTTP header information," Proceedings of the Korea Institutes of Information Security and Cryptology Conference, pp. 637-640, June. 2006
[12] Girardin, Luc, "An eye on network intruder-administrator shootouts," Proceedings of the Workshop on Intrusion Detection and Network Monitoring, pp. 19-28, 1999.
[13] K.Nyarko, T.Capers, C.Scott, and K.Ladeji-Osias, "Network intrusion visualization with NIVA, an intrusion detection visual analyzer with haptic integration," Proceedings 10th Symposium on Haptic Interfaces for Virtual Environment and Teleoperator Systems. HAPTICS 2002, pp. 277-284, Mar. 2002.
[14] Y.Zhao, F.Zhou, X.Fan, X.Liang, and Y.Liu, "IDSRadar: a real-time visualization framework for IDS alerts," Science China Information Sciences, vol. 56, no. 8, pp. 1-12, 2013.
[15] Roesch, Martin, "Snort: Lightweight intrusion detection for networks," In Proceedings of the 13th USENIX conference on System administration (LISA '99), vol. 99, no. 1, pp. 229-238, Nov. 1999.
[16] Koike, Hideki, and Kazuhiro Ohno, "SnortView: visualization system of snort logs," Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, pp. 143-147, 2004.
[17] K.Abdullah, C.P.Lee, G.Conti, J.A.Copeland, and J.Stasko, "IDS rainStorm: visualizing IDS alarms," IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05), pp. 1-10, 2005.
[18] Shiravi, Hadi, Ali Shiravi, and Ali A.Ghorbani, "IDS alert visualization and monitoring through heuristic host

selection," Proceedings of the 12th International Conference on Information and Communications Security, pp. 445-458, 2010.

[19] F.Fischer, J.Fuchs, F.Mansmann, and D.A.Keim, "BANKSAFE: A visual situational awareness tool for large-scale computer networks: VAST 2012 challenge award: Outstanding comprehensive submission, including multiple vizes," In 2012 IEEE Conference on Visual Analytics Science and Technology (VAST), pp. 257-258, Oct. 2012.

[20] T.Itoh, H.Takakura, A.Sawada and K.Koyamada, "Hierarchical visualization of network intrusion detection data," In IEEE Computer Graphics and Applications, vol. 26, no. 2, pp. 40-47, 2006.

[21] D.Inoue, M.Eto, K.Suzuki, M.Suzuki, and K.Nakao, "DAEDALUS-VIZ: novel real-time 3D visualization for darknet monitoring-based alert system," Proceedings of the ninth international symposium on visualization for cyber security, pp. 72-79, Oct. 2012.

〈저자소개〉

문 형 우 (Hyeongwoo Moon) 정회원
2005년 2월: 배재대학교 컴퓨터공학과 졸업
2015년 2월: 충남대학교 컴퓨터공학과 석사
2012년 2월~2018년 12월 국가보안기술연구소 기술원
2019년 4월~현재: 한국과학기술정보연구원 과학기술사이버안전센터 연구원
〈관심분야〉 보안관제, 침해사고대응, 악성코드 분석, 네트워크 보안

권 태 웅 (Taewoong Kwon) 정회원
2012년 2월: 숭실대학교 컴퓨터학부 졸업
2014년 8월: 고려대학교 정보보호대학원 정보보호학과 석사
2014년 12월~현재: 한국과학기술정보연구원 과학기술사이버안전센터 연구원
〈관심분야〉 정보보호, 보안관제, 네트워크 보안, 네트워크 가시화

이 준 (Jun Lee) 정회원
2010년 2월: 한국항공대학교 정보통신공학과 졸업
2012년 2월: 한국항공대학교 정보공학 석사
2017년 8월: 한국항공대학교 정보공학 박사
2017년 4월~2017년 11월: 일본산업기술종합연구소(AIST) 연구보조원
2017년 12월~2019년 12월: 일본산업기술종합연구소(AIST) 박사후연구원
2019년 12월~현재: 한국과학기술정보연구원 과학기술사이버안전센터 선임연구원
〈관심분야〉 인공지능, 보안관제, 지식추출, 자연언어처리, 네트워크보안

류 재 철 (Jaecheol Ryou) 종신회원
1985년 2월: 한양학교 산업공학과 졸업
1988년 5월: Iowa State University 전산학 석사
1990년 12월: Northwestern University 전산학 박사
1991년 2월~현재: 충남학교 컴퓨터공학과 교수
〈관심분야〉 인터넷보안, 블록체인, 전자지불 시스템

송 중 석 (Jungsuk Song) 정회원
2003년 2월: 한국항공학교 통신정보공학 졸업
2005년 2월: 한국항공학교 정보공학 석사
2009년 3월: 교토학교(일본) 지능정보학 박사
2009년 4월~2010년 9월: 일본정보통신연구원 정보통신 보안연구소 전문연구원
2010년 10월~2011년 9월: 일본정보통신연구원 네트워크 보안연구소 선임연구원
2011년 10월~2018년 3월: 한국과학기술정보연구원 과학기술사이버안전센터 선임연구원
2018년 3월~현재: 한국과학기술정보연구원 과학기술사이버안전센터 책임연구원
2012년 9월~현재: 과학기술연합학원학교 데이터 및 HPC 과학 교수
〈관심분야〉 보안관제, 침해사고대응, 악성코드 분석, 네트워크 보안