디지털산업정보학회 논문지 제16권 제1호-2020년 3월
http://dx.doi.org/10.17662/ksdim.2020.16.1.067

APT 공격 탐지를 위한 공격 경로 및 의도 인지 시스템*

김 남 욱** · 엄 정 호***

Attack Path and Intention Recognition System for detecting APT Attack

Kim Namuk · Eom Jungho

〈Abstract〉

Typical security solutions such as intrusion detection system are not suitable for detecting advanced persistent attack(APT), because they cannot draw the big picture from trivial events of security solutions. Researches on techniques for detecting multiple stage attacks by analyzing the correlations between security events or alerts are being actively conducted in academic field. However, these studies still use events from existing security system, and there is insufficient research on the structure of the entire security system suitable for advanced persistent attacks. In this paper, we propose an attack path and intention recognition system suitable for multiple stage attacks like advanced persistent attack detection. The proposed system defines the trace format and overall structure of the system that detects APT attacks based on the correlation and behavior analysis, and is designed with a structure of detection system using deep learning and big data technology, etc.

Key Words : Advanced Persistent Threat, Correlation Analysis, Behavior Analysis, Trace Format, Intrusion Detection

Ⅰ. 서론

사이버공격은 점차 고도화되고 있으며, 그 규모와 피해는 광범위해지고 있다. 그 뿐만 아니라 과거와는 달리 뚜렷한 목표를 가진 사이버공격이 주를 이르고 있으며, 공격자들은 공격 목적과 대상에 따라 오랜 시간동안 준비과정을 걸쳐서 각 공격단계에 필요한 공격 도구와 방식을 선정한 후 공격 대상 기관과 기업 네트워크에 침투하여 정보를 습득하거나 시스템을 파괴하는 형태의 정밀공격을 수행한다. 이러한 지능형 지속공격(APT)은 IT 인프라에 크게 의존하고 있는 대부분의 기관과 기업에서 큰 위협으로 다가오고 있다.

지능형 지속공격과 같은 정교한 사이버공격을 탐지하기 위해서는 대규모 네트워크를 구성하는 많은 수의 노드와 노드 간의 통신을 통해 발생하는 이벤트들을 종합적으로 분석할 수 있는 알고리즘이 필요하다. 학계에서는 이와 관련된 다양한 알고리즘 개발이 활발히 이루어지고 있는 가운데, 인공지능을 활용한

* 이 논문은 2019년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임(NRF-2019R1F1A1041782).
** 성균관대학교 컴퓨터공학과 박사과정
*** 대전대학교 군사학과&안전융합학부 교수(교신저자)

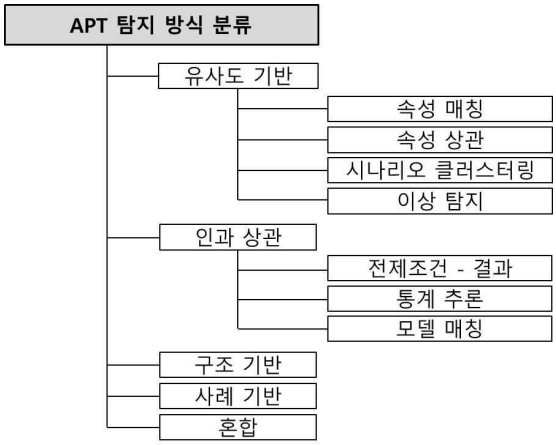
사이버공격 경로와 의도를 사전에 식별하여 공격 대상의 핵심 시스템까지 침입하지 못하도록 하는 기술 연구도 진행되고 있다. 이제는 더 이상 침입탐지시스템(IDS)과 같이 단일 공격만을 탐지하여 보안 이벤트나 경고신호를 전송하는 보안 솔루션으로는 지능형 지속공격과 같은 정교한 사이버공격을 차단할 수 없다[1, 2]. 따라서 본 논문에서는 APT 공격 탐지에 특화된 공격 경로 및 의도 인지 시스템을 제안하고자 한다. 2장에서는 관련연구를 살펴보고, 3장에서는 공격 경로 및 의도 인지 시스템 설계에 대해서 설명한다. 4장에서는 제안한 시스템을 시나리오 기반 실험을 진행하고 5장에서 결론을 맺는다.

II. 관련연구

여러 단계의 공격절차로 이루어진 사이버공격을 탐지하고 공격 경로를 예측하기 위한 연구는 활발하게 진행되고 있다. 이러한 연구들은 모두 네트워크 모니터링 로그와 시스템 로그를 포괄하는 트레이스를 사용한다는 것과 트레이스를 이용하여 예상되는 공격 시나리오 또는 공격 경로에 대한 모델링을 통해 공격을 인지한다는 점에서 일치한다. 다만, 다양한 트레이스간의 연관성을 파악하는 방식에서 차이를 보이는데, 트레이스간 유사도에 의해 공격 시나리오의 구성을 결정하는 방식과 각 공격 단계의 인과관계에 초점을 맞춘 방식이 주를 이루며, 그 밖에 구조기반, 사례기반 등의 방식이 있다. <그림 1>에서 보시는 바와 같이 유사도기반 방식은 다시 속성매칭, 속성상관, 시나리오 클러스터링, 비정상 탐지방식으로 구분되며, 인과상관 기반 방식으로는 전제 조건-결과 방식, 통계추론 방식, 모델매칭 방식으로 구분된다. 앞서 언급한 APT 공격 탐지 방식 중 유사도기반의 분석 방식은 공격의 각 단계 간의 유사성에 따라 시나리오를 구성하는 방식이다. 이 방식의 기본 전제는 서로 유사한 점을 갖는 alert들은 동일한 근원으로부터 발생한 것이기 때문에 동일한 공격 시나리오로 묶을 수 있다는 점이다. 따라서 이 방식에서는 alert 간의 유사성을 어떻게 계산하느냐가 가장 중요한 이슈이다. 트레이스간 유사성은 각 트레이스가 지닌 속성 또는 필드 값을 이용해 계산된다. 속성 값의 예로는 IP 주소, 포트 주소, 타임스탬프, 트레이스의 종류 등이 있다. 이 속성 값들 간의 비교연산은 탐지 방식에 따라 다르며 연산 결과를 일반적으로 상관지수라고 부른다. 탐지방식에 따라 상관지수는 가장 단순하게는 이진값일 수도 있고 복잡한 상관함수 형태로 표현될 수도 있다. 유사도기반 방식은 트레이스 간 상관관계를 찾기 위한 알고리즘을 설계하는 것이 어렵다. 단순히 몇 개의 필드만을 비교하는 단순한 알고리즘의 경우에 오류 (false positive)가 발생할 확률이 높으며, 상관 매트릭스 기반의 복잡한 분석 알고리즘의 경우에는 지나치게 좁은 범위의 공격만 탐지하는 단점이 있다. 하지만, 일단 알고리즘이 결정되면 구현이 쉽고 성능이 좋으며, 알려지지 않은 APT 공격도 찾을 수 있기 때문에 유사도기반 방식은 다른 방식에 비해 많이 연구되고 실질적으로도 많이 사용되고 있다[3-16]. <그림 1>은 APT 탐지방식의 분류를 보여준다.

현재까지 진행된 연구들은 대부분 기존의 특정 침입탐지 시스템에서 생성되는 alert만을 트레이스로 이용하는데, 이는 단일 공격을 탐지하여 alert를 발생시키는 데 있어서는 우수하지만, 지능적인 공격자가 각 사이버공격 단계를 정상적으로 활동으로 보이도록 잘 설계된 표적공격과 APT를 탐지하는 데는 한계가 있다[3]. 따라서 표적공격과 APT 공격을 탐지하고 공격 양상을 예측하는 데 필요한 트레이스의 종류와 수집 방식, 또한 이들을 통합하여 분석하기 위한 모델을 재정의 할 필요가 있다. 또한, 대부분의 연구들은 공격 시나리오를 구성하기 위해 수집된 트레이스들

을 연관 짓기 위한 방법으로 단일 방식으로 연관분석을 수행하는데, 공격 유형에 따라 효율적이고 정확한 예측을 위한 방식을 다양하게 적용할 필요가 있다 [17].



<그림 1> APT 탐지 방식 분류 [1]

본 논문에서는 유사도분석 기반으로 APT 공격 탐지하는 시스템의 전반적인 구조를 정의한다. 기존의 IDS나 보안 솔루션에서 생성되는 이벤트나 alert 등에 의존하지 않도록 새롭게 APT 공격 탐지에 적합한 트레이스 형식을 정의하였으며, 다양한 탐지방식이 적용될 수 있는 구조를 갖도록 설계하였다.

Ⅲ. 공격 경로 및 의도 인지 시스템

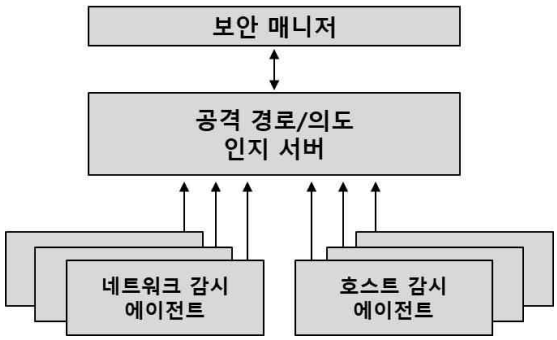
제안하는 시스템은 <그림 2>와 같은 프레임워크를 갖으며, 각 서브시스템의 기능은 다음과 같다.

○ 보안 매니저 : 침입탐지 관련 보안정책들을 관리하고 이를 분석모듈에 통보하여 사이버공격과 관련된 시스템의 이상 징후 판단과 자동 반응에 대한 기준을 제공하며, 보안관제 담당자가 사용하는 PC에 설치되며 공격 경로 및 의도 인지 서버와 네트워크를 통해 연결된다.

○ 공격 경로 및 의도 인지 서버 : 네트워크/호스트 에이전트들로부터 수집한 데이터를 가공한 후 분석하여 정상행위를 학습한다. 이를 기반으로 사이버공격과 관계된 이상 징후를 식별하며, 내부망에서 접근성이 가장 좋은 위치에 배치시킨 각 에이전트들로부터 감시 트레이스 정보를 실시간으로 수신한다.

○ 네트워크 감시 에이전트 : 내부망을 이루는 각 부분 망에 하나씩 배치되어 네트워크 송·수신 패킷을 감시하고 수집된 트레이스를 공격 경로 및 의도 인지 서버로 전송한다.

○ 호스트 감시 에이전트 : 내부망의 모든 노드에 배치되어 노드의 행위를 모니터링하면서 트레이스를 수집한 후에 공격 경로 및 의도 인지 서버로 전송한다.

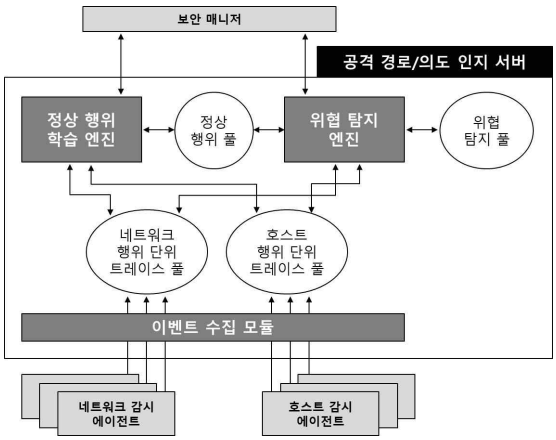


<그림 2> 공격 경로 및 의도 인지 시스템의 프레임워크

3.1 공격 경로 및 인지 서버 구성

공격 경로 및 인지 서버의 세부 구성은 <그림 3>과 같다. 서버는 이벤트 수집 모듈, 정상행위 학습 엔진, 위협탐지 엔진 등의 주요 컴포넌트로 구성되고 데이터 저장소는 네트워크/호스트 행위 단위 트레이

스 풀, 정상행위 풀, 그리고 위협탐지 풀을 갖는다. 주요 모듈의 기능은 다음과 같다.



<그림 3> 공격 경로 및 의도 인지 서버의 구성

○ 이벤트 수집 모듈 : 네트워크/호스트 감시 에이전트로부터 수집한 트레이스를 종합하고 수집된 감시 트레이스는 네트워크/호스트 행위 단위 트레이스 풀에 저장된다.

○ 정상행위 학습 엔진 : 수집된 감시 트레이스들로부터 정상적인 행위 범위를 도출하여 이를 정상 행위 풀에 저장한다. 정상행위 범위의 도출에 있어서는 자동학습으로 얻어진 결과를 보완하고 수동 설정이 필요한 경우에 보안 매니저가 정상행위 학습에 기여할 수 있도록 지원한다.

○ 위협 탐지 엔진 : 수집된 감시 트레이스들을 정상행위 풀에 저장된 트레이스들을 이용해 비교분석하여 의심이 가는 트레이스를 추출하고 이를 그룹화시켜 위협탐지 풀에 저장한다. 의심 트레이스 그룹들은 의심 등급을 설정하여 임계치에 도달하면 보안 매니저에게 알려준다.

○ 데이터 저장소 : 단위 트레이스 풀은 네트워크와 호스트 각각 감시대상 속성을 선정하고 선택한 속성에 대한 단위 트레이스를 종합하여 고유한 트레이스 풀을 생성한다. 정상행위 풀은 외부에서 학습된 각종 사이버 위협 트레이스와 이를 학습하여 생성한 유사패턴을 종합하여 특정 이벤트나 패턴이 공격과 관련되었는지를 판단하는 기준을 수립한다. 위협탐지 풀은 단위 트레이스 풀로부터 의심되는 트레이스를 추출하였을 때 이를 그룹화 시켜 저장하기 위해 사용한다.

본 시스템에서 사용하는 수집 이벤트는 크게 네트워크 행위 단위 트레이스와 호스트 행위 단위 트레이스가 있다[18]. 네트워크 행위 단위 트레이스는 전송중인 하나의 패킷에 대한 트레이스를 나타낸다. 일반적으로 <표 1>과 같은 세부정보를 포함한다.

<표 1> 네트워크 행위 단위 트레이스의 포맷

세부 정보명		내 용
Time		패킷을 발견한 시간
Flow ID		각 플로우마다 고유 식별 번호를 부여하여 해당 패킷이 어느 플로우에 속하는지 알 수 있게 함
Source Addr		송신측 IP 주소 + Port 번호
Dest Addr		수신측 IP 주소 + Port 번호
Protocol	Lower Protocol	애플리케이션 계층의 하위 계층에 대한 프로토콜 정보 (TCP / UDP / ICMP / ETC)
	Upper Protocol	애플리케이션 계층에 대한 프로토콜 정보 (HTTP / SMTP / POP / IMAP / FTP / Telnet / SSH / DNS / SSL / TLS / SIP / GTP 등)
Hdr Info	IP Header	IP 헤더 필드 값
	Lower Protocol Header	TCP / UDP / ICMP 등의 프로토콜 헤더 정보
	Upper Protocol Header	HTTP / SMTP / POP / IMAP / FTP / Telnet / SSH / DNS / SSL / TLS / SIP / GTP 등의 프로토콜 헤더 정보
Content		데이터 영역의 모든 비트 들
Alarm		네트워크 감시 에이전트에서 감지한 침해 정보

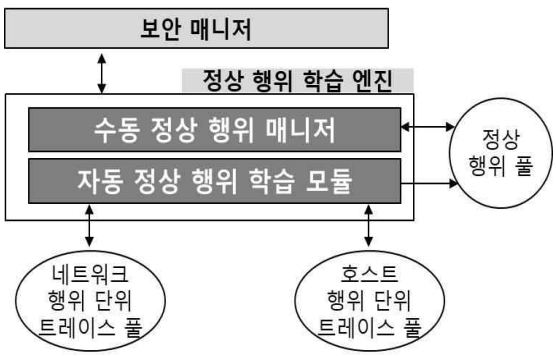
호스트 행위 단위 트레이스는 하나의 프로세스가 다른 프로세스 또는 프로세스 외부에 영향을 미친 동작에 대한 정보를 나타낸다. 일반적으로 <표 2>와 같은 세부정보를 포함한다.

<표 2> 호스트 행위 단위 트레이스의 포맷

세부 정보명	내 용
Time	Action이 발생한 시간
Action	발생한 Action의 구체적인 내용
Action Source	Action을 발생시킨 주체에 대한 모든 정보 (Host 이름 및 주소, Process 정보 등)
Action Destination	Action이 영향을 미치는 지점에 대한 모든 정보 (Host 이름 및 주소, Process 정보, 파일명, 레지스트리 정보 등)
Protocol	애플리케이션 계층에 대한 프로토콜 정보 (HTTP / SMTP / POP / IMAP / FTP / Telnet / SSH / DNS / SSL / TLS / SIP / GTP)
Alarm	호스트 감시 에이전트에서 감지한 침해 정보

1) 정상행위 학습 엔진

정상행위 학습 엔진에서는 단위 트레이스별로 가치 있는 학습 데이터를 생성하기 위한 기준(기간, 데이터량 등)을 설정하여 분석 목적에 부합하는 의미 있는 학습 트레이스를 생성한다. 정상행위 학습 엔진은 <그림 4>와 같이 구성된다.



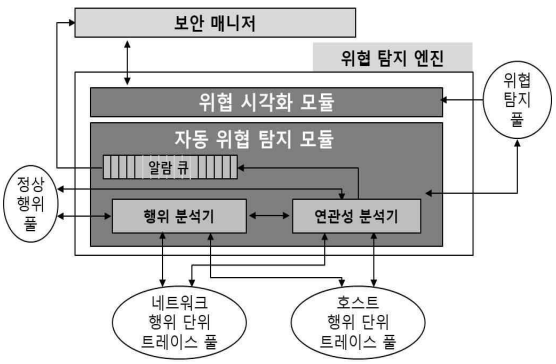
<그림 4> 정상행위 학습 엔진

수동 정상행위 매니저는 보안관제 담당자가 얻어진 정상행위 단위 트레이스들에 대하여 수동적 설정이 가능하도록 한다. 이는 정상행위 범위를 도출하는데 있어서 자동화된 학습으로 얻어진 결과를 보완하고 수동적인 설정이 필요할 수 있기 때문이다. 이를 통해 보안 정책을 추가 및 삭제할 수 있다.

자동 정상행위 학습 모듈은 일반적인 상태에서 수집된 대량의 트레이스를 딥러닝 기술로 학습하여 행위 주체 별 정상행위 범주를 정하는 역할을 한다. 행위 주체별 정상행위 범주를 하나의 정상행위 단위 트레이스로서 정상행위 풀에 저장한다.

2) 위협탐지 엔진

위협탐지 엔진은 수집된 감시 트레이스를 정상행위 트레이스와 비교하여 의심 트레이스에 대한 알람을 생성하는 방식으로 위협을 탐지하며, 보안 매니저에게 위협을 알리거나 의심되는 감시 트레이스를 시각화하여 보여주는 기능을 포함한다. 위협탐지 엔진은 <그림 5>와 같이 위협 시각화 모듈과 자동 위협탐지 모듈로 구성된다.



<그림 5> 위협탐지 엔진

위협 시각화 모듈은 위협탐지 풀에 저장되어 있는

의심 트레이스 그룹 내 트레이스 정보와 그들의 연관 관계를 표현한 트레이스 정보를 보안 매니저에게 전달함으로써 보안관제 담당자가 위협정보를 보다 효과적으로 인지할 수 있게 한다.

자동 위협탐지 모듈은 행위 분석기와 연관성 분석기가 있다. 행위 분석기는 유입된 단일 트레이스에 대하여 정상여부를 판별하되, 판별 기준은 정상행위 풀로부터 참조한다. 연관성 분석기는 정상행위 범주에 들지 않는 의심 트레이스에 대한 2차 분석을 하고 의심 트레이스로 분류된 단위 트레이스들에 대하여 그룹화 시킴으로서 사이버공격의 절차와 경로를 파악한다. 또한, 특정 의심 트레이스 그룹의 의심 등급이 위험 등급에 도달하면, 보안 매니저에게 전달하기 위한 알람 정보를 알람 큐에 저장한다.

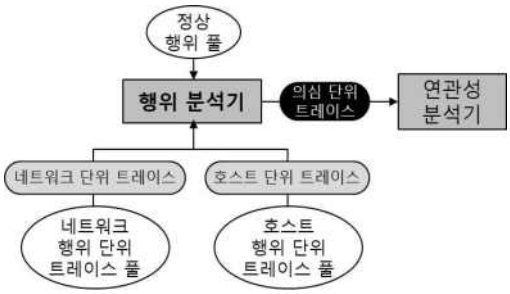
3.2 위협 탐지 메커니즘

자동 위협탐지 모듈의 위협탐지 메커니즘은 행위 분석기와 연관성 분석기가 주 기능을 담당하며, 데이터 마이닝 기법을 활용하여 사이버공격과 관련된 네트워크 속성과 호스트 속성을 도출하고 선택한 속성 사이의 연관관계를 파악하여 침입을 탐지한다.

1) 행위 분석기

행위 분석기는 유입된 단위 트레이스의 정상 여부를 판별하여, 그 결과에 따라 의심 트레이스일 경우에는 트레이스를 연관성 분석 모듈로, 정상일 경우에는 원래 있던 풀로 전달하는 역할을 수행한다.

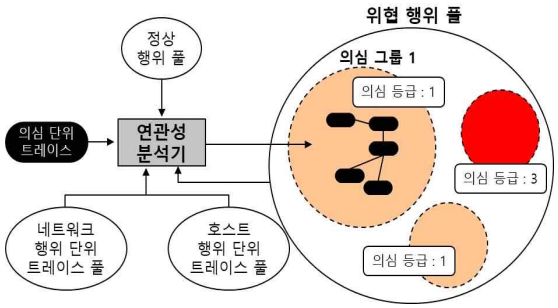
동작과정은 우선 네트워크 단위 트레이스 또는 호스트 단위 트레이스가 위협 탐지 엔진에 입력되면, 트레이스로부터 행위 주체를 추출해 내고 정상행위 풀로부터 동일한 행위 주체를 갖는 정상행위 단위 트레이스를 가져온다. 정상행위 단위 트레이스와 트레이스의 각 필드 값의 비교 연산을 통해 정상 여부를 파악한 후에 의심 트레이스로 판별되는 경우에 연관성 분석기에 전달하며, 정상행위로 판별될 경우 다시 원래 있던 풀에 저장한다.



<그림 6> 행위 분석 메커니즘

2) 연관성 분석기

연관성 분석기는 전달된 의심 트레이스와 연관된 트레이스를 찾아 의심 행위 그룹을 구성하는 역할을 수행한다.



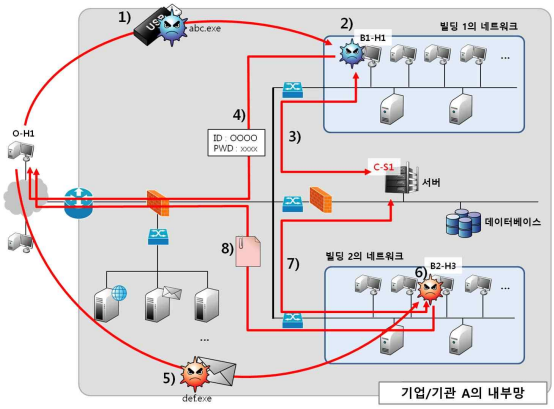
<그림 7> 연관성 분석 메커니즘

위협행위 풀에는 의심 트레이스들로 이루어진 의심 행위 그룹이 존재하며, 하나의 의심 행위 그룹은 하나의 단위 공격을 의미한다. 의심 행위 그룹을 설정한 후 해당 의심 단위 트레이스에 대하여 공격이 이루어진 시간순서와 각 행위들의 연관성을 나타내

는 상호관계 트레이스를 정리하여 그룹 트레이스를 생성한다. 각 의심 행위 그룹에는 위험 수준과 공격의 확실성에 따라 의심 등급을 설정하며, 이 트레이스를 기반으로 보안 관리자에게 알람을 전달할 것인지 보류할 것인지 결정한다. 자동 위협탐지 모듈의 연관성 분석기는 행위 분석기로부터 수신한 의심 단위 트레이스를 위협행위 풀에 저장한다. 위협행위 풀에 트레이스를 저장하기 전에 위협행위 풀에 있는 의심 행위 그룹들과의 연관성 분석을 통해 특정 의심 행위 그룹에 속하는지 판단해야 한다. 특정 의심 행위 그룹에 속하면 해당 그룹의 멤버 단위로서 저장하고 상호관계 트레이스를 갱신한다. 만약, 특정 의심 행위 그룹에 속하지 않으면 새로운 그룹을 생성하여 저장한다. 그리고 네트워크 행위 단위 트레이스 풀과 호스트 행위 단위 트레이스 풀에 있는 트레이스들과 연관성 분석을 통해 연관된 단위 트레이스들을 모두 추출하여 의심 단위 트레이스로서 동일한 그룹에 저장하되 인과적/시간적 순서에 따른 그래프 형태로 저장한다.

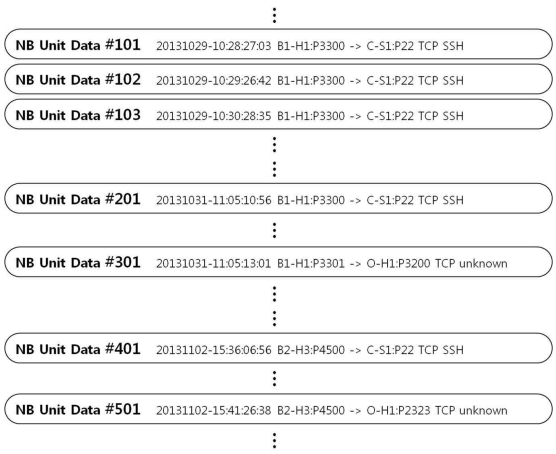
IV. 공격 시나리오에 의한 실험

제안한 시스템의 실험은 APT 공격 시나리오에 기반하여 위협을 탐지하는 방식으로 진행한다[19]. 시나리오는 제안한 시스템이 다단계 정밀 공격의 공격 경로를 예측하는 것으로 일반적인 APT 공격 방식을 활용한다. APT는 공격 대상 시스템에 침투하고 정보를 검색한 후에 주공격 대상 시스템에 대한 정보를 수집하고 시스템에 저장된 정보를 유출한다. <그림 8>은 해커가 APT 공격을 통하여 특정 기업의 내부망 중앙 서버에 존재하는 내부정보를 갈취하는 시나리오를 도식화한 것으로 다음과 같은 공격 절차를 거친다고 가정한다.



<그림 8> APT 공격 시나리오

1) 해커가 악성코드(abc.exe)를 제작 후 유포하여 A기업 사원의 USB를 통하여 A기업 내부망으로 잠입하도록 유도
2) A기업 사원의 PC(B1-H1)에 악성코드 abc.exe 설치
3) 악성코드 abc.exe는 기업 내부망에서만 접근할 수 있는 중앙 서버(C-S1)의 원격 접속(SSH) 로그인 아이디와 비밀번호를 알아내기 위한 작업을 지속 수행
4) 악성코드 abc.exe는 중앙 서버의 원격 접속 계정정보를 알아낸 후 로그인 아이디와 비밀번호를 해커의 PC(O-H1)로 전송
5) 해커는 또 다른 악성코드(def.exe)를 제작 후 스팸메일을 통하여 A기업의 사원 PC에 설치되도록 유도
6) A기업의 사원 PC(B2-H3)에 악성코드 def.exe 설치
7) 악성코드 def.exe는 해커가 미리 갈취한 계정정보를 이용하여 중앙 서버에 접속하여 중요정보 열람
8) 악성코드 def는 열람한 중요 정보를 해커의 PC (O-H1)에게 전달



<그림 9> 생성된 네트워크 행위 단위 트레이스

<그림 8>과 같은 공격 시나리오를 제안 시스템이 어떤 순서로 탐지하는지 살펴본다. 내부망의 호스트와 네트워크에서 감시를 수행하는 에이전트들은 행위 단위 트레이스를 <그림 9>와 <그림 10>과 같이 생성한다.

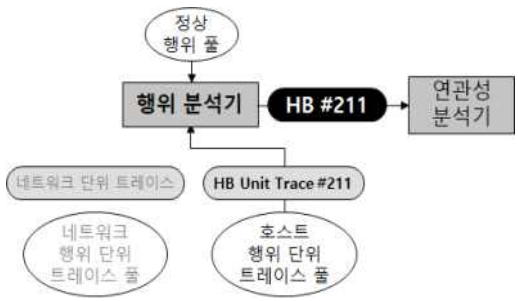
<그림 9>는 네트워크 감시 에이전트가 생성한 네트워크 행위 단위 트레이스들 중 공격 시나리오와 직접적인 관련이 있는 트레이스들만 표현한 것이다.

<그림 10>은 호스트 감시 에이전트가 생성한 호스트 행위 단위 트레이스들 중 사이버공격 시나리오와 직접적인 관련이 있는 트레이스들만 표현한 것이다. <그림 10>과 같이 생성된 행위 단위 트레이스들은 차례대로 위협탐지 모듈의 행위 분석기로 유입되어 의심여부를 판별 받는다.

<그림 10>의 트레이스들 중 가장 먼저 의심 여부를 판별받은 트레이스를 'HB Unit Data #211' 이라고 하면, 행위 분석기에서는 <그림 11>과 같이 동작하여 해당 트레이스를 연관성 분석기로 넘겨준다.

이후에 연관성 분석기에서는 'HB Unit Data #211'과 연관성 있는 그룹이 위협행위 풀에 있는지를 먼저 판단한다. 예제에서 없다고 가정하면, 위심 행위 그룹

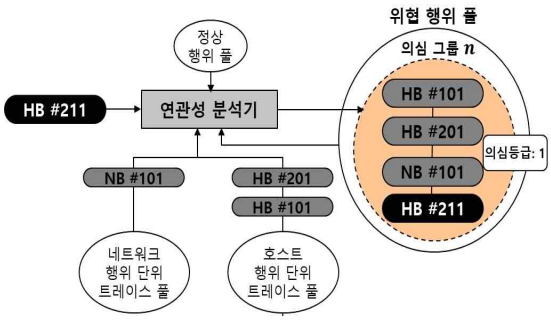
<그림 10> 생성된 호스트 행위 단위 트레이스



<그림 11> HB Unit Data #211에 대한 행위 분석

1이 생성된다. 또한, 각 행위 단위 트레이스 풀로부터 연관된 트레이스를 찾아내어 그룹에 추가하고 상호

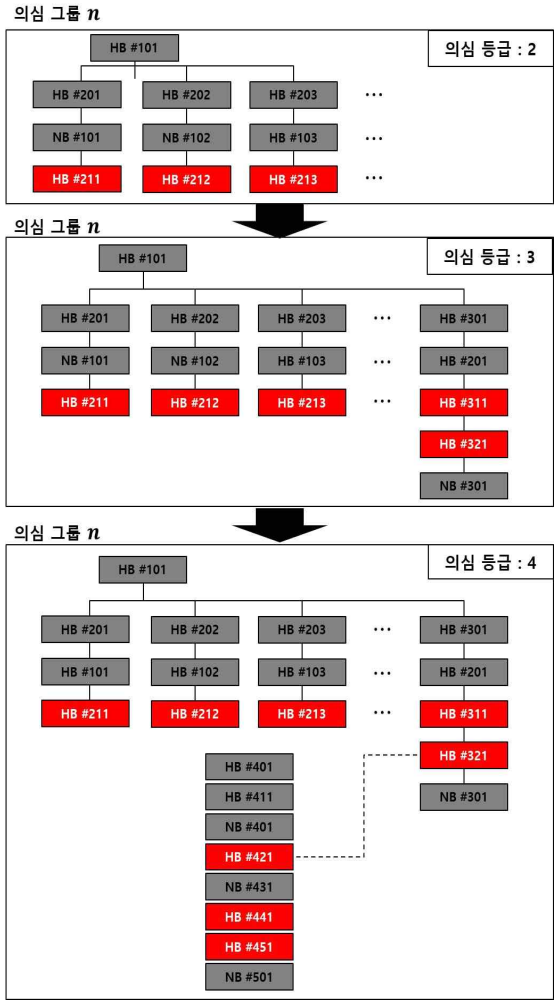
관계를 표시한 후에 그룹에 대한 의심 등급을 1로 설정한다.



<그림 12> HB Unit Data #211의 연관성 분석

이와 같이 계속해서 유입된 행위 단위 트레이스들에 대한 판단과 연관성 분석을 진행하면, 의심 행위 그룹에 아래 <그림 13>의 순서대로 단위 트레이스들이 저장되며 상호 연관성도 표현되어 공격의 전체적인 흐름을 파악할 수 있다.

<그림 13>의 단계를 보면, 우선 첫 단계에서 HB #211, HB #212, HB #213이 로그인 시도가 수차례 실패했음을 나타내는 트레이스로서 탐지된다. 이는 로그인 계정정보를 모르는 해커가 로그인을 성공할 때까지 시도했음을 짐작할 수 있다. 또한, HB #211는 HB #101 (abc.exe 설치), HB #201 (abc.exe가 중앙 서버 SSH 접속 시도) NB #101 (abc.exe가 중앙 서버 SSH로 로그인 패킷 전송)과 의 상관관계를 연관성 분석을 통해 계산되고 의심 그룹 n이 형성되어 저장된다. 이로부터 사원 PC에 알 수 없는 프로그램이 설치된 후, 그 프로그램이 중앙 서버 SSH의 로그인을 갈취하기 위해 수차례 로그인을 시도하고 있음을 유추할 수 있다. 여기까지가 의심 등급 2수준으로서, 이에 대한 조기 알람은 구체적인 공격 경로 및 잠정 의도 정보와 함께 보안 매니저에 전송되어 신속한 대응을 할 수 있게 한다.



<그림 13> 공격 경로 및 의도 판단

만약에 공격이 지속적으로 이루어진다고 가정한다면, #HB 311은 abc. exe가 서버의 SSH에 대한 로그인 시도가 성공했음을 나타는 트레이스로서 #HB 321는 해당 로그인 계정정보를 외부망으로 전달함을 나타내는 트레이스로서 탐지된다. 이 또한 연관성 분석기를 통해 #HB 301, #HB 201, NB#301과 묶인다. 공격이 한 단계 더 진행되었다고 판단되므로 의심 등급이 3수준으로 올라간다.

마지막으로 #HB 421이 또 다른 사원 PC의 def.exe 프로그램이 앞선 공격에서 사용한 로그인 계정으로 서버의 SSH 로그인했고 #HB 441은 서버에서 vi 명령을 이용해 특정 문서를 열람하고, #HB 451은 해당 문서를 외부로 전송했음을 나타내는 트레이스이다. 각 의심 트레이스로서 행위 분석기에 의해 감지되며, 연관성 분석기에 의해 이와 직접적으로 연관된 트레이스들이 시간 순으로 묶인다. 또한, #HB 421은 #HB 321을 통해 유출된 로그인 계정으로 로그인했음을 나타내므로 #HB 421과 #HB가 간접적인 연관이 있을 것으로 연관성 분석기에 의해 유추되어 연결된다. 이와 같이 시간과 인과 순으로 그래프 형태로 각 단위 트레이스를 구성하면, 공격 경로와 의도 파악이 가능하다.

Ⅴ. 결론

본 논문에서는 APT 공격 탐지에 적합한 공격 경로 및 의도 분석 시스템을 제안하였다. 우선, 전체적인 구조를 설계하였으며, 분석에 사용될 단위 트레이스를 정의하였다. 단위 트레이스들은 네트워크/호스트 감시 에이전트를 통해 획득하며, 공격 경로 및 의도 인지 서버에서 분석된다. 제안한 시스템에서는 수집된 단위 트레이스로부터 정상/비정상 행위를 학습하는데 있어서 최신 학습기술을 접목시킨다.

공격 발생 시 단위 트레이스들은 행위 분석과 연관성 분석을 통해 의심 그룹으로 관리되어 관련된 의심 트레이스들이 수집됨에 따라 의심 등급이 증가 또는 감소하게 되며 보안 매니저는 그룹화된 트레이스들을 토대로 공격 경로와 의도를 파악할 수 있다.

향후 제안한 시스템의 구현을 통해서 알고리즘을 평가하고 성능평가를 진행할 계획이다.

참고문헌

[1] 이세열, “블록체인을 적용한 사설 클라우드 기반 침입시도탐지”, 디지털산업정보학회 논문지, 제14권, 제2호, 2018, pp.11-17.

[2] 김창식 · 김남규 · 곽기영, “머신러닝 및 딥러닝 연구동향 분서: 토픽모델링을 중심으로”, 디지털산업정보학회 논문지, 제15권, 제2호, 2019, pp.19-28.

[3] J. Navarro, A. Deruyver and P. Parrend, “A systematic survey on multi-step attack detection,” Computers & Security, Vol.76, 2018, pp.214-249.

[4] Z. Liu, C. Wang and S. Chen, “Correlating multi-step attack and constructing attack scenarios based on attack pattern modeling,” in 2008 International Conference on Information Security and Assurance, 2008, pp.214-219.

[5] A. Ebrahimi, A. H. Z Navin, M. K. Mirnia, H. Bahrbegi and A. A. A. Ahrabi, “Automatic attack scenario discovering based on a new alert correlation method,” in 2011 IEEE International Systems Conference, 2011, pp.52-58.

[6] M. Bateni and A. Baraani, “An architecture for alert correlation inspired by a comprehensive model of human immune system,” International Journal of Computer Network & Information Security, 2014, pp.47-57.

[7] J. Wang, H. Wang and G. Zhao, “A GA-based solution to an NP-hard problem of clustering security events,” in Proceedings of the 2006 International Conference on Communications, Circuits and Systems, 2006, pp.2093-2097.

[8] S. Mathew and S. Upadhyaya, “Attack scenario

recognition through heterogeneous event stream analysis," IEEE Military Communications Conference, 2009, pp.1-7.

[9] S. Shin, S. Lee, H. Kim and S. Kim, "Advanced probabilistic approach for network intrusion forecasting and detection," Expert systems with applications, Vol. 40, No. 1, 2013, pp.315-322.

[10] N. K. Pandey, S. K. Gupta, S. Leekha and J. Zhou, "ACML: capability based attack modeling language," in Fourth International Conference on Information Assurance and Security, 2008, pp.147-154.

[11] Y. Lv, S. Xiang, J. Geng, Y. Li and C. Xia, "An alert correlation algorithm based on the sequence pattern mining," in IEEE Advanced Information Technology, Electronic and Automation Control Conference, 2015, pp.1146-1151.

[12] R. Katipally, W. Gasior, X. Cui and L. Yang, "Multistage attack detection system for network administrators using data mining," in Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, April 2010, pp.1-4.

[13] C. M. Chen, D. J. Guan, Y. Z. Huang and Y. H. Ou, "Anomaly network intrusion detection using Hidden Markov Model," International Journal of Innovative Computer Information and Control, Vol.12, No.2, 2016, pp.569-580.

[14] S. Fayyad and C. Meinel, "New attack scenario prediction methodology," in Tenth International Conference on Information Technology: New Generations, 2013, pp.53-59.

[15] Y. Luo, F. Szidarovszky, Y. Al-Nashif and S. Iariri, "A fictitious play based response strategy for multistage intrusion defense systems," Security and Communication Networks, Vol.7, No.3, 2014, pp.473–491.

[16] A. Sadighian, J. M. Fernandez, A. Lemay and S.T. Zargar, "ONTIDS: a highly flexible context-aware and ontology based alert correlation framework," in 6th International Symposium on Foundations and Practice of Security, 2013, pp.161-177.

[17] 임창완 · 신영섭 · 이동재 · 조성영 · 한인성 · 오행록, "실시간 사이버 위협 지능형 분석 및 예측 기술," 정보과학회 컴퓨팅의 실제 논문지, 제25권, 제11호, 2019, pp.565-570.

[18] 김현진 · 손태식, "스마트시티의 보안을 위한 사이버보안위협정보 활용 연구," 한국디지털콘텐츠학회 논문지, 제20권, 제6호, 2019, pp.1173-1180.

[19] J.H Eom, "Modeling of Cyber-attack Intentions Analysis Reflecting Domestic / International Situations," International Journal of Grid and Distributed Computing, Vol.11, No.1, 2018, pp.13-26.

■ 저자소개 ■

김 남 욱
Kim, Nam Uk

2012년 3월~ 현재 성균관대학교 컴퓨터공학과 박사과정
2012년 2월 성균관대학교 컴퓨터공학과(석사)
2009년 2월 성균관대학교 컴퓨터공학과(학사)

관심분야 : 네트워크/시스템 보안, 프로그래밍 언어
E-mail : nukim8275@gmail.com

엄 정 호
Eom, Jung Ho

2011년 3월~ 현재 대전대학교
군사학과&안전융합학부 부교수
2011년 2월 성균관대학교 정보통신공학부
BK21 연구교수
2008년 2월 성균관대학교 컴퓨터공학과(박사)
2003년 2월 성균관대학교 컴퓨터공학과(석사)
1994년 2월 공군사관학교 항공공학과(학사)

관심분야 : 네트워크/시스템 보안, 사이버전, 접근제어, 내부자보안
E-mail : eomhun@gmail.com

논문접수일 : 2020년 1월 31일
수 정 일 : 2020년 3월 7일
게재확정일 : 2020년 3월 9일