페이로드 시그니처를 이용한 Adobe 소프트웨어 사용자 행위 탐지

이민성, 최정우, 권윤주, 박지태
고려대학교
{min0764, choigoya97, tkwkf12, pjj5846}@korea.ac.kr

Adobe Software User-behavior Detection Using Payload Signature

Lee Min-Seong, Park Jee-tae, Choi jeong-woo, Kwon Yun-Ju
Korea Univ.

요 약

SaaS는 클라우드 기반 소프트웨어 제공 모델로서 구독의 형태로 서비스를 사용 할 수 있다. SaaS 서비스가 확산되면서 많은 기업 및 단체에서 Office365, Adobe, G-suite 등 많은 서비스들을 구입하여 사용하고 있다. 서비스를 구매하여 사용하다 보니 기업과 단체는 소프트웨어 사용 시 모니터링을 통한 관리가 필요하다. 이러한 모니터링을 진행하기 위해서는 각 서비스별로 사용자가 어떤 소프트웨어를 사용하며, 소프트웨어의 어떤 행위를 했는지 파악을 할 필요가 있다. 본 논문에서는 여러 서비스들 중 Adobe 서비스를 대상으로 사용자가 소프트웨어 사용을 위해 어떤 행동을 해야 하는지 정의하고, 정의된 행위를 탐지할 수 있는 방법론에 대해 제안한다.

Ⅰ. 서 론

SaaS는 클라우드 기반 소프트웨어 제공 모델로서 구독의 형태로 서비스를 배포하고 있다. 마이크로소프트의 Office 365, 구글의 G Suite, Adobe의 Creative Cloud 등이 대표적인 SaaS 서비스에 해당한다. SaaS 어플리케이션은 초기 도입 비용이 상대적으로 적고 필요에 따라 사용을 조절할 수 있기 때문에 많은 기업에서 서비스를 구매하여 사용 하고 있다. 이에 따라 기존 소프트웨어를 SaaS 어플리케이션 형태로 제공하는 소프트웨어 회사들도 증가하였으며 구매의 형태도 다양하게 진행되고 있다. 예를 들어, 가장 많이 사용되어온 소프트웨어들만 구매하여 사용을 할 수 있게 하고, 추가적인 금액으로 더 많은 소프트웨어를 사용 할 수 있도록 한다. 기업 및 단체는 필요한 소프트웨어를 사용하기 위하여 선택적으로 구매하여 SaaS 서비스를 사용 할 수 있다. 기업 및 단체의 입장에서 서비스를 구매하여 사용하다 보니 모니터링을 통한 관리가 필요하게 된다. 구매한 서비스를 사용을 하고 있는지 확인하여 적절한 금액으로 필요한 서비스만 사용 할 수 있도록 관리 할 수 있고, 이는 기업이나 단체의 효율적인 자산 운용을 가능하게 한다. 이러한 모니터링을 진행하기 위해서는 각 서비스별로 사용자가 어떤 소프트웨어를 사용했는지 파악 할 수 있어야 하며, 각 소프트웨어에서 사용자가 필수적으로 어떤 행위를 하게 되는지 정의되어야 한다. 본 논문에서는 Adobe 서비스를 대상으로 트래픽을 분석하여 사용자의 행위를 정의하고 정의된 행위를 탐지 할 수 있는 방법론을 제시한다.

Adobe 트래픽을 분석하기 위하여 접근하기 쉬운 페이로드 시그니처를 정의하여 행위를 탐지 할 수 있도록 한다. Adobe트래픽은 여러 SaaS 서비스들과 마찬가지로 SSL/TLS를 기반으로한 암호화된 패킷으로 통신을 한다.[1][2] 따라서 Adobe 소프트웨어 사용 시 발생하는 모든 플로우를 분석하는 것이 아닌 443Port에 해당하는 플로우들만 수집하여 분석하고 페이로드 시그니처를 정의한다.

Adobe에서 제공하는 여러 서비스들의 트래픽을 분석하기 위하여 여러 행위들을 포함한 트래픽을 수집하고 행위를 정의한다. 본 논문의 구성은 서론에 이어, 2장에서 Adobe 행위 탐지를 위한 행위 분석 및 정의와 트래픽 분석 방법론에 대해 기술하고, 마지막으로 결론 및 향후 연구에 대해 기술한 후 마친다.

Ⅱ. 본 론

본 장에서는 Adobe 트래픽을 분석하여 사용자가 Adobe 소프트웨어를 사용할 때의 행위를 탐지하는 방법론에 대하여 기술한다. Adobe의 소프트웨어를 사용하기 위해서는 여러 소프트웨어를 설치하고 사용할 수 있는 통합 서비스인 Adobe Creative Cloud를 사용하는 방법이 있다. 또한, Adobe Creative Cloud를 통해 각 소프트웨어들을 미리 설치 한 후 원하는 소프트웨어를 개별적으로 실행하는 방법이 있다. 본 논문에서는 Adobe Creative Cloud에서 소프트웨어를 실행하는 것은 제외하였다. 소프트웨어는 Premiere Pro, Photoshop, Illustrator 3가지 소프트웨어를 사용하여 각 소프트웨어에서 발생한 트래픽을 대상으로 분석을 진행하였다.

A. Adobe 사용자 행위 분석

Adobe 사용자의 행위 분석을 위하여 소프트웨어를 사용하기 위하여 필수적으로 진행해야 하는 행위를 정의하였다. 3가지 소프트웨어를 사용하면서 여러 가지 공통된 행위를 진행하여 플로우를 분석하였으며, 분석 시 공통적으로 발생한 플로우를 바탕으로 행위를 정의하였다. 기본적으로 3가지 소프트웨어를 사용하였기 때문에, 어떤 소프트웨어를 사용했는지 분석을 진행해야 한다. 하지만, 현재 페이로드 시그니처 기반 분석 방법으로는 소프트웨어를 구분 할 수 없었다. 따라서 소프트웨어 이름 탐지는 제외하였다.

사용자가 Adobe를 사용할 때 나타나는 행위는 크게 소프트웨어 실행, 로그인, 로그아웃, 소프트웨어 종료로 4가지로 정의하였다. 소프트웨어 실행은 사용자가 소프트웨어를 실행을 할 때의 행위이다. 로그인은 사용자가 Adobe 소프트웨어를 사용하기 위하여 필수적으로 해야 하는 행위이다. Adobe 서비스 자체가 구독의 형태로 진행되기 때문에 로그인이 되어 있지 않으면 소프트웨어를 사용 할 수 없다. 또한, 로그인을 하지 않으면 실

행했던 소프트웨어가 자동으로 종료된다. 로그아웃은 사용자가 로그아웃을 하는 행위이며, 소프트웨어 종료는 소프트웨어 사용을 마치고 종료하는 행위이다. 로그인에서와 마찬가지로, 로그아웃을 하게 되면 소프트웨어가 자동적으로 종료된다.

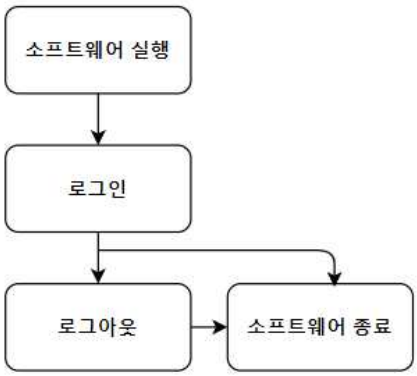

그림 1. 사용자 행위 분석

B. 트래픽 분석 방법 및 행위 탐지

트래픽 분석 방법으로는 각 행위 별 페이로드 시그니처를 정의하여 각 4가지 행위를 탐지하였다. Adobe 소프트웨어를 사용하게 되면 SSL/TLS 기반으로 암호화된 패킷으로 이루어진 플로우가 발생한다. 암호화된 패킷은 443 Port를 사용하여 통신하기 때문에 443 Port에서 발생한 플로우를 기준으로 플로우를 모아서 해당 행위에 대한 페이로드 시그니처를 정의하였다. 정의된 시그니처는 표1에서 확인 할 수 있다.

표 1. 페이로드 시그니처

Behavior	Payload Signature
소프트웨어 실행	"hbrt.adobe.com"
로그인	"oobe.adobe.com"
	"adobeid-nal.services.adobe.com"
	"workflowlicenses.adobe.com"
로그아웃	"sstats.adobe.com"
	"ims-prod06.adobelogin.com"
소프트웨어 종료	"hbrcv.adobe.com"

소프트웨어 실행 시 정의된 페이로드 시그니처를 포함하는 플로우가 발생하며 이를 통해 소프트웨어 실행을 탐지한다. 실행 시 발생하는 시그니처를 가진 플로우는 Adobe 실행 중에도 발생을 한다. 따라서 해당 플로우가 최초로 탐지된 경우에만 실행을 탐지한다. 로그인 행위는 "oobe.adobe.com"시그니처를 가진 플로우 발생 이후 나머지 2가지 시그니처를 포함한 플로우가 5초 이내에 발생하면 탐지된다. 로그아웃 행위 시에는 "sstats.adobe.com"시그니처를 포함한 플로우가 발생 한 후 5초 이내에 나머지 시그니처를 가진 플로우가 발생하면 로그아웃 탐지를 할 수 있다, 소프트웨어 종료 시 정의된 시그니처를 포함한 플로우 발생 시 소프트웨어 종료를 탐지 할 수 있다.

C. 실험 및 검증

개인 PC, 노트북, 학내망 등 여러 환경에서 사용자가 Adobe 서비스를 사용하고 어떤 행위를 하였는지 탐지 하는 실험을 진행하였다. 개인 PC나 노트북에서 수집한 트래픽의 경우, 수집하면서 여러 행동을 조합하여 트래픽을 수집하였으며, 실험 시 해당 행위가 잘 탐지되는지 확인하였다. 실험을 진행하였을 때, 정확하게 사용자의 행위를 탐지 할 수 있었다. 학내망 트래픽의 경우 Adobe 서비스를 사용하는 행위를 탐지 할 수 있었으나 여러 호스트에서 발생하는 트래픽이 모여있기 때문에 정확한 탐지가 되었는지 확인 할 수 없었다. 하지만 호스트 정보와 행위 탐지가 가능하다는 것은 확인하였다.

실험 결과 일반적으로 전체 행위를 진행한다고 가정하였을 때, 소프트웨어가 실행 된 후 로그인을 하고 로그아웃 후 소프트웨어 종료를 진행한다. 하지만 결과에서 소프트웨어 실행 이전에 로그인이 탐지가 되는 경우가 있었다. 이는 소프트웨어 실행 시 발생하는 플로우를 소프트웨어를 실행하자마자 탐지를 진행하는 것이 아닌, 사용자가 작업을 시작하기 위하여 작업 창을 띄우는 시점을 소프트웨어 실행으로 정의하였기 때문이다. 로그인이 되어있지 않을 때, 로그인을 진행하지 않으면 소프트웨어가 종료되고 작업 창을 띄울 수 없다. 따라서 로그인을 한 후 작업창이 뜨게 되는데, 이러한 결과로 소프트웨어 실행시보다 로그인 행위가 먼저 탐지가 되었다. 또한 3가지 소프트웨어(Premiere Pro, Photoshop, Illustrator)를 사용하여 행위를 분석하였는데, 사용자가 같은 행위를 하였을 때 소프트웨어의 구분 없이 공통적으로 행위가 탐지되는 것을 확인하였다. 향후 어떤 서비스의 어떤 행위를 하였는지 탐지하기 위해서는 논문에서 제시한 사용자 행위 탐지 이전에 소프트웨어의 구분이 필요하다.

Ⅲ. 결론 및 향후 연구

SaaS 서비스의 사용량이 많아지면서 기업 및 단체에서 서비스를 구매하여 여러 가지 소프트웨어들을 사용하고 있다. 적절한 구매를 통해 효율적인 자산 운용을 위하여 SaaS 서비스에 대한 모니터링이 필수적이다. 모니터링을 하기 위해서는 SaaS 서비스의 소프트웨어를 사용 할 때 사용자의 행위 분석이 필요하다.

본 논문은 SaaS 서비스 중 Adobe 서비스를 대상으로 사용자 행위를 정의하고 탐지할 수 있는 페이로드 시그니처를 정의하였다. 제시한 방법론으로 사용자가 Adobe 서비스의 소프트웨어 사용 시 어떤 행위를 하였는지 탐지 할 수 있었다. 하지만, 페이로드 시그니처는 버전이 바뀌는 등 페이로드의 내용이 변할 수 있기 때문에 페이로드 시그니처만 사용하여 행위를 정의하는 것은 한계가 있다. 향후 연구로 사용자가 소프트웨어를 사용하면서 발생하는 플로우의 통계 정보를 바탕으로 탐지 알고리즘을 정교화 할 예정이다.

ACKNOWLEDGMENT

이 논문은 2018년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(NRF-2018R1D1A1B07045742)과 2020년도 산업통상자원부 및 한국산업기술평가관리원(KEIT) 연구비 지원에 의한 연구임 (No. 20008902, IT비용 최소화를 위한 5채널 탐지기술 기반 SaaS SW Management Platform(SMP) 개발)

참 고 문 헌

[1] 김성민, 박준상, 윤성호, 김종현, 최선호, 김명섭, "SSL/TLS 기반 암호화 트래픽의 서비스 식별 방법", 통신학회 논문지 Vol 40 No.11, Nov.2015, pp.2160-2168.

[2] 김성민, 구영훈, 김명섭, "Session ID - Server IP 캐싱 기반의 SSL/TLS 암호화 트래픽의 서비스 식별 방법", 2015년도 한국통신학회 하계종합학술발표회, 라마다호텔, 제주도, Jun. 23-25, 2015.