SNI 정보를 활용한 Office 365 사용자 행위 탐지

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

Identification of Office 365 User Behaviors using SNI Information

Jeong Woo Choi, Jee-tae Park, Min-Seong Lee, Yun-Ju Kwon
Korea Univ.

요 약

SaaS는 클라우드 기반으로 소프트웨어 제공 모델이다. 최근 많은 기업들에서 SaaS의 사용이 증가하고 있다. 기업의 효과적인 자산 관리를 위해서는 관리 부서에서 SaaS의 구매 및 사용을 관리해야 한다. 하지만 승인하지 않은 클라우드 소프트웨어를 구매하여 사용하는 Shadow IT 현상이 발생하면서 문제가 발생하고 있다. 이러한 문제를 해결하고 효율적으로 사용하기 위해서는 SaaS 사용 모니터링이 필요하다. 본 논문에서는 설치 기반 Office 365를 사용한 트래픽을 IP / Port 기반 분석 방법과 SNI 정보를 활용한 분석 방법을 사용하여 사용자의 행위를 탐지하는 방법론에 대해 제안한다.

Ⅰ. 서 론

SaaS는 공급자나 서비스 제공자가 서버 상에 애플리케이션을 호스팅하고, 고객은 웹 브로우져 등 온라인을 통해 사용한 만큼 비용을 지불하고, 소프트웨어를 서비스로 이용할 수 있도록 하는 소프트웨어 배포 모델을 의미한다[1]. 마이크로소프트의 Office 365, Adobe Creative Cloud 등이 있다. SaaS 서비스는 초기 비용이 상대적으로 적고 사용자의 필요에 따라서 사용할 수 있다는 장점으로 인해서 최근 사용이 많아지고 있다. 특히 기업에서도 많이 사용하는 추세이다. 최근 소프트웨어의 관리에 대한 새로운 방식의 필요성이 대두되면서 SaaS 애플리케이션을 모니터링하고 관리하는 방법에 대한 연구가 진행되고 있다.

모니터링을 통한 관리가 중요한 이유는 Shadow IT 때문이다. Shadow IT란 승인하지 않은 클라우드 소프트웨어를 구입하고, 이를 IT 관리부서나 책임자가 파악하지 못하는 현상을 의미한다.[2] 기업에서 SaaS 애플리케이션을 사용할 때 관리가 제대로 이루어지지 않는 경우가 발생하게 되며, 이는 기업의 손해로 이어진다. 따라서 이러한 문제를 해결하고 기업의 손해를 줄이기 위해서 SaaS 사용 모니터링의 필요성이 대두되고 있다.

트래픽 분석에 사용되는 방법론으로는 IP / Port 기반 분석 방법, 통계 정보를 활용한 분석 방법, 머신 러닝을 활용한 분석 방법, SNI 정보를 활용한 분석 방법 등이 있다. 본 논문에서는 IP / Port 기반 분석 방법과 SNI 정보를 활용한 분석 방법을 사용해서 설치기반 Office 365의 사용자 행위를 탐지하는 방법을 제안한다.

설치 기반 Office 365는 우리가 가장 많이 사용해온 SaaS 애플리케이션이며, 현재도 문서 작업이나 발표를 위해 많이 사용되는 애플리케이션이다. 따라서 본 논문에서는 설치 기반 Office 365를 사용한 트래픽을 분석하여 사용자의 행위를 탐지하여 사용자가 어떤 행위(로그인, 로그아웃, 실행 등)를 했는지에 대한 정보를 제공할 수 있는 방법을 제안하고자 한다.

본 논문의 구성은 본론에서 설치 기반 Office 365 사용자의 행위를 정의한다. 이 후, 설치 기반 Office 365 사용자의 행위를 탐지하는 방법론에 대해 언급한다. 결론에서는 해당 연구를 정리하고 향후 연구에 진행할 내용에 대해 언급하는 순서로 진행된다.

Ⅱ. 본론

본 장에서는 설치 기반 Office 365를 사용한 트래픽을 분석하여 사용자의 행위를 탐지하는 방법론에 대해 기술한다. 트래픽 분석은 SNI 정보를 활용한 분석 방법과 IP / Port 기반 분석 방법을 사용했다. 표 1은 사용자의 행위를 정의해놓은 것이다. 본 논문에서는 기본적인 사용자 행위에 대한 탐지를 목적으로 진행되었기 때문에 Onedrive 접속과 설치형 종료에 대한 탐지는 제외한다.

행위	정의
설치 기반 Office 365 실행	애플리케이션 실행
로그인 시도	ID, Password 입력
로그인 성공	로그인 시도 후 로그인 성공
Onedrive 접속	애플리케이션 실행 후 최초 Onedrive 접속
설치형 종료	애플리케이션 종료
로그아웃	시스템 애플리케이션에서 마이크로소프트 로그아웃

표1.사용자행위정의

각 행위 탐지에 대한 알고리즘의 공통적인 틀은 HTTPS의 Port 번호인 443에 해당하는 플로우들만 대상으로 SNI 정보를 확인해서 각 행위에 대한 시그니처를 정의한다. 이 후, 행위 별로 정의된 시그니처를 포함하는 플로우가 발생하면 해당 행위가 탐지되었다고 판단한다. 그림1, 그림 2, 그림 3 은 각각 설치 기반 Office 365 실행, 로그인 시도 & 로그인 성공, 로그아웃의 알고리즘을 그림으로 표현한 것이다.

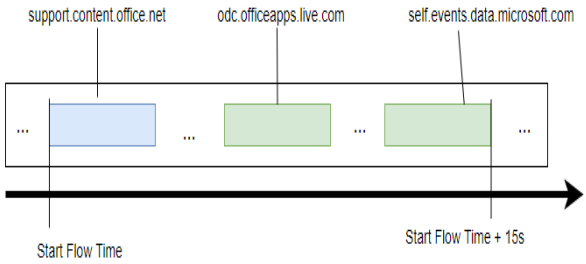

그림 1. 설치 기반 Office 365 실행 탐지

우선 설치 기반 Office 365 실행을 탐지하는 알고리즘에 대해 기술한다. 설치 기반 Office 365 실행을 탐지하는 알고리즘은 HTTPS의 Port 번호인 443 Port에 해당하는 플로우들만 고려한다. 이 후, 설치 기반 Office 365 실행 시 발생하는 공통적인 플로우의 SNI 정보를 바탕으로 정의된 시그니처로는 [support.content.office.net], [odc.officeapps.live.com], [self.events.data.microsoft.com]이 있다. [support.content.office.net]을 포함한 플로우가 발생하면 해당 시간을 저장한다. 이 후, 해당 시점으로부터 15초 이내에 동일한 Host IP에서 [odc.officeapps.live.com], [self.events.data.microsoft.com]을 포함한 플로우가 발생하게 되면 설치 기반 Offce 365 가 실행이 탐지되었다고 판단한다.

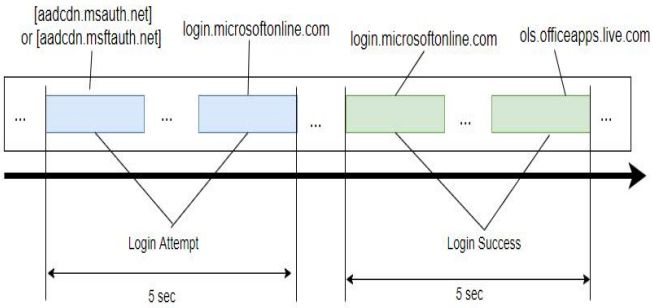

그림 2. 로그인 시도 & 로그인 성공 탐지

본 절에서는 로그인 시도와 로그인 성공을 탐지하는 알고리즘에 대해 기술한다. 로그인 시도, 로그인 성공, 로그아웃의 경우에는 백그라운드에서 작동하는 시스템 앱에서 작동한다. 로그인 과정은 로그인 시도와 로그인 성공으로 구분할 수 있다. 로그인 시도는 ID 입력과 Password를 입력하는 과정을 의미한다. 로그인 성공은 로그인 시도가 발생한 후에 로그인이 성공하는 것을 의미한다. 로그인 시도만 발생하는 경우는 로그인이 실패했다고 판단한다.

로그인 시도 와 로그인 성공을 탐지하는 알고리즘 또한 HTTPS의 Port 번호인 443 Port에 해당하는 플로우들만 고려한다. 이 후, 로그인 시도 시 발생하는 공통적인 플로우의 SNI 정보를 바탕으로 정의된 시그니처로는 [aadcdn.msauth.net], [aadcdn.msftauth.net], [login.microsoftonline.com]이 있다. [aadcdn.msauth.net] 또는 [aadcdn.msftauth.net]을 포함한 플로우가 발생하면 해당 시간을 저장한다. 이후, 해당 시점으로부터 5초 이내에 [login.microsoftonline.com]을 포함한 플로우가 발생하게 되면 로그인 시도가 탐지되었다고 판단한다.

로그인 시도 탐지 후에 로그인 성공 시 발생하는 공통적인 플로우의 SNI 정보를 바탕으로 정의된 시그니처로는 [login.microsoftonline.com], [ols.officeapps.live.com]이 있다. 두 개의 시그니처를 포함한 플로우가 발생하게 되면 로그인 성공이 탐지되었다고 판단한다.

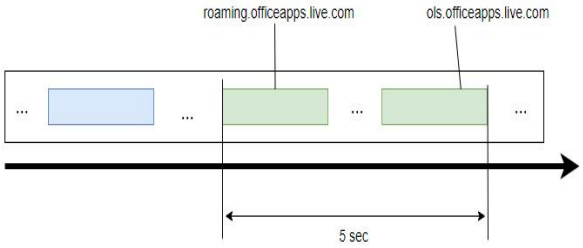

그림 3. 로그아웃 탐지

마지막으로 로그아웃을 탐지하는 알고리즘에 대해 기술한다. 로그아웃은 시스템 애플리케이션에서 마이크로소프트 로그아웃하는 것을 의미한다. 로그아웃을 탐지하는 알고리즘도 HTTPS의 Port 번호인 443 Port에 해당하는 플로우들만 고려한다. 로그아웃 시 발생하는 공통적인 플로우의 SNI 정보를 바탕으로 정의된 시그니처로는 [roaming.officeapps.live.com]이 있다. 해당 시그니처를 포함한 플로우가 발생하면 해당 시간을 저장한다. 이 후, 해당 시점으로부터 5초 이내에 [ols.officeapps.live.com]을 포함한 플로우가 발생하게 되면 로그아웃이 탐지되었다고 판단한다.

Ⅲ. 결론

본 논문에서는 SNI 정보를 활용하여 설치 기반 Office 365 사용자의 행위를 탐지하는 방법론에 대해 제안한다. 최근 많은 기업들에서 SaaS 어플리케이션의 많은 장점들 때문에 사용이 증가하는 추세이다. 하지만 기업에서는 관리되지 않고 승인되지 않은 사용이 발생하면, 이는 기업의 손실로 돌아온다. 이러한 Shadow IT 현상을 해결하기 위한 방법으로 SaaS 모니터링 기술의 필요성이 대두되고 있다.

본 논문에서는 SaaS 어플리케이션 중에서도 우리가 많이 사용하는 파워포인트, 엑셀, 워드와 같은 서비스를 제공하는 마이크로소프트사의 설치 기반 Office 365를 대상으로 트래픽 분석을 진행했다. 트래픽 분석 방법으로는 IP / Port 기반 분석 방법과 플로우의 SNI 정보를 활용하는 분석방법을 사용한다. HTTPS의 Port 번호인 443 Port에 해당하는 플로우들만 고려하여 SNI 정보를 바탕으로 시그니처를 정의해 설치 기반 Office 365 실행, 로그인 시도와 로그인 성공, 로그아웃에 대한 사용자 행위를 탐지하는 방법론에 대해 제안한다.

향후 연구로 본 논문에서 제안한 방법론을 활용해서 Onedrive 접속, 설치형 종료와 같은 추가적인 행위들에 대해서도 분석을 진행할 예정이다. 또한 Adobe Creative Cloud와 같은 다른 SaaS 애플리케이션 서비스에 대해서도 사용자 행위 탐지를 위한 트래픽 분석을 진행할 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] 김형환 외 12명, “SaaS 기술 개발 동향”, 전자통신 동향분석, 제24권, 제4호, 2008.

[2] 이민성, 박지태, 최정우, 김명섭, “페이로드 시그니처를 이용한 마이크로소프트 Office 365 서비스 탐지”, 2020년도 한국통신학회 추계종합학술발표회, Nov. 13, 2020