Headline

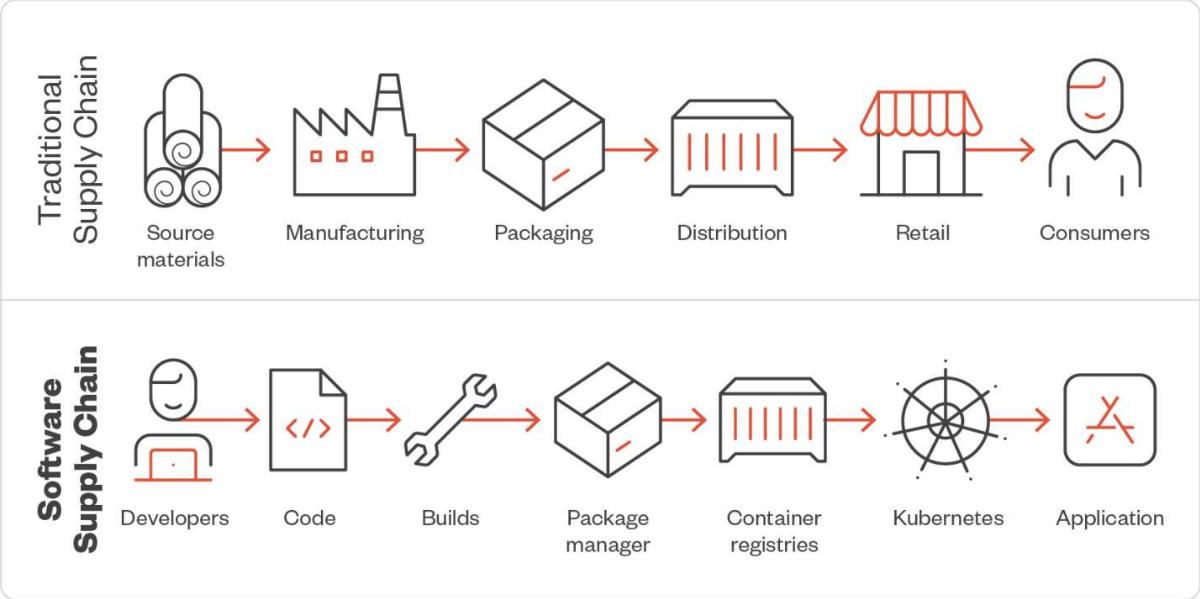
SW 공급망 보안 위협과 대응 방안

하이테크운영팀 송영식 수석

■ 개요

경쟁력 있는 소프트웨어를 개발하는 데 있어 오픈소스 활용은 자연스러운 현상이 되었다. 기존 코드와 Log4j와 같은 오픈소스 라이브러리를 사용함으로써 불필요한 재작업을 피하고, 효율적으로 개발을 진행할 수 있어서다. 이를 통해 개발 비용을 절감하는 것은 물론, 더 높은 품질의 코드를 개발하여 기술 경쟁력을 강화할 수 있다. 하지만, 이 현상을 악용하는 '소프트웨어 공급망 공격'이 최근 기업 네트워크를 침해하는 일반적인 공격으로 자리 잡으며 우려를 낳고 있다.

소프트웨어 공급망 공격은 공격자가 소프트웨어 개발 또는 배포 과정에 악의적으로 개입하여 발생하는 위협이다. 공격자는 악성 코드를 신뢰할 수 있는 소프트웨어에 삽입하여 사용자의 시스템에 침투하는 것을 목표로 한다.

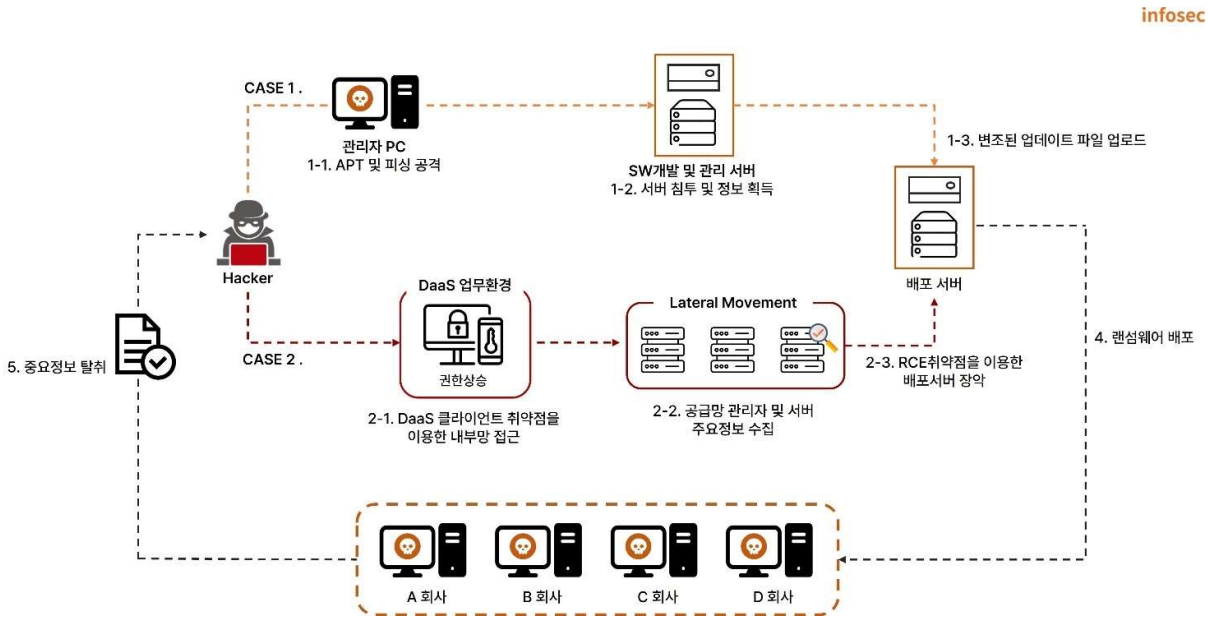


* 출처 : Trendmicro

그림 1. 일반적 공급망과 소프트웨어 공급망 구조 비교

■ 공격 유형 및 사례

공급망 공격은 단기간에 큰 피해를 초래할 수 있고, 매년 발생하는 주요 공격 중에서도 발생빈도 상위에 속하고 있다. 해커들은 일반적으로 APT(지능형 지속 공격) 및 피싱 공격을 통해 소프트웨어 공급업체를 먼저 공격한 뒤, 내부망에 있는 소프트웨어 배포 서버 파일을 변조하는 방식을 이용한다. 또한, 오픈소스/라이브러리 취약점을 발견해 이를 악용하는 등 다양한 방법으로 공급망을 공격하고 있다.



* 출처 : SK쉴더스 2022년 보안위협 전망

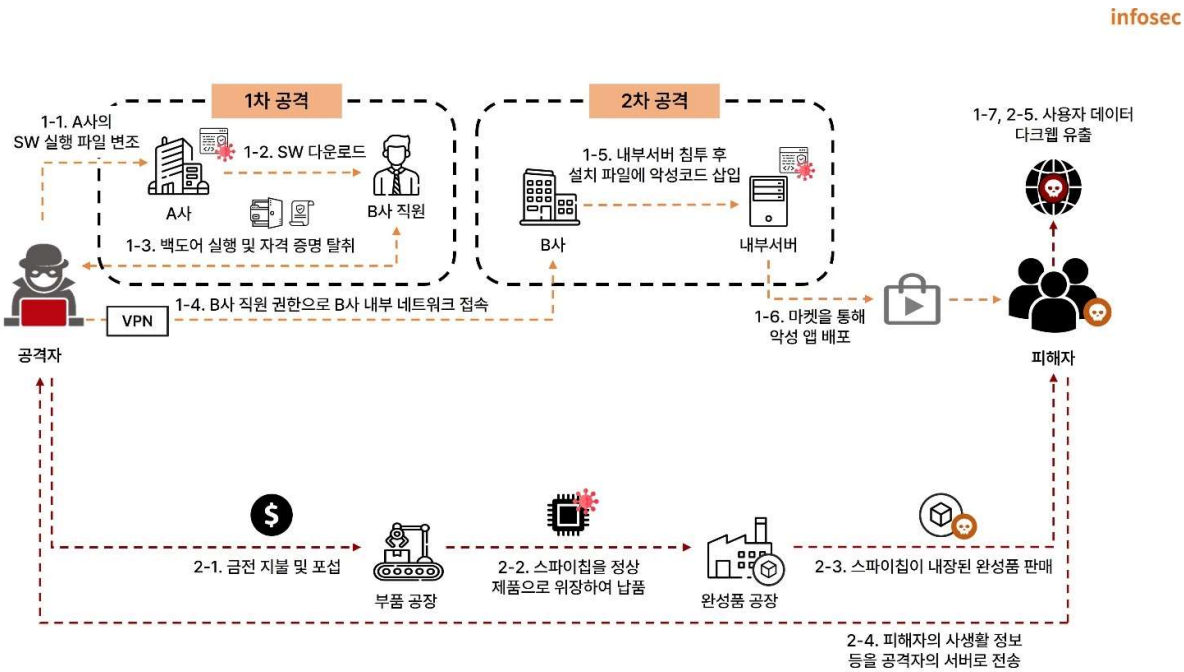
그림 2. 공급망 공격 방식

1. 소프트웨어 공급업체 공격 및 사례

공격자는 소프트웨어 개발자나 공급업체 시스템에 침투하여 제공되는 소프트웨어에 악성 코드를 삽입한다. 사용자는 신뢰할 수 있는 소스에서 소프트웨어를 다운로드한다고 생각하지만, 실제로는 감염된 소프트웨어인 것이다. 이를 통해 공격자는 공급업체의 권한을 악용하여 고객 및 파트너 조직의 데이터 탈취, 악성코드 유포 등 공격을 수행하여 랜섬웨어 감염과 정보 유출을 발생시킨다.

지난 2021 년, 사이버 범죄 그룹 REvil 은 미국 IT 관련 기업 Kaseya 를 공격하기 위해 기업의 원격 모니터링 및 관리 솔루션에 사용되는 소프트웨어의 취약점을 악용하여 공격한 바 있다. 당시 탈취한 권한으로 수백 명의 고객에게 랜섬웨어를 배포한 사례가 있다.

북한의 라자루스로 추정되는 한 해커 집단은 소프트웨어 기업 3CX 에 연쇄적인 공급망 공격을 개시했다. 단일 기업을 표적으로 삼지 않고, 해당 기업의 제품과 서비스를 사용하거나 네트워크가 연결된 기업을 목표로 삼아 공격을 확산시켰다.



* 출처 : EQST 2023 상반기 보안 트렌드 리포트

그림 3. 확정된 공급망 공격 시나리오

3CX 공급망 공격은 1차 소프트웨어(X_Trader) 공급망 공격이 2차 소프트웨어(3CX) 공급망 공격으로 이어진 사례다.

3CX 직원이 소프트웨어 제공업체 트레이딩 테크놀로지스에서 악성코드가 삽입된 X_Trader 프로그램을 내려받으면서 해당 직원의 PC가 악성코드에 감염됐다. 공격자는 3CX 직원의 PC 권한을 탈취한 뒤 자격 증명을 악용해 3CX 빌드 서버에 침투했고, 3CX S/W에 멀웨어를 삽입했다. 변조된 소프트웨어는 공식 홈페이지를 통해 설치 파일로 전 세계 각국에 배포되었다.

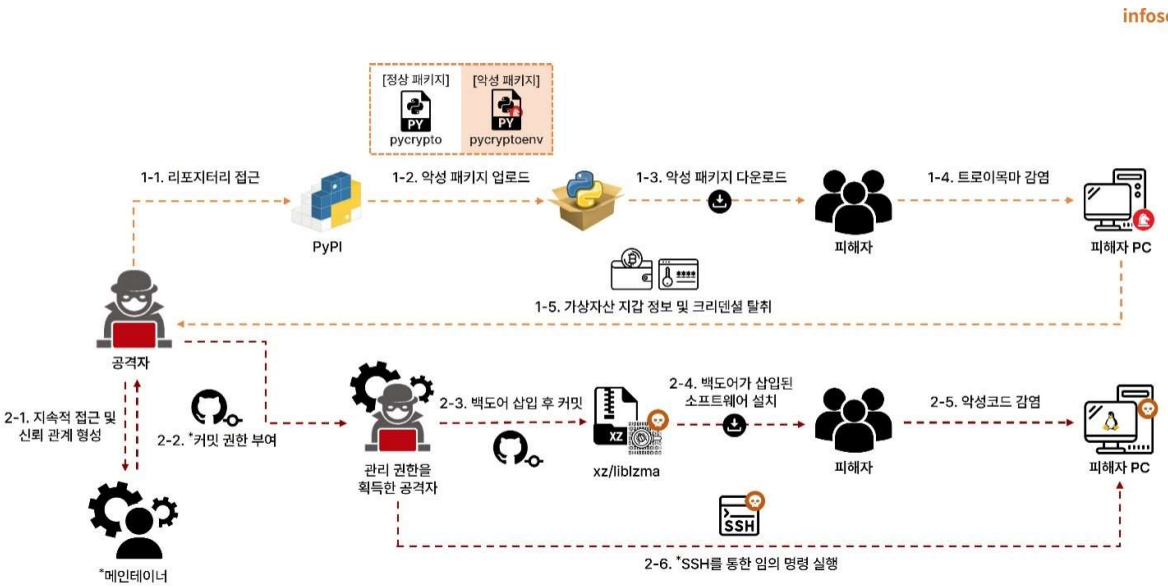
1차 공격으로 감염된 X_Trader에서 북한 해킹그룹 라자루스가 사용하는 백도어인 베일드시그널(VEILEDSIGNAL)이 발견되었으며, 2차 공격인 3CX 공급망 공격에서 고푸람(Gopuram) 멀

웨어가 발견되었다. 이를 근거로 배후에는 북한의 라자루스가 있는 것으로 추정된다.

2. 오픈소스/라이브러리 공격과 사례

최근에는 많은 기업이 소프트웨어 개발의 효율성을 극대화하기 위해 오픈소스(또는 공개적으로 접근 가능한) 코드를 자주 활용하고 있다. 하지만 해당 코드에서 취약점이 발견될 경우, 이를 사용하는 조직은 큰 위험에 노출된다. 공격자는 이미 알려진 취약점 악용 이외에도 패키지에 악성 코드를 삽입해 악성 소프트웨어(Malware)를 유포하는 방식의 공격을 시도할 수 있다.

대표적인 오픈소스 공격 사례로는 PyPI(Python Package Index) 커뮤니티를 통한 공급망 공격이 있다.



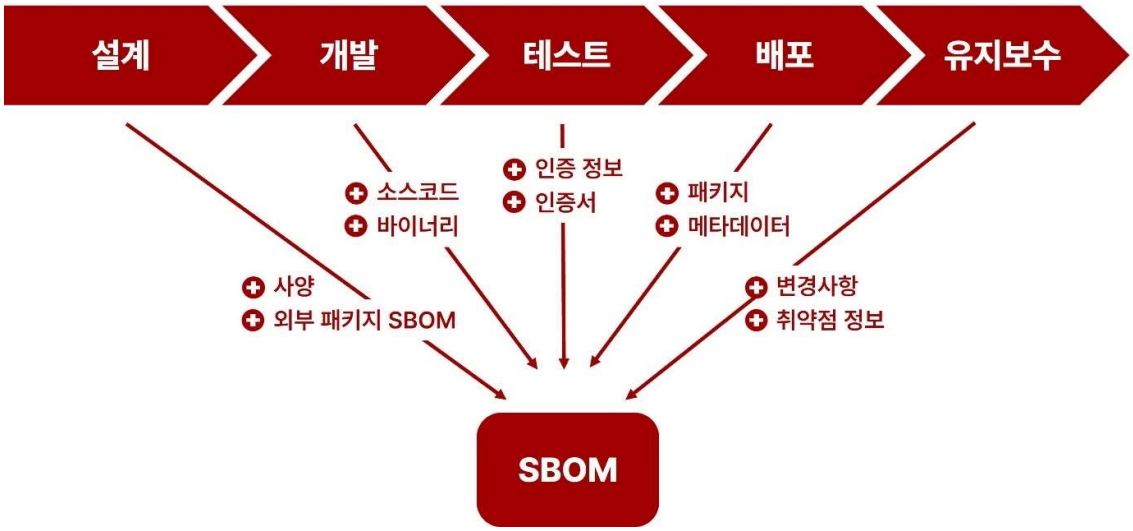
* 출처 : SK쉴더스 2024년 상반기 보안트렌드

그림 4. PyPI(Python Package Index) 커뮤니티를 통한 공급망 공격

공격자는 Python 리포지터리인 PyPI에 접근한 뒤 정상 패키지와 유사한 이름의 악성 패키지에 트로이 목마를 삽입하여 업로드한다. 악성 패키지를 내려받을 시 트로이목마가 실행되어 피해자 PC에서 가상자산 지갑 정보와 크리덴셜이 탈취된다. 타이포스쿼팅 기법을 사용하여 유명 Python 라이브러리인 'pycrypto'와 유사한 'pycryptoenv', 'pycryptoconf'를 패키지 이름으로 사용하거나, 또는 'pycryipto'와 같이 사용자 오타 실수를 이용하는 공격이다. 자세한 내용은 SK쉴더스 상반기 보안트렌드 자료를 참고하길 바란다.

이처럼 소프트웨어 기반 공격은 매우 광범위하며, 전체 공격의 66%가 공급업체 코드를 목표로 한다. 다만, 공급망 공격은 다양한 형태로 발생하기 때문에 주의가 필요하다. 예를 들어, 마이크로칩, 노트북, 사물인터넷(IoT) 장치, 운영 기술(OT) 등이 모두 손상될 수 있고, 하드웨어에 내장된 소프트웨어인 펌웨어도 공격 대상이 될 수 있다.

■ 대응 방안



* 출처 : 한국인터넷진흥원

그림 5. SBOM(Software Bill of Materials)의 체계적인 관리 방법

1. SBOM(Software Bill of Materials) 부품명세서 관리

소프트웨어 공급망 보안의 첫 번째 단계는 소프트웨어 구성 요소 파악이다. 제품의 상용 및 오픈소스 소프트웨어 컴포넌트 정보를 포함하는 소프트웨어 재료 명세서(SBOM) 관리가 중요하다. SBOM을 체계적으로 잘 관리하고 있다면 새로 발견된 취약점에 대해 즉시 확인하고 조치하는 것이 가능하다. 이에 미국, 유럽 등에서는 소프트웨어 공급망 보안 강화를 위해 SBOM 제출을 의무화했다.

2. 공급 소프트웨어 검사

외부에서 공급받은 소프트웨어 대한 검사가 필요하다. 소프트웨어가 공식 경로를 통해 제공된 것인지, 코드사인은 되어있는지 확인해야 한다. 소프트웨어 설치/업데이트 이후에는 외부 연결 시도 등 PC에서 발생하는 이상 행동을 분석해야 한다.

3. 취약점 대응 강화

공급망 공격이 발생하는 지점은 운영 중인 소프트웨어다. 대부분의 경우 공급된 소프트웨어는 개발, 테스트, 배포 과정에서 취약점이 제거되지만, 운영 과정에서 신규 취약점이 발견될 수 있다. 운영 조직은 이러한 취약점을 분석하여 실제로 어떠한 영향을 미치는지 파악한 뒤 고위험 취약점은 즉시 조치를 취해야 한다. 비교적 저위험 취약점에 대해서는 시스템 서비스 중단 등을 고려하여 적절한 대응을 해야 한다.

■ 맺음말

대부분의 소프트웨어는 버그 및 보안 문제 해결을 위한 유지관리를 목적으로 소프트웨어 공급업체의 중앙 서버를 통해 업데이트가 이뤄진다. 이러한 소프트웨어 공급망 생태계 환경에서 공격자는 공급업체의 네트워크에 침투하여 외부로 나가는 업데이트에 악성 코드를 삽입하거나 변경하는 방식을 사용한다. 이후 소프트웨어의 정상 기능에 대한 제어를 획득하고 랜섬웨어, 정보 유출 등의 공격을 이어간다.

공급망 공격의 위험성은 단일 기업 타깃을 넘어, 해당 기업 제품을 사용하거나 네트워크가 연결된 다른 기업들로 확산할 수 있기 때문에 더욱 위험하다. SK쉴더스 2024 EQST Annual Report에서는 이러한 소프트웨어 공급망 공격을 2024년 5대 사이버 위협 전망으로 제시했다. 러시아-우크라이나 전쟁에 이어 올해 이스라엘-팔레스타인 분쟁이 발발하면서 기업 및 세계 주요 인프라를 노린 새로운 공급망 공격이 지속적으로 발생할 것을 예상한 바 있다.

SK쉴더스는 오픈소스 SW 관리 체계 구축과 관련한 컨설팅을 제공하고 있다. 자세한 내용은 SK쉴더스 홈페이지나 문의하기를 통해 확인할 수 있다.