## 시나리오 제목

SW 공급망 공격 기반 ZTNA 침해사고 대응 훈련 시나리오

## 시나리오 단계

4

## 시나리오 목적

SW 공급망 공격을 통해 무력화된 ZTNA 환경에서 SBOM 기반 구성요소 변경 추적 기술과 더불어 종단 간 암호화로 패킷 분석이 제한된 조건에서의 침해사고 대응 역량을 강화한다.

## 시나리오 줄거리

**[시나리오 배경]**

주요 정보통신기반시설인 OO 기관은 정부의 「사이버 보안 강화 시범 사업」에 따라, 오픈소스인 OpenZiti를 기반으로 ZTNA(Zero Trust Network Access) 인프라를 도입하였다. 또한, 엔드포인트부터 서버, 네트워크까지 통합적인 위협 탐지 및 대응을 위해 Wazuh를 SIEM 및 EDR 솔루션으로 구축하였으며, 내부 네트워크 트래픽에 대한 심층 분석을 위해 Suricata 네트워크 침입 탐지 시스템(NIDS)를 운영 중이다. 내부에서 운용되는 중요 소프트웨어 구성요소 정보는 Dependency-Track을 통해 SBOM (Software Bill of Materials) 기반으로 체계적으로 관리되고 있다.

**[시나리오 가정]**

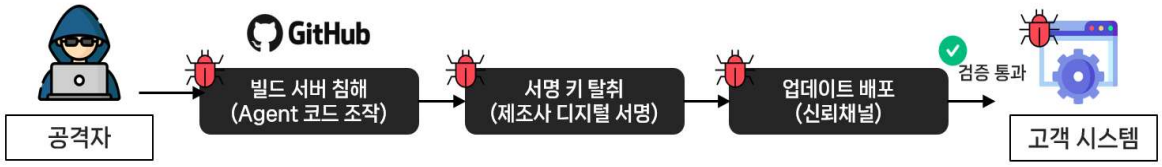
- 훈련 대상자는 ZTNA(OpenZiti), SW 공급망 보안 및 SBOM 기반 자산관리 도구(Dependency-Track), SIEM/EDR(Wazuh)의 제반 사항을 이해하고 있다.
- OO 기관의 ZTNA 정책은 사용자 편의성을 고려해 동일 계정의 최대 2개 세션 동시 연결을 허용하고 있으며, 'Admin-A' 계정은 내부 웹 서비스에 대한 접근 권한을 보유하고 있다.
- 공격자는 ZTNA 제조사의 빌드 서버와 서명 키를 장악하여 악성 업데이트를 유포하며, 이 업데이트에는 Agent의 무결성 검사 알고리즘을 조작하고, 사용자 세션 연결 정보를 탈취하여 C2(Command & Control)서버로 전송하는 백도어를 포함한다.

**[시나리오 줄거리]**

**(1. 초기 접근)** 공격자는 OO 기관이 도입한 ZTNA 솔루션 제조사의 빌드 시스템과 코드 서명 키를 모두 장악하여, 사용자의 로그인 세션 정보를 탈취하는 기능이 내재된 악성 업데이트 파일을 제작한다. 이 파일은 정상적인 디지털 서명과 해시값

을 바탕으로 공식 업데이트 채널을 통해 배포된다[그림 1].

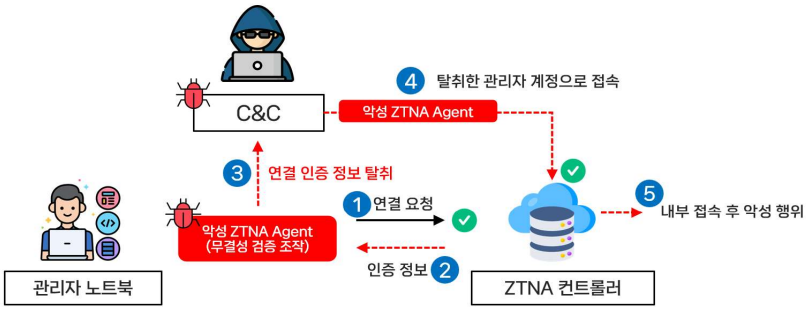
기관의 보안 담당자(이하 방어자)는 내부 규정에 따라 업데이트 파일의 무결성을 검토하지만, 이상 여부를 판단하지 못하고 업데이트를 승인한다. 이 과정에서 SBOM 관리 시스템은 구성요소 변경 알림을 생성했으나, 방어자는 해당 알림을 최근 릴리즈 노트에 명시된 기능 개선 과정의 일부로 오인하여 별도의 조치를 취하지 않는다.




[그림 1] ZTNA 제품에 대한 SW 공급망 공격 발생

**(2. 침해 발생)** 업데이트가 완료된 후, 기관의 관리자 A는 노트북을 이용해 Admin-A 계정으로 ZTNA에 원격 접속한다. 이 시점에서, 악성 ZTNA Agent는 A 계정의 로그인 세션 정보를 실시간으로 탈취하여 공격자의 C2(Command & Control) 서버로 전송한다. EDR 에이전트는 비인가된 외부 IP와의 비정상적인 통신을 감지하지만, 해당 IP가 차단 목록에 등록되어 있지 않아, 단순 비인가 네트워크 연결로만 기록된다.

동시에, 공격자는 탈취한 ZTNA Agent 세션들 중, OO 기관의 Admin-A 계정의 로그인 시도를 식별하고 즉시 해당 세션 정보를 사용하여 ZTNA에 접속한다. 이때, 공격자의 위조된 Agent는 하드웨어 정보가 관리자 A 노트북과 다름에도, ZTNA가 정상 연결로 인식하도록 한다. 이후 공격자는 Admin-A 계정의 권한으로 내부 웹 서비스에 접근하고, C2 서버에서 웹쉘(WebShell)을 다운로드하여 시스템 내부에 은밀히 설치한다[그림 2].




[그림 2] 조작된 Agent를 통한 공격자의 비인가 접근

이후 공격자는 웹쉘을 통해 ZTNA의 접근 제어 정책을 우회하고, 정찰 활동을 하는 과정에서 우연히 접근 가능한 내부 파일 서버를 식별한다. 이에 따라, 공격자는 내부 파일 서버에서 기밀문서를 유출한다. 이후에도 공격자는 지속적으로 내부 시

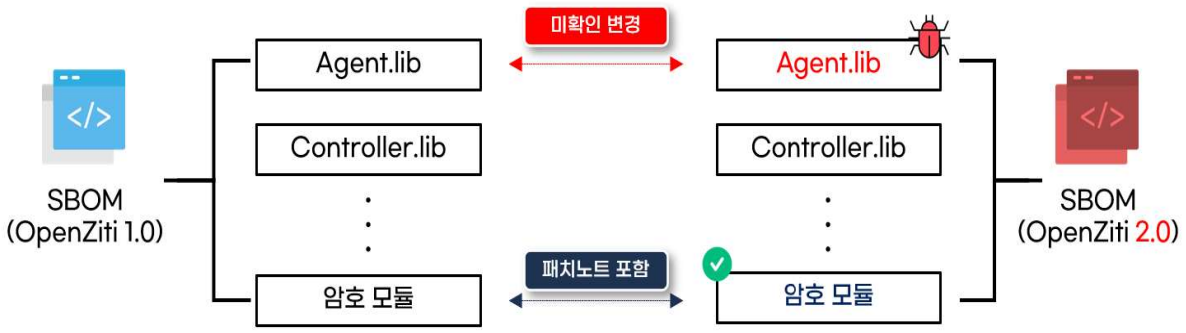
스템 탐색이나 계정 정보 수집과 같은 악성 명령어를 전송한다. 공격자는 마지막으로 자신이 시스템을 장악했음을 과시하기 위해, 웹 서비스의 메인 페이지를 변조(Deface)한다. 이에 따라, 방어자는 웹 서비스 메인 페이지의 변조(Deface) 상황과 SIEM에 기록된 악성 명령어 및 정보 유출 관련 Suricata 경보를 통해 침해 사실을 최초 인지한다.

**(3. 초기 대응 및 분석)** 방어자는 초기 로그 점검을 통해 모든 악성 행위가 Admin-A 계정으로 생성된 ZTNA 세션을 통해 수행된 것을 확인한다. 하지만 ZTNA 컨트롤러의 인증 및 세션 로그 상에서는 별다른 이상 징후가 확인되지 않는다. 다만, Suricata와 SIEM에서 지속적인 공격 시도 패킷이 포착됨에 따라, 방어자는 즉시 웹 서비스 시스템에 대해 네트워크 차단(격리) 조치를 수행한다.

이후 SIEM 로그를 중심으로 중요 장비의 로그를 분석하여 공격 타임라인을 구성한 결과, 악성 행위는 관리자 A의 노트북에서 시작된 C2 서버 IP와의 통신을 기점으로 발생했고, 해당 IP가 Suricata 악성 행위 경보의 출발지 IP와 일치함을 확인한다.

**(4. 원인 규명 및 대응)** 방어자는 관리자 A의 노트북이 본 침해사고의 최초 감염 지점임을 예상하고, 해당 기기의 EDR 로그를 심층 분석한다. 분석 결과, 해당 노트북에서 외부 C2 서버와 통신을 수행한 프로세스가 OpenZiti Agent임을 확인하였다. 또한, 이 노트북 Agent가 통신한 C2 서버의 IP가 웹쉘에 명령을 전달한 공격자의 IP와 같은 것을 확인했다. 이를 통해, 방어자는 해당 ZTNA 솔루션 자체가 악성 행위를 수행했음을 인지하고, OpenZiti에 대한 SW 공급망 공격 정황을 의심한다.

방어자는 이 가정을 검증하기 위해 CycloneDX CLI의 diff 기능을 사용하여 업데이트 전/후의 OpenZiti SBOM 구성요소 변경 이력을 분석한다. 그 결과, 제조사의 공식 릴리즈 노트에는 언급되지 않은 Agent.lib이 변경된 것을 확인한다. 이를 통해 방어자는 이번 침해사고의 근본 원인이 OpenZiti의 변조된 Agent로 인해 발생한 것을 규명한다[그림 3]. 이후 방어자는 악성 ZTNA 업데이트를 롤백하고, 내부 피해 복구 및 사이버 복원력 강화를 위한 대책을 마련한다.



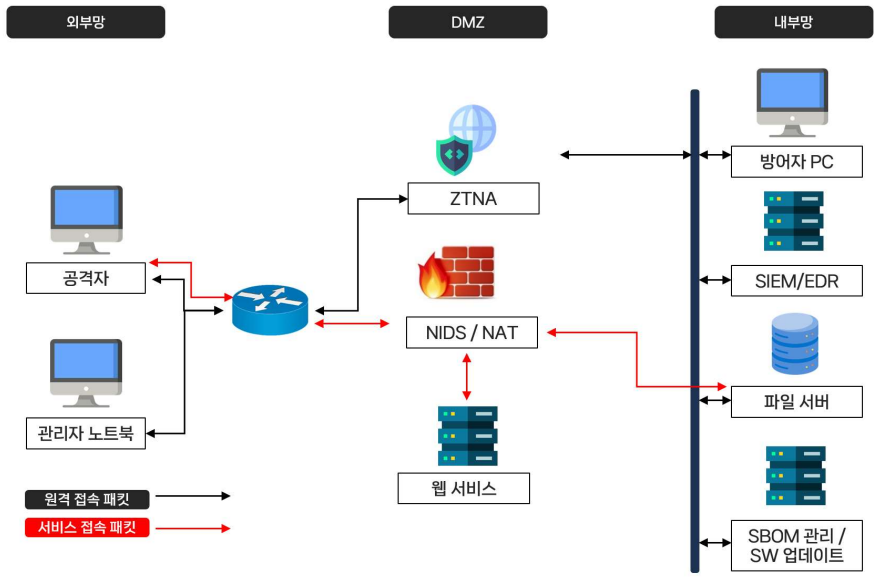

[그림 3] SBOM 비교 결과, 의심스러운 구성요소 변경 확인

[시나리오 레퍼런스]

본 시나리오는 다음과 같은 실제 공급망 공격 사례와 지침을 바탕으로 하였다.

- SolarWinds Orion 제품 공급망 공격 (2020)
- 3CX 데스크톱 앱 공급망 공격 (2023)
- SW 공급망 보안 가이드라인 1.0
- NIST SP 800-61r3 (Incident Response Recommendations and Considerations for Cybersecurity Risk Management)

## 시나리오 네트워크 구성도




| 네트워크 대역 | 구성요소 | 역할 |
|---|---|---|
| 인터넷망 | 공격자 / C2 서버 | 악성 업데이트 배포 및 공격 |
| | 원격 근무자 | 악성 ZTNA Agent 설치 대상 |
| DMZ | ZTNA 게이트웨이 / 컨트롤러 (OpenZiti) | ZTNA 인증·권한 관리 |
| | NIDA (Suricata) | 트래픽 분석 및 경보(Alert) |
| | 웹 서버 (tomcat) | 공격자의 1차 침투 목표 (웹쉘/Deface) |
| 내부망 | 파일 서버 (tomcat) | 공격자의 2차 침투 목표 (데이터 유출) |
| | SIEM/EDR 서버 (Wazuh) | 훈련자 로그 분석·이상 행위 탐지 |
| | SBOM 관리(Dependency-Track) / 업데이트 서버 | SW 변경 이력 관리, 공급망 이상 탐지 |

| | | |
|---|---|---|
| **단계 번호** | | 1 |
| **단계 명** | | 초기 접근 (Initial Access) |
| **주요 목표** | | 운영 중인 ZTNA 제품 정기 업데이트를 위해 제조사가 제공한 패치 파일의 디지털 서명과 해시값 무결성을 검증한다. |
| **유형** | **공격** | 무기화, 전달, 설치 |
| | **방어** | - |
| **주요 활동** | | [공격자]<br>① 공격자는 OO 기관이 사용하는 ZTNA 제품의 빌드 시스템에 침입해 디지털 서명 키를 탈취하고, Agent 코드에 인증 정보 수집 및 우회를 위한 백도어 삽입<br>② 조작된 Agent가 포함된 패치는 제조사 공식 디지털 서명 및 해시값과 함께 공식 업데이트 채널을 통해 배포됨<br>① OO 기관을 포함한 전 세계에 시스템에 백도어가 포함된 ZTNA가 설치되어 공격자의 비인가 통신 및 인증 우회 경로가 확보됨<br><br>[방어자]<br>① 방어자는 ZTNA 제품의 새로운 패치를 수신하여 디지털 서명과 해시값을 검증하지만, 모두 정상으로 판단됨<br>② SBOM 기반 자산관리 시스템은 제조사로부터 전달된 SBOM 정보를 통해 구성요소의 변경 알림을 발생시키지만, 방어자는 이를 정상적인 기능 개선에 따른 변경으로 오인 |
| **주요 사용 도구 및 기술** | | - 디지털 서명 검증 도구(OpenSSL)<br>- 파일 해시값 검증 도구(sha256sum)<br>- SBOM 관리 및 변경 탐지 도구(Dependency-Track, CycloneDX CLI diff)<br>- 빌드 시스템 공격 및 신뢰 채널 악용 공격 기법<br>(사전 구축된 OpenZiti ZTNA를 백도어 삽입 버전으로 변경) |
| **예상 결과물 및 상태** | | - 방어자 시스템 및 엔드포인트에 악성 ZTNA 배포<br>- 공격자는 모든 ZTNA 네트워크에 대한 접근 권한 확보<br>(C2 서버 연계 기반 후속 공격에 대한 발판 마련) |

| | | |
|---|---|---|
| **단계 번호** | | 2 |
| **단계 명** | | 침해 발생 (Incident Trigger) |
| **주요 목표** | | 공격자에 의한 웹 서비스 침해사고 발생을 인지하고, 피해 사실 파악 및 대응 방안을 수립한다. |
| **유형** | **공격** | 명령 및 제어 |
| | **방어** | 탐지 |
| **주요 활동** | | [공격자]<br>① OO 기관의 원격 근무자 A의 노트북은 ZTNA 접속을 위해 악성 Agent를 실행하며, 로그인 과정에서 생성된 ZTNA 인증 및 세션 형성 정보가 중국에 위치한 C2 서버로 전송<br>② C2 서버는 수집된 정보를 바탕으로, ZTNA Controller와의 통신에서 무결성 검사 결과를 위조하여 정상 세션처럼 내부 ZTNA 리소스에 접근<br>③ 공격자는 Admin-A 계정 권한으로 ZTNA 내부에 존재하는 웹 서비스에 접근하여, C2 서버로부터 전달된 웹쉘을 은밀한 경로에 설치<br>④ 이후 공격자는 웹쉘을 통해 ZTNA의 통제를 우회하며, 동일 네트워크 대역 내 내부 파일 서버에 접근 가능한 사실을 파악하고, 기밀문서를 외부로 유출<br>⑤ 공격 마지막 단계에서, 공격자는 웹 서비스 메인 페이지를 변조(Defacement)<br><br>[방어자]<br>① 방어자는 웹 서비스의 메인 페이지가 변조된 사실을 확인<br>② 또한 Suricata NIDS가 생성한 '심각도 높음' 경보를 SIEM을 통해 확인 |
| **주요 사용 도구 및 기술** | | - EDR/SIEM 도구 및 이벤트 로그 분석 기술 (Wazuh)<br>- NIDS 도구 및 위협 알림 분석 기술 (Suricata) |
| **예상 결과물 및 상태** | | - Admin-A 계정의 ZTNA 정상 접속 로그<br>- SIEM 내 공격 탐지로 로그 (웹쉘 명령어 및 파일 유출)<br>- 웹 페이지 변조 및 웹쉘 은닉 |

| | | |
|---|---|---|
| **단계 번호** | | 3 |
| **단계 명** | | 초기 대응 및 분석 (Initial Response & Analysis) |
| **주요 목표** | | 지속적인 침해 시도와 이상 징후 발생 상황에서 보안 경보를 기반으로 신속한 대응 조치와 로그 타임라인 분석을 수행한다. |
| **유형** | **공격** | 명령 및 제어, 목표 달성 |
| | **방어** | 분석 |
| **주요 활동** | | [공격자]<br>① 공격자는 설치한 웹쉘을 통해 C2 서버로부터 지속적인 악성 명령어 실행을 시도<br><br>[방어자]<br>① 방어자는 초기 로그 점검을 통해 모든 악성 행위가 Admin-A 계정으로 생성된 ZTNA 세션을 통해 시작되었음을 확인하지만 ZTNA Controller의 인증 및 세션 로그에는 이상 징후 없음<br>② Suricata 및 SIEM을 통해 지속적인 공격 시도 패킷이 탐지됨에 따라, 웹 서비스 시스템을 즉시 네트워크 격리<br>③ 이후 SIEM 로그를 중심으로 중요 시스템의 로그를 분석하여 공격 타임라인을 구성한 결과, Admin-A 계정이 로그인 된 시점에 통신한 C2 서버의 IP와 현재 NIDS에 탐지되는 공격자 IP가 일치하는 것을 확인<br>④ 로그 분석을 통해 공격자 IP가 웹쉘을 통해 실행한 명령어를 분석한 결과 웹쉘 은닉 경로와 내부 파일 유출 정황 확인 |
| **주요 사용 도구 및 기술** | | - EDR을 이용한 로그 검색 및 상관관계 분석<br>- 중요 조치 이행 능력 (IP 차단 또는 네트워크 격리)<br>- SIEM을 활용한 침해사고 로그 타임라인 분석 기술 |
| **예상 결과물 및 상태** | | - 웹 서비스 네트워크 격리로 인한 추가 공격 차단 상태<br>- EDR/SEIM에 기록된 공격자(C2) IP 주소 정보 확보<br>- 웹 페이지 변조 내역, 웹쉘 은닉 경로, 정보 유출 확인 |

| | | |
|---|---|---|
| **단계 번호** | | 4 |
| **단계 명** | | 원인 규명 및 대응 (Analysis & Response) |
| **주요 목표** | | 침해사고 로그와 SW 구성요소 변경 내역의 상관관계 분석을 통해 침해사고 발생의 근본적인 원인이 SW 공급망 공격임을 규명한다. |
| **유형** | **공격** | - |
| | **방어** | 대응 |
| **주요 활동** | | [공격자]<br>① 공격 대상의 네트워크 차단을 확인하고, 공격을 중지함<br><br>[방어자]<br>① 방어자는 C2 서버와 최초로 통신한 관리자 A 노트북이 감염원일 가능성을 확인하고, 해당 기기의 EDR 로그를 심층 분석<br>② 분석 결과, 해당 노트북에서 외부 C2 서버와 통신한 프로세스가 OpenZiti Agent임을 확인하였으며, 이를 통해 ZTNA 솔루션 자체가 악성 행위를 수행했음을 인지<br>③ 방어자는 최근 업데이트한 ZTNA의 업데이트에 대한 SW 공급망 공격을 의심하며, SBOM 관리 시스템의 ZTNA 구성요소 변경 알림 이력 재조사 착수<br>① CycloneDX CLI의 diff 기능을 사용해 업데이트 전후의 SBOM을 비교 분석한 결과, 제조사 패치 노트에 없는 Agent.lib 변경 사항을 확인<br>② 방어자는 이를 근거로 본 침해사고의 원인이 OpenZiti Agent.lib에 삽입된 백도어로 인한 SW 공급망 공격임을 최종 규명함 |
| **주요 사용 도구 및 기술** | | - SBOM 비교 분석 기술 (CycloneDX CLI diff) |
| **예상 결과물 및 상태** | | - 네트워크 격리 해제 및 웹 서비스 정상 구동<br>- 침해사고 분석 보고서<br>- 사이버 복원력을 위한 SW 공급망 검증 절차 강화 방안 |