Special Report

클라우드 공격 유형과 사례 분석을 통한 보안 대책 수립

최근 기업들의 클라우드 환경 전환이 매우 빠르게 진행되고 있다. 기존 전산시스템이 클라우드로 전환되면서 여러 장점이 부각되고 있지만, 반대로 보안에 대한 기업들의 고민은 여전히 해결되지 않은 상태이다. 이에 클라우드에서 발생 가능한 보안 위협과 사고 유형, 이슈 사례를 설명하고, 보안 대책에 대해 살펴보고자 한다.

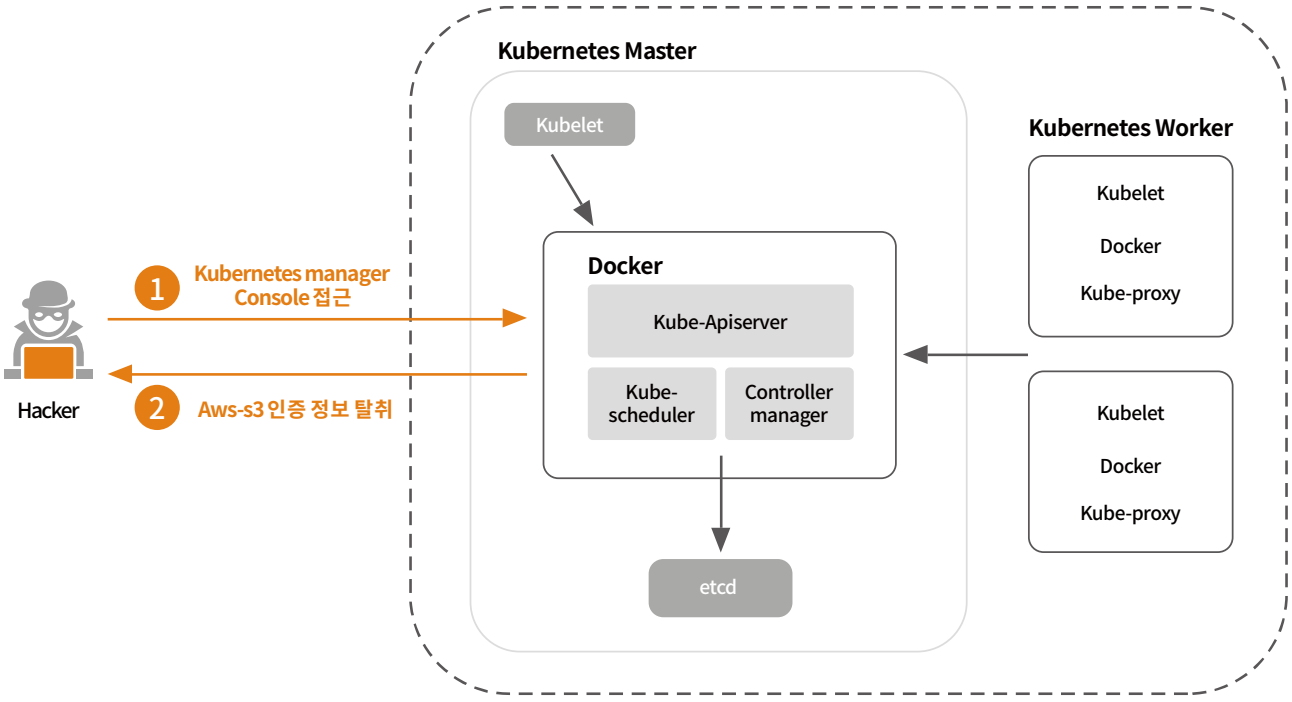
클라우드 환경에서 파생되는 위협들은 복합적이고 특수한 경우가 많아 이를 고려한 종합적인 보안 대책이 필요하다. 먼저 클라우드 환경 내에서 발생할 수 있는 보안 사고 유형을 살펴보면, 다음과 같이 크게 3가지로 나눌 수 있다.

1) 데이터 유출 : 스토리지의 설정 오류로 인한 중요 기밀 데이터 유출
2) 계정 탈취 및 손상 : 사용자/관리자의 계정 관리 문제로 인한 계정 탈취 후 시스템 오동작 유발 및 기업의 업무 방해
3) 자원 착취 및 손상 : 클라우드 인프라 및 컨테이너 취약점을 이용해 악성코드 또는 악성 이미지를 배포해 암호화폐 채굴 수단으로 클라우드 자원을 도용

이 3가지 유형들은 설정 오류와 데이터 암호화, 계정 관리 등 기본적인 보안 관리 미흡으로 인해 발생한 경우이다. 공유 자원 활용을 이용한 취약점의 경우는 클라우드 환경의 특수성을 악용한 것이라 볼 수 있다.

클라우드 보안 이슈 사례

클라우드 환경에서 실제로 발생한 보안 이슈 사례 3가지는 다음과 같다.



[kubernetes Manager Console 보안 이슈]

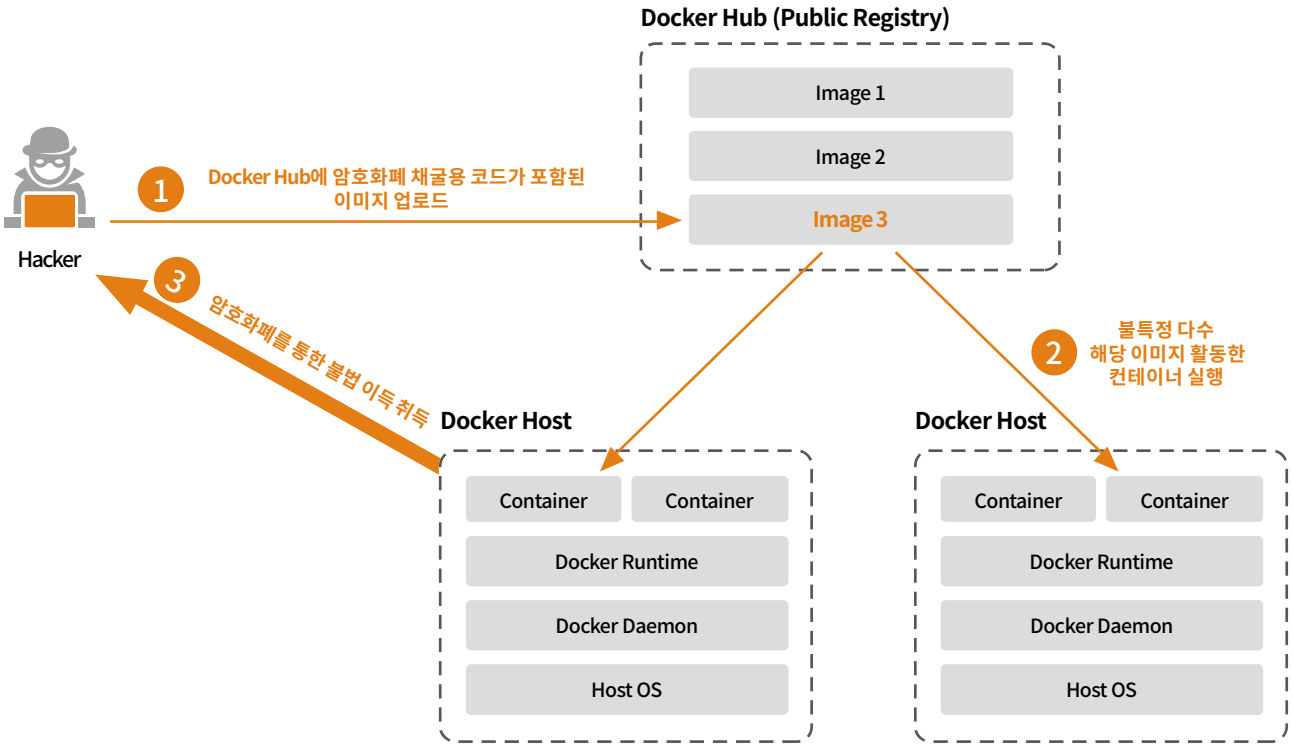
① 공격자가 Public Cloud 운영 중인 전기자동차 T社의 Kubernetes Manager Console 오픈 상태를 확인

② Kubernetes Manager Console에서 Public Cloud의 인증정보를 획득

③ Public Cloud 내 Kubernetes 인스턴스에 채굴 악성코드 설치

④ CloudFlare에 원격 서버를 통해 채굴 악성코드를 제어

⑤ 공격자는 Cloud 자원으로 암호화폐 채굴을 통해 불법 이득 취득



[Docker Hub Image 활용 보안 이슈]

① 공격자가 암호화폐 채굴 코드가 포함된 이미지 생성

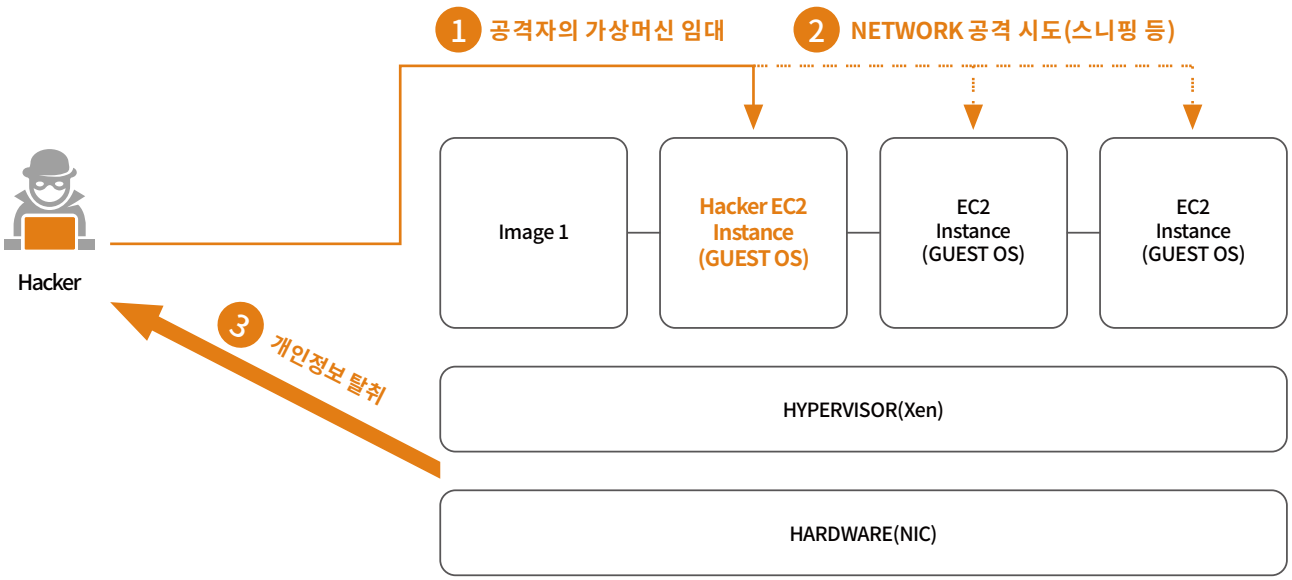
② 생성한 이미지를 Public Registry인 Docker Hub에 업로드

③ 업로드된 이미지는 1년 동안 Docker Hub에서 활성화됨

④ 다른 사용자들이 업로드된 이미지를 활용하여 컨테이너 실행

⑤ 해당 이미지를 통한 컨테이너 실행 시 암호화폐 채굴 코드가 악의적인 bash 파일을 다운로드 및 해당 파일을 통한 암호화폐 채굴 프로그램 동작

⑥ 공격자는 Cloud 자원으로 암호화폐 채굴을 통해 불법 이득 취득



[Public Cloud Network Sniffing 보안 이슈]

① 공격자는 가명을 통해 Public Cloud 가입 및 인증 서버 임대
② 임대한 가상 서버를 좀비 PC로 활용
③ PSN 네트워크에 신용카드 정보가 평문으로 전송되는 것을 확인
④ 네트워크 공격 시나리오(스니핑 등)를 구상 후 실행
⑤ 네트워크 취약점을 통해 약 7천만 건의 개인정보 탈취

지금까지 클라우드 환경에서의 보안 위협과 유형, 이슈 등을 살펴보았다. 클라우드의 보안 취약점은 기존의 인프라보다 위험이 클 수 있기 때문에 현재보다 좀 더 발전된 복합적인 예방책이 마련되어야 한다.
이에 SK인포섹은 기업들의 보안 수준 제고를 위해 클라우드 보안 가이드를 발간하고 있다. 클라우드 보안 가이드에서는 Public 클라우드와 컨테이너 보안으로 영역을 분류하고 플랫폼별로 접근제어, 인증/권한 제어, 네트워크 제어, 통신 및 데이터 암호화, 설정 제어 등을 상세히 다루고 있다. 보안 가이드를 활용해 예방책을 강구하고, 보안사고가 발생하였을 때 피해를 최소화할 방안을 미리 모색한다면, 기업별 특성에 맞는 보안 방어 체계 시스템을 확립하는 데 도움이 될 것이다.