동아일보

AI 맘대로 PC 조작… 네이버 등 ‘오픈클로’ 금지령

입력 2026.02.09. 오전 12:31

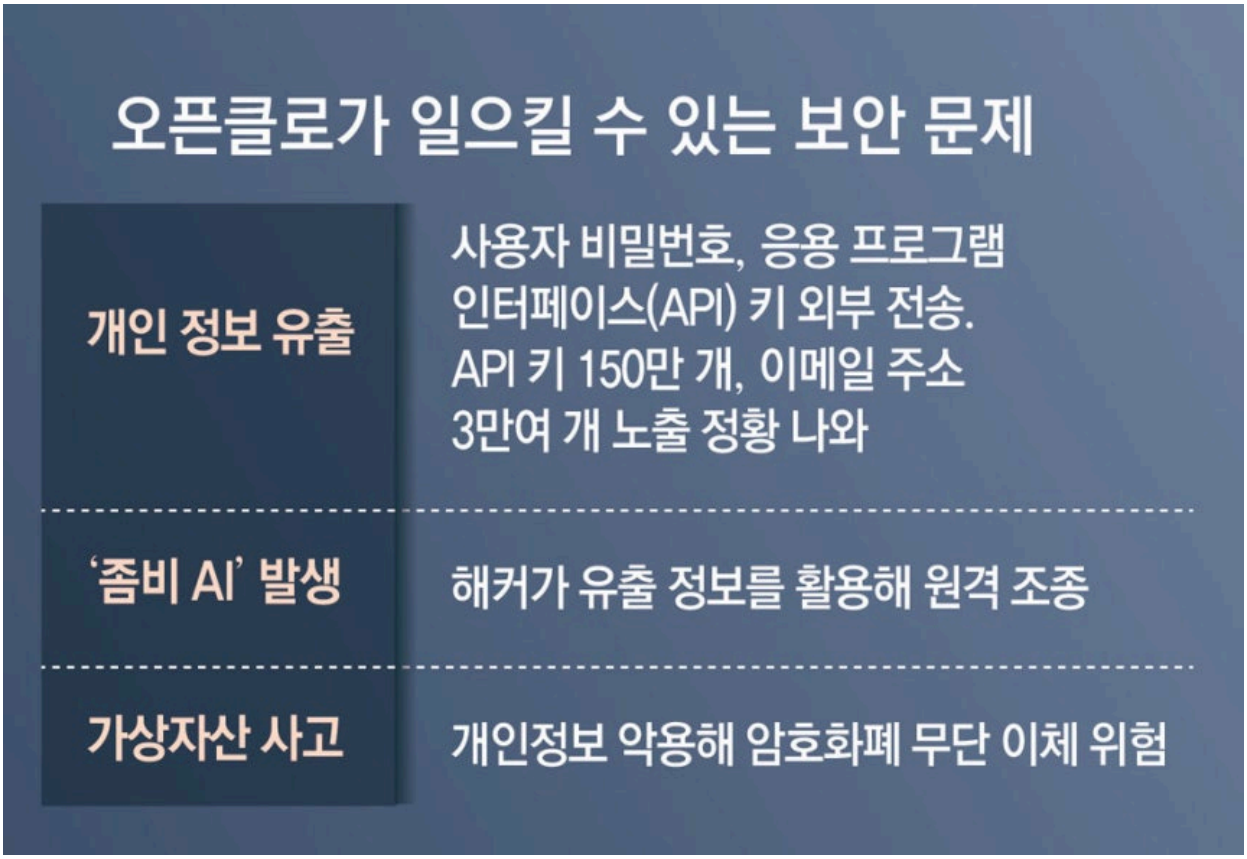
스스로 판단-결정하는 AI 에이전트
사용자 컴퓨터 광범위한 접근 가능
주요 정보 유출-악성코드 통로 위험
카카오도 업무용 기기서 사용 제한

스스로 판단하고 결정하는 인공지능(AI) 에이전트 ‘오픈클로’(옛 클로드봇·몰트봇)가 세계 개발자들의 관심을 받고 있지만 주요 테크 기업들은 오히려 ‘오픈클로 금지령’에 나섰다. 글로벌 보안 기업에서는 오픈클로가 심각한 보안 취약점을 가지고 있어 해커가 사용자의 시스템을 원격 조종하는 최악의 사태가 발생할 수도 있다는 경고가 나오고 있다.

● 네이버-카카오 “오픈클로 쓰지 마”

8일 정보기술(IT) 업계에 따르면 네이버, 카카오 등 국내 일부 IT 기업들은 내부망에서 오픈클로를 사용하지 못하도록 하는 내용의 공식 지침을 내렸다. 카카오는 개발자들을 대상으로 회사 정보 자산 보호를 위해 사내망과 업무용 기기에서 오픈클로 사용을 제한한다고 공지했다. 네이버 역시 사내에 유사한 지침을 내린 것으로 알려졌다.

국내 기업들이 보안을 우려해 특정 AI 서비스의 접근을 막은 것은 지난해 중국 AI '딥시크-R1' 이후 처음이다. 삼성전자, SK하이닉스, 한화에어로스페이스 등 안보와 직결된 기술을 취급하는 기업들은 딥시크 발표 이전부터 사내망에서 외부 AI를 사용하지 못하도록 한 상태다.



오픈클로는 사람이 일일이 지시하지 않아도 AI가 사용자의 컴퓨터 정보를 확인해 업무를 '수행'하는 AI 에이전트다. AI가 메일이나 메시지를 알아서 보내는 등 광범위한 권한을 가질 수 있어 챗GPT, 제미나이 등 기존 AI와 다르다. 최근에는 오픈클로들이 모여 이야기를 나누는 AI만의 소셜네트워크서비스(SNS) '몰트북'이 화제가 되기도 했다.

최첨단 기술이기는 하지만 사내망에서 사용 시 내부 정보에 쉽게 접근해 외부로 유출할 가능성이 높아 많은 기업들이 금지령을 내리고 있다. 이호석 SK쉴더스 이큐스트랩 팀장은 "오픈클로가 사내망을 돌아다니며 주요 정보를 유출할 수도 있고, 악성코드가 내부망에 들어오는 주요 통로가 될 위험도 높다"고 말했다.

● 통제 불가능한 재앙, 금융 사고로 이어질 수도

이미 해외에서는 오픈클로가 대규모 개인 정보를 유출하고 있다는 정황이 발견됐다. 글로벌 보안 기업 위즈는 오픈클로들이 모인 커뮤니티인 몰트북 계정 정보를 분석한 결과 대규모 개인 정보 유출 정황을 찾았다고 밝혔다. 여기엔 계정 주인의 정보에 접근할 수 있는 응용 프로그램 인터페이스(API) 키 150만 개와 3만5000여 개의 이메일 주소, 4000개 이상의 개인 메시지 등이 포함됐다.

블룸버그통신 역시 최근 한 소프트웨어 엔지니어의 사례를 소개하며, 아이폰 문자메시지 서비스 '아이메시지'의 접근 권한을 얻은 오픈클로가 저장된 연락처에 500여 개의 메시지를 무단으로 발송했다고 보도했다. 만약 접근 권한이 넓은 오픈클로 계정을 해커가 탈취할 경우 사용자의 시스템을 원격 조종하거나 암호화폐 거래를 진행하는 등 금융 사고로 이어질 수도 있다.

업계에서는 AI의 도움을 받아 개발된 오픈클로가 보안 관점에서는 '폭탄'과 다름없다는 우려가 적지 않다. AI의 위험도를 측정하는 3대 요소인 △개인 정보에 접근 가능한가 △외부와 소통할 수 있는가 △신뢰할 수 없는 콘텐츠에 노출될 수 있는가 등에 오픈클로가 모두 해당된다는 것이다. 오픈AI의 창립 멤버인 안드레이 카르파티는 오픈클로에 대해 "사생활과 데이터를 모두 심각한 위험에 빠뜨리는 현 상황은 '(무법지대와 다름없는)서부 개척 시대' 같다"고 우려했다.

최지원 기자 jwchoi@donga.com

이 기사 주소 https://n.news.naver.com/mnews/article/020/0003695890