NETWORK TIMES

The United States federal civil service had to avoid spreading hacking to……
11/16

Insight News

AI 보안 기술, 美 연방공무원 해킹 피해 확산 방지

사일런스 '사일런스프로텍트' 주목 … 완벽한 방어 위해 AI 이용해야

지난해 4월 미국 연방인사관리처에 해킹으로 인해 2150만명이라는 엄청난 수의 공무원 신상정보가 유출되는 사고가 발생한 바 있다. 미국 정부는 사고 초기에 420만명에 달하는 연방공무원들이 해킹 피해를 입었다고 발표했지만 몇 개월이 지난 후 9배 정도의 피해자가 생겨났다는 공식 발표를 하면서 문제의 심각성이 증폭되기도 했다.

아직까지도 이 사고의 범인이 누구인지 정확히 파악되지 않는 상황이지만 미국 정부는 중국 해커들의 소행으로 추정하고 있다. 그들은 연방인사관리처 네트워크의 최고 운영자 인증을 위조해 최고 관리자 권한을 획보한 후 해킹을 감행할 수 있었던 것으로 알려졌다.

▲ 스튜어트 맥클루어 사일런스 CEO는 "완벽한 방어를 위해서는 AI를 이용할 수밖에 없다"고 강조했다.

사일런스프로텍트, 중요 역할 수행

이와 관련해 지난 9월 미국 하원 정부개혁위원회(The House Committee on Oversight and Government Reform)와 제이슨 샤페츠(Jason Chaffetz) 위원회 회장은 공동으로 보고서 발표를 통해 이번 사고에서 AI 기술을 활용한 보안 솔루션이 더 큰 피해 확산을 저지한 중요한 역할을 담당했다고 밝혔다.

이 보고서에는 중국에서 활동하는 것으로 추정되는 쉘크루(Shell Crew)나 데퓨티 독(Deputy Dog) 해킹 팀의 소행으로 보이는 APT가 탐지됐다고 기술돼 있다. 연방인사관리처에서 해킹 발견 후 즉시 중단시키기 위해 AI 기술 기반으로 동작하는 사일런스의 '사일런스프로텍트(CylancePROTECT)'가 처음으로 사용됐으며, 이 솔루션이 더 이상의 피해자 확산 방지를 위해 중요한 역할을 수행했다.

미국 연방정부 컴퓨터 비상대응팀(US-CERT)은 지난해 4월 24일 보고서를 통해 인사처가 4월 16일 네트워크에서 의심스러운 활동을 발견했다는 내용을 보고했다. 다음날 연방인사관리처의 제프 와그너(Jeff Wagner) 보안 운영 책임자는 당시 미국 인사처의 도나 세이모어(Dona Seymour) CIO에게 보낸 이메일에서 "사일런스의 보안 솔루션으로 현재 공격이 진행 중인 악성코드를 발견했다. 사일런스프로텍트는 인사처 네트워크가 공격을 받았다는 것을 인지한 후 처음으로 사용한 툴이었고, 그 툴을 통해 악성코드를 즉각 발견, 인사처 전체를 보호하는 작업에 착수했다"고 말했다.

사일런스 고유 방법으로 해킹 발견

또한 보고서에는 사일런스가 다른 툴이 찾아내지 못한 공격을 발견해 낼 수 있었던 이유에 대해 독특한 AI 방식을 통해 보안이 구현되기 때문이며 일반적인 표준 지표 시그니처가 아니라 사일런스 고유의 방법으로 해킹을 찾아낼 수 있었다고 보고했다.

사고 당시 인사관리처 네트워크에는 어떤 솔루션도 공격을 탐지하지 못했던 것으로 나타났다. 인사관리처는 이전에 사일런스의 V라는 스캐닝 툴을 사용하고 있었지만 opmsecurity.org라는 도메인으로 가는 수상한 트래픽을 발견한 이후 곧바로 사일런스프로텍트를 도입했다.

스튜어트 맥클루어 사일런스 CEO는 "인사처의 정보유출과 같은 비슷한 형태의 셀 수 없이 많은 정보유출 사고 발생으로 인해 해커, 국가 활동세력, 조직적 범죄집단, 사이버 테러리스트 등과 맞서 싸우기 위한 노력이 이어지고 있다"며 "완벽한 방어를 위해서는 AI를 이용할 수밖에 없다. 사일런스의 임무는 이 세상의 모든 사람을 보호하는 것이고, 이제 단지 그 일을 시작했을 뿐이다"고 밝혔다. 〈정용달 기자〉