

AI의 정보보호산업 활용 최신 현황

-AI 활용으로 정보보호체계 강화에 기여-

AI(인공지능)는 시간 또는 위치 등에 대한 환경적 제약에서 자유로워 낮은 비용으로 빠르게 정해진 작업을 수행할 수 있는데, 정보보호분야도 중요한 역할을 할 것으로 기대되고 있습니다. 이번 뉴스레터에서는 정보보호 영역에서 AI의 기술적 활용 현황을 살펴보면서 AI의 정보보호산업분야의 순기능과 역기능 등 최신 활용 현황을 살펴 보겠습니다.

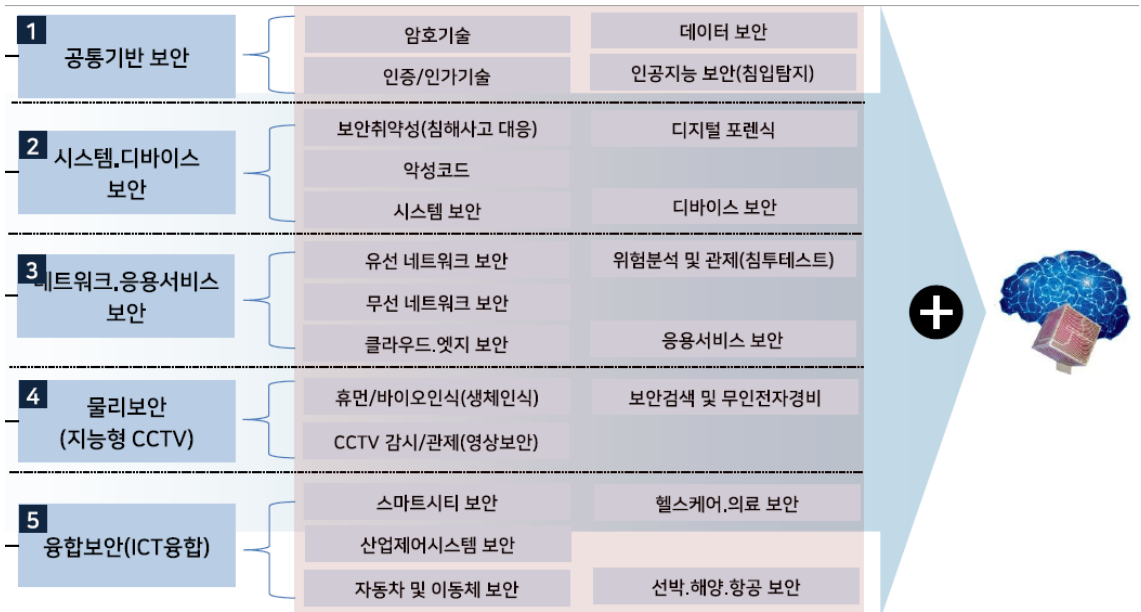
1. AI와 정보보호

AI는 최근 IT 환경의 변화로 인해 강력하고 저렴한 하드웨어, AI 알고리즘의 개선 그리고 대량의 데이터를 이용하여 비약적인 발전을 이루게 되었습니다.

2016년 해커 올림픽이라 불리는 세계 최대 해킹방어대회인 '데프콘(DEFCON) 2016' 본선에 카네기멜론대학 연구팀에서 만든 완전 자동화 AI 컴퓨터인 메이헴(Mayhem)이 경연자로 참가하여 세계 최고 해커들과 경쟁을 펼쳐, 취약점을 보완하고 수정하는 패치(Patch) 능력 등에서 매우 높은 수준을 보여 경연 참가자들을 놀라게 하였습니다. 이후 정보보호 분야에서도 AI는 비약적인 발전을 거듭하고 있습니다.

2. (순기능) AI 정보보호 산업분야 활용 현황

정보보호분야에서는 나날이 지능화, 정교화, 대규모화 되고 있는 사이버 공격에 대하여 기존 방식의 대응은 방어 대상이 되는 방대한 데이터와 숙련된 전문가 부족 문제 등으로 한계에 이르게 되었으며 이는 곧 AI 도입을 앞당기는 계기가 되었습니다. AI는 기존 5대 전통적인 보안기술 영역에 적용될 수 있으며 탐지/대응을 고도화하고 자동화하는 형태로 발전하고 있습니다.



[그림1] AI 보안기술분류 체계 (출처: KISA한국인터넷진흥원)

위와 같이 시가 정보보호 분야에 적용되는 영역은 크게 위협(이상) 탐지 및 분석, 악성코드 분석, 취약점 분석 및 모의해킹으로 구분할 수 있습니다.

가. 위협(이상) 탐지 및 분석

위협(이상) 탐지 및 분석은 통합보안관제와 패킷분석, 사용자 행위 및 사기 탐지로 나눌 수 있습니다. 이중 통합보안관제분야에서 가장 활발히 적용되고 있습니다. 통합보안관제 분야에서는 경계보안장비로 구분되는 방화벽, 웹로그, 침입방지장비, 웹 방화벽 등의 장비에서 수집되는 로그/이벤트를 SIEM으로 수집하여 보안관제 대상으로 발생하는 행위를 AI를 활용하여, 알려진 공격 패턴과 유사한 공격은 실시간으로 판단하고, 상관분석에서 발견하지 못하는 이상행위는 통계적인 기법을 활용하여 식별하도록 발전하고 있습니다. 해외에서는 IBM이 133개 국가의 2만 개 이상 기기에서 매일 200억 건 이상 발생하는 이벤트를 실시간으로 감시하고 위협을 탐지하는 보안 솔루션인 "X포스"를 운영 중이며, 국내에서는 이글루코퍼레이션의 SIEM(Security Information Event Management)인 SpiderTM과 함께 Spider AI제품을 선보였으며 보안관제 노하우를 반영한 표준 데이터셋과 적용 대상 기업의 데이터를 활용하여 위협 탐지 성능을 제고하고 있습니다.

패킷 분석은 컴퓨터 네트워크 통신 내용을 분석하여 인가되지 않은 사용자가 정보자원에 불법으로 접근하거나, 정보자원을 고갈시키는 행위를 식별하는 것으로, 정상상태를 학습하여 다양한 머신러닝 알고리즘을 적용하여 학습된 지식을 기반으로 실시간으로 생성되는 패킷들에 대해 정상 및 비정상 여부를 판단할 수 있습니다.

사용자 행위 및 사기 탐지는 광범위한 IT, 보안 인프라에 대한 분석과 비즈니스 혹은 사용자 활동 패턴을 기반으로 해킹 피해, 정보유출을 모니터링 하거나 전자금융사기 탐지를 위한 FDS(Fraud Detective System)로 비정상거래의 거래 특성을 기반으로 이상 패턴을 인지하여 거래를 차단하거나 추가로 본인확인 후 거래할 수 있도록 프로세스를 변경하는 데 활용되고 있습니다.

나. 악성코드 분석

악성코드 분석은 패턴/시그니처(Signature)를 실시간 업데이트해야 하는 제한점과 알려진 악성코드의 유입 및 감염을 차단하는 수준에서 벗어나 반복적으로 발생하는 이상 행위를 실시간으로 추적하거나 악성코드내 Opcode와 문자열들을 추출하여 악성여부를 신속하게 판별하여 대응할 수 있는 인텔리전스 보안 솔루션으로 발전하고 있습니다.

다. 취약점 분석 및 모의해킹

취약점 분석 및 모의해킹은 다양한 애플리케이션 소스코드에 대한 취약점 분석, 소프트웨어 구성요소 분석을 통해 소프트웨어 개발 전 과정의 보안 취약점을 진단하는 기술과 더불어 앞서 언급했던 메이헴과 같은 AI 슈퍼컴퓨터를 활용하여 목표 시스템의 취약점을 스스로 발견하고 공격코드 작성 및 수정보완조치를 모두 수행하는데 활용될 수 있습니다.

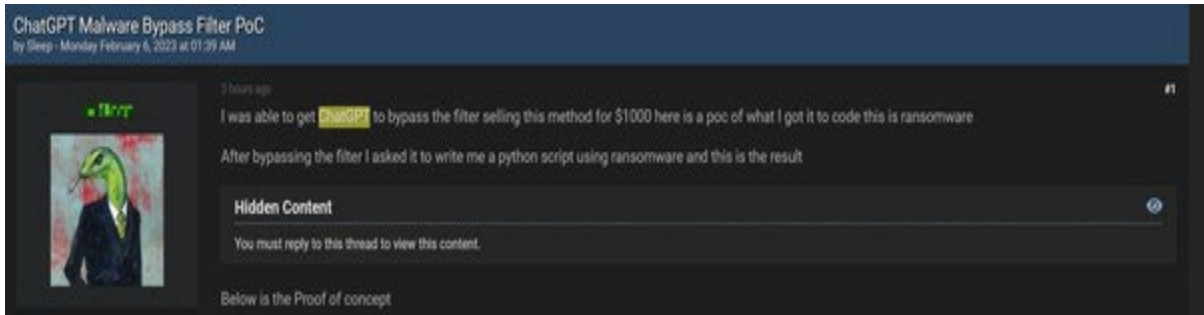
라. 기타 활용 방안

앞서 설명드린 이상탐지, 악성코드분석, 취약점 분석 이외에도 개인정보 파기, 관리나 정보유출 탐지를 위한 다양한 솔루션이 개발되고 있습니다.

분류	기능
파기	PC내 개인정보를 관리하기 위하여 검출/삭제 등 중앙집중식 솔루션
관리	SSL/TLS의 가시성을 확보하고 첨부파일내 개인정보 패턴 및 이상징후 분석
관리	개인정보의 주요 이동경로를 모니터링하여 개인정보 유출 행위를 원천 차단
분석/활용	PC내 개인정보를 실시간으로 검출하고 암호화로 보호하는 솔루션
관리	PC내 개인정보를 실시간으로 검출하고 암호화로 보호하는 솔루션
분석/활용	AI 기술을 활용하여 개인정보가 존재하는 모든 시스템의 데이터를 통합하여 분석하고 평가하여 컴플라이언스 위반에 대한 알림 기능
분석/활용	여러 디바이스에서 발생하는 메시지의 흐름을 시나리오화 하고 분석

3. (역기능) ChatGPT 를 활용한 손쉬운 해킹공격

정보보호 전문가인 세르게이 샤이케비치(Sergey Shykevich)는 "챗GPT와 같은 챗봇은 사람의 말을 듣고(혹은읽고) 반응하는 기술이기 때문에 '코드를 짜라'는 명령만 인간의 언어로 내릴 줄 알면 소프트웨어를 완성할 수 있게 된다"고 설명하고 있습니다. 즉, 악성코드 제작의 난이도를 챗봇들이 크게 낮춰서 해킹공격의 기술적 난이도를 한층 수월하게 해주는 역기능이 있게 되는 것입니다. 한 해커는 챗GPT를 사용해 실크 로드 및 알파베이와 같은 다크 웹 시장의 코드업 기능을 만드는 방법을 공유했습니다. 다른 해커는 파일을 암호화할 수 있는 파이썬 코드를 공유했으며 챗GPT가 파일을 만드는 데 도움이 됐다고 말하고 있습니다.



[그림2] 다크웹에서 챗GPT 기반으로 랜섬웨어 코드 작성 방안을 연구했다는 공격자 (출처 : 다크웹)

이러한 코드는 완전히 무해한 목적으로 사용될 수 있지만 랜섬웨어가 작동하는 방식과 유사하게 누군가의 시스템을 완전히 암호화하도록 쉽게 수정할 수 있는 해킹을 보다 손쉽게 해주는 역기능인 것입니다. 또한 챗GPT를 사용해 사용자가 정보를 공유하도록 속이고 고도로 표적화된 사기 및 피싱 캠페인을 시작하는 봇 및 사이트를 구축할 수도 있습니다. 그러한 가운데 최근에 다크웹에서는 챗GPT 기반의 악성코드와 랜섬웨어가 등장하였는데, "챗GPT가 1000달러에 판매되는 필터를 우회하도록 할 수 있었다"며 "필터를 우회한 후 랜섬웨어를 사용해 파이썬 스크립트를 작성해달라고 요청했고 이것이 결과"라며 사진을 공유하는 등 생성형 AI가 정보보호측면에서 어려운 해킹기술에 대한 손쉬운 접근이 가능하게 하는 역기능을 다시 한번 확인할 수 있습니다.

4. 시사점

IBM은 2025년에는 AI 시장이 2,000조 원 규모에 이를 것 이라고 예측하고 있고, UN미래보고서에서는 30년 내에 AI가 인간의 지능을 능가할 것이라는 전망을 내놓고 있습니다. 이렇듯 사회 전반적으로 AI 적용이 활성화되고 있고 정보보호 분야에서도 예외가 아닙니다. 현재 AI의 기술 성숙도, 구현에 필요한 시간과 전문 자원의 부족, 경영진의 의지와 예산 부족 등은 반드시 해결해야 할 부분이며 개인정보 침해, AI 알고리즘에 대한 과도한 신뢰, 알고리즘 한계에 대한 이해 부족, 특정 부분에서 잘못된 알고리즘 적용, 데이터 보호 제한 등도 고려해야 할 부분이라 볼 수 있습니다.

AI 기술은 정보보호산업에서 순기능과 역기능을 동시에 제공하는 기술적 특징을 가지고 있습니다. 인공지능의 기본적인 주요기능 즉 의사결정과정에서 보다 더 신속하고 정확하게 인간을 도와서 업무효율성을 높이는 순기능이 정보보호산업 분야에서는 앞으로도 광범위하게 적용될 것입니다. 그러나 동시에 해킹기술을 손쉽게 학습하고 악성코드를 제작할 수 있는 역기능은 기술적 법률 제도적으로 강력하게 대응해야 할 항목일 것 입니다.

AI는 자동차, 국방, SW, 바이오, 항공, 우주산업까지 거의 모든 분야에서 4차 산업혁명을 가속화 시키는 중심기술입니다. 보다 더 효과적인 해킹탐지와 정보보호를 위하여 더욱더 AI인공지능의 활용과 R&D 투자 확대 및 기술개발이 필요하고, 랜섬웨어 같은 기업에 치명적인 피해를 입히는 악성코드 제작 등이 매우 쉬워지기 때문에 각 기업에서는 기존보다 더욱 강화된 정보보호 기술과 법률적 대응이 필요할 것입니다.

화우 정보보호센터는 오랜 경험과 축적된 노하우를 기반으로 기업 고객을 위한 최적의 솔루션을 제공하고 있습니다. 정보보호 관련 법령의 해석 및 그 대응과 정보보호 기술적 자문(해킹 진단, 보안취약점) 등 포괄적인 올인원(All-in-One) 서비스를 제공하고 있습니다. 관련하여 문의사항이 있으신 경우 언제든지 화우에 연락하여 주시기 바랍니다.

Contacts

이근우

파트너변호사

T. (+82) 2 6003 7558

E. klee@yoonyang.com

석제범

고문

T. (+82) 2 6182 8147

E. jbseok@yoonyang.com

이광욱

파트너변호사

T. (+82) 2 6003 7535

E. kwlee@yoonyang.com

이수경

파트너변호사

T. (+82) 2 6182 8132

E. sgyi@yoonyang.com

백재환

전문위원

T. (+82) 2 6182 8366

E. jhb@yoonyang.com

지재원

연구위원

T. (+82) 2 6003 7568

E. jwji@yoonyang.com