EQST insight

딥페이크 기술을 악용한 보안 위협 증가

최근 딥페이크를 이용한 사회공학적 공격(Social Engineering Attack)[1]이 증가하는 추세다. 딥페이크는 딥러닝(Deep learning) [2]과 가짜(fake)의 합성어이며, 딥러닝을 기반으로 실제 같은 가상 정보를 만들어낼 수 있는 기술이다. 공격자들은 이러한 딥페이크를 이용하여 사회공학적 공격을 더 정교하게 발전시키고 있어 관심과 주의가 필요하다.

현재 다양한 딥러닝 오픈소스가 인터넷상에 공개되어 누구나 딥페이크 기술을 이용할 수 있는 상태이며, 다크웹에서도 사회공학적 공격을 위한 딥페이크 도구가 활발하게 공유되고 있는 상황이다. 딥페이크는 인공지능(AI) 기술이 발전할수록 더 정교해지고 현실적인 결과물을 만들어내기 때문에 이를 이용한 보안 위협은 앞으로도 증가할 전망이다. 이번 헤드라인에서는 딥페이크 기술 악용으로 인해 발생할 수 있는 보안 위협에 대해 알아보고자 한다.

[1] 사람의 심리와 관련된 보안 취약점을 타깃으로 하는 공격 기법

[2] 머신러닝의 한 종류로, 컴퓨터가 대규모 데이터에서 중요한 패턴을 스스로 학습하는 모델

BEC(Business Email Compromise) 공격

최근 크립토윈터(Crypto Winter)[3]와 가상자산 관련 규제 강화로 랜섬웨어 공격 조직의 수익이 감소하고 자금 세탁에 어려움을 겪고 있는 상황이다. 이에 랜섬웨어 공격 조직들은 랜섬웨어에 제한되지 않은 다른 방식의 공격 기법을 병행하려는 움직임을 보이고 있다.

랜섬웨어 공격 조직의 다음 공격 수단으로 전망되는 공격은 BEC(Business Email Compromise)다. BEC는 비즈니스 이메일, 업무 전화, 화상회의에서 특정 대상을 사칭하여 금전을 탈취하는 사회공학적 공격이다. 예를 들어 특정 기업의 주요 거래처 직원을 사칭하여 전화나 이메일로 거래 계좌가 변경되었다며 속이고 거래대금을 가로채는 것이다.

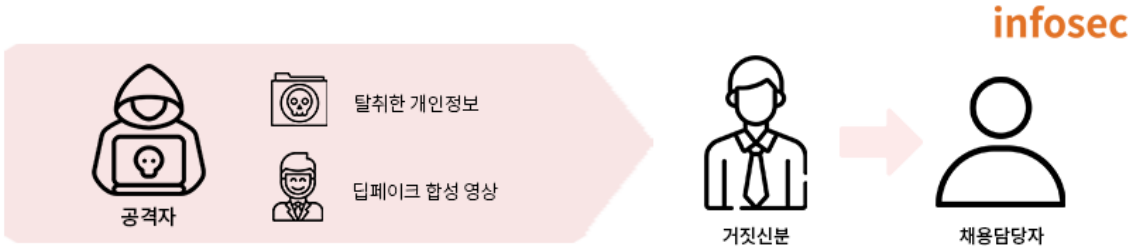
BEC공격 역시 사회공학적 공격이기 때문에 딥페이크 기술을 적극적으로 활용하고 있다. 대상을 속이기 위한 이미지, 영상, 음성에 딥페이크가 사용되면 피해자는 사칭 여부를 판별하기가 매우 어려워진다.

올해 2월 미국 FBI는 최근 들어 화상회의 플랫폼에서 CEO를 사칭하고 자금 이체를 요청하는 방식의 BEC 공격이 증가하고 있다고 경고했다. 공격자는 사전에 SNS, 영상, 오디오 등에서 데이터를 수집하여 딥러닝 인공지능을 통해 대상의 목소리를 학습하고, 위조된 이메일로 기업 화상회의에 참여하여 자금 이체를 지시하는 식으로 금전적 이득을 취했다.

BEC는 기술적 취약점이 아닌 사람의 심리를 속이는 사회공학적 공격이기 때문에 내부 직원의 보안 교육 외에는 명확한 방어책이 없다. 보안 교육과 함께 사회공학적 공격에 대한 사기 범죄에 대응 훈련을 병행하고, 이메일과 전화로 받는 요청을 이중으로 확인하는 프로세스를 만들어야 BEC로 인한 피해를 최소화할 수 있다.

[3] 가상자산 시장 침체기, 자금이 빠져나가며 거래량이 장기간 저조해지는 현상

온라인 취업 사기

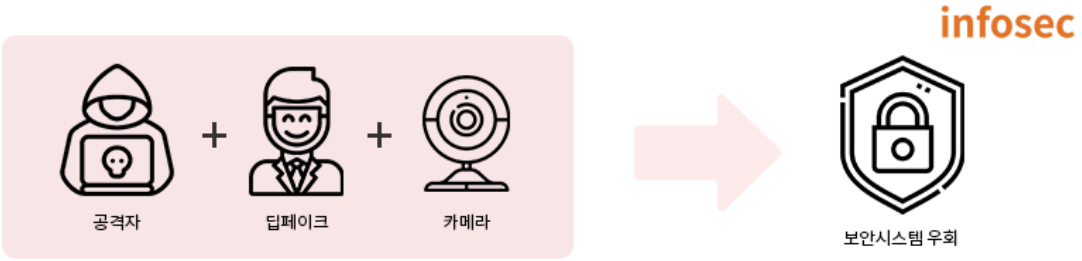


최근 미국에서는 딥페이크가 온라인 취업 사기에 악용되어 이슈가 되고 있다. 딥페이크 기술을 이용하면 타인의 얼굴이나 음성을 영상에 실시간으로 합성할 수 있기 때문에 공격자는 온라인 면접에서 위장된 신분으로 채용 담당자를 속일 수 있다.

실제로 북한의 IT 인력들이 온라인 면접에서 딥페이크를 사용하여 거짓 신분으로 미국 기업과 기관에 취업을 시도하다 적발된 사례가 있다. 이에 FBI는 해커들이 유출된 개인 정보와 딥페이크를 이용해 면접을 응시하는 경우가 증가하고 있다며 주의를 당부하기도 했다. 해커들은 주로 개인 정보관리, 재무담당, 사내 IT 인프라 관리자와 같이 기업의 주요 정보에 쉽게 접근할 수 있는 직무를 지원했다. 취업에 성공하는 경우, 해커는 곧바로 기업의 주요 정보 접근 권한을 갖게 되는 것이다.

미국의 경우 팬데믹으로 인해 대부분의 채용 절차를 비대면으로 진행하고, 원격 근무가 도입된 기업이 많기 때문에 이러한 온라인 취업 사기가 활개칠 수 있었다. 국내의 경우 아직 온라인 취업 사기 사례는 보고되지 않았으나, 취업 면접을 비롯하여 금융, 의료, 보험 등의 서비스가 비대면으로 전환되고 있는 추세이기 때문에 딥페이크를 이용한 공격에 노출될 가능성이 증가하고 있다. 특히 보험산업 분야의 경우 딥페이크로 인한 보험 사기가 증가할 것을 우려하여 이에 대한 법안 마련과 기술적, 사회적 조치 대응 마련을 촉구하고 있는 상황이다.

생체 인증 우회



딥페이크는 공격자가 생체 인증을 우회하는 방법으로 사용될 수 있다. 외모나 목소리는 개인의 고유한 특성이기 때문에 개인을 식별할 수 있는 수단 중 하나로 쓰인다. 예를 들어 사람마다 발음, 억양, 속도, 성대 특성, 비강 구조가 다르기 때문에 목소리를 분석해 개인을 구분하고 특정할 수 있다. 하지만 딥페이크 기술을 악용할 경우 이러한 특성들을 쉽게 모방할 수 있다. 이와 같은 딥페이크 기반 신원 사기는 주로 금융, 보험 관련 사기에 악용된다.

생체 인증 우회는 PAD(Presentation Attack Detection) 기술이 적용된 인증 시스템을 사용하면 어느 정도 방어가 가능하다. PAD는 머신러닝을 이용하여 영상 속의 사람이 실제 사람인지, 또는 딥페이크 소프트웨어를 사용하고 있는지 탐지한다. 딥페이크로 생성된 영상 정보는 기존 영상에서 볼 수 없는 특징을 가지고 있기 때문에 이러한 점을 이용하여 진위 여부를 판별할 수 있다. 영상 속 사람이 움직일 때 부자연스러운 영상 처리, 깜빡이지 않는 눈, 제대로 생성되지 않은 눈 또는 치아 등의 변수를 통해 딥페이크를 구분하는 것이다.

마치며

현재의 딥페이크 기술은 눈으로 보았을 때 이상한 점을 느낄 수 있는 정도로 아직 완성되지 않은 기술이다. 하지만 인공지능 기술이 발전함에 따라 점차 정교해지고 현실과 구분하기 어려워지고 있다. 딥페이크 기술이 정교해질 수록 온라인 취업 사기, BEC(Business Email Compromise) 등의 사회공학적 공격이 심각한 사회적 문제로 떠오를 것이다. 또한 딥페이크는 누구나 사용할 수 있도록 오픈소스로 공개된 기술이기 때문에 이에 대한 심각성을 인지하고 보안 대책을 마련할 필요가 있다.

참고문헌

https://www.boannews.com/media/view.asp?idx=108013

https://www.boannews.com/media/view.asp?idx=107306

https://www.shrm.org/resourcesandtools/hr-topics/global-hr/pages/inadvertently-hiring-it-workers-from-north-korea.aspx

https://www.cio.de/a/wie-hacker-mit-machine-learning-angreifen

https://www.ic3.gov/Media/Y2022/PSA220216