서울과학기술대학교

Cybersecurity Forecast

Google Cloud Security

컴퓨터 보안

11장. 최신 ICT 보안기술(2)

최신 사이버보안 공격 전망

박종혁

서울과학기술대학교 컴퓨터공학과

jhpark1@seoultech ac kr

글로벌 보안환경 개요

- AI·사이버범죄·국가위협이 동시에 고도화됨
  - 2026년은 기술·보안 변화가 정점에 도달하는 시기임
  - 공격 속도가 증가하면서 기존 보안체계의 한계가 명확해짐
  - 조직은 'AI 기반 위협 대응 구조'로의 전환이 필수적임

AI 공격자 활용 범위 확대

- 공격자들이 AI를 표준 도구처럼 활용함
  - 공격 준비·실행·확산 속도가 비약적으로 빨라짐
  - 이전에는 전문 인력이 필요했던 공격이 자동화됨
  - 다양한 공격 시나리오를 AI가 자율적으로 생성함

AI 악성코드 자동화

- 악성코드 제작이 AI에 의해 실시간 자동화됨
  - AI는 탐지 회피 전략을 수초 내 재설계할 수 있음
  - 폴리모픽·메타모픽 코드 변형이 자동 생성됨
  - 보안 분석 속도보다 공격 변형 속도가 더 빨라짐

✅ **폴리모픽(Polymorphic)**

- 악성코드가 **암호화 키·외형만 계속 바뀌지만 기능은 동일함**.
- **시그니처 기반 탐지 우회** 목적의 빠른 외형 변조 방식임.

✅ **메타모픽(Metamorphic)**

- 악성코드가 **자신의 코드를 재작성해 완전히 다른 프로그램처럼 보이게 함**.
- 구조 자체를 바꾸기 때문에 **정적 분석을 거의 불가능하게 만드는 고급 변형 방식**임

프롬프트 인젝션 위협 확대

- AI 시스템을 속여 정책 우회 유도하는 공격 증가
  - LLM 기반 내부 서비스가 모두 공격 표면을 가짐
  - 악의적 요청을 정상 요청처럼 보이게 변조함
  - 데이터 탈취·시스템 명령 실행 등 심각한 피해 가능

AI 모델 자체 공격

- 훈련데이터·파라미터 조작 공격 증가
  - 모델 편향·오류를 의도적으로 삽입하는 공격 성행
  - 기업 내부 RAG·LLM 서비스가 주요 타깃으로 떠오름
    - 기업이 내부 데이터(문서·DB·지식베이스)를 LLM과 연결해 사내 전용 AI 검색·질의응답 시스템을 구축한 형태
    - 내부 정보가 LLM으로 전달되기 때문에 보안·접근권한 관리가 매우 중요
  - 데이터 오염으로 기업 의사결정에 왜곡 발생 가능

AI 기반 사회공학 심화

- AI 음성·이미지·텍스트 활용한 사칭 정교화
  - 목소리·얼굴·대화 패턴을 모두 AI로 재현 가능함
  - 임직원·IT팀 사칭 공격의 성공률 증가
  - 개인별 맞춤형 피싱으로 전통적 필터링 우회 가능

AI 기반 정보조작·심리전

- 딥페이크·가짜뉴스 기반 공격 증가
  - 국가·기업 대상 여론 조작이 체계적으로 이루어짐
  - SNS·메신저에서 대량 자동 생성 콘텐츠 확산
  - 심리전·선전 전략에 생성 AI가 적극 활용됨

AI 에이전트 도입 증가

- 기업 내 업무 자동화 위해 AI 에이전트 도입 급증
  - AI 에이전트는 독립적 판단·행동을 수행함
  - 기존 사람 중심 보안모델로는 제어 어려움
  - AI 에이전트 관리·모니터링 체계 필요

Agentic Identity Management

- AI 에이전트용 권한 관리체계 필요
  - JIT (Just In Time)기반 접근 제어가 필수
    - 필요한 순간에만 잠깐 권한을 부여하고, 작업이 끝나면 즉시 권한을 회수하는 방식
    - 지속적인 고정 권한을 없애 권한 오남용·침해사고 위험을 크게 줄임
  - 행동 기반 리스크 평가가 요구됨
  - AI가 권한을 잘못 사용하면 엄청난 피해 발생 가능

Shadow Agent 리스크

- 비인가 AI 시스템이 그림자 인프라로 확산됨
  - 직원이 임의로 외부 AI 연동 시 정보유출 위험 증가
  - 관리되지 않는 AI 트래픽을 통해 데이터 누출 발생
  - AI 전용 트래킹·감사 시스템 구축 필요

보안 분석가 역할 변화

- AI가 분석·요약·탐지 수행으로 업무 구조 변화
  - SOC는 분석가 중심에서 AI 중심 자동화 구조로 이동
  - 분석가는 '판단·감독·결정' 중심 역할 맡게 됨
  - 반복 업무는 AI가 수행해 효율 대폭 상승

Agentic SOC 등장

- AI 기반 실시간 대응 SOC가 구현됨
  - AI가 위협을 자동 헌팅하고 우선순위까지 판단함
  - 분석가는 AI 결과를 검증·승인하는 역할 수행
  - 대응 속도·정확도가 기존 대비 크게 향상됨

랜섬웨어 구조 변화

- 암호화 + 탈취 기반 다중 갈취 모델 정착
  - 단순 암호화에서 벗어나 데이터 유출이 핵심 압박 요소
  - 복합 갈취로 피해자 협상 압박이 훨씬 강화됨
  - 초기 침투는 여전히 인간 취약점 활용 비중 높음

공급망 공격 증가

- 3rd-party 공격이 대규모 확산 피해 유발
  - 공급업체 하나가 침해되면 연관 조직 수백곳 영향
  - 제로데이 조합한 공급망 공격 증가
  - 공급망 보안은 차년도 핵심 전략 요소

온체인/Web3 범죄 증가

- 블록체인 기반 사이버 범죄 급증
  - 스마트계약 취약점·지갑 탈취 공격 확대됨
  - 탈중앙형 C2·데이터 탈취 등 새로운 공격 증가
  - 암호자산 가치 상승과 함께 공격 ROI가 커짐

블록체인 포렌식 중요성

- 온체인 데이터는 조작 불가·영구 기록됨
  - 공격자의 지갑 이동 경로를 추적 가능함
  - 분석 기술 격차가 조직 보안 성패를 좌우함
  - Web3 전문 보안팀 필요성이 높아짐

가상화 인프라 위협 증가

- 하이퍼바이저·VM 인프라 공격 증가
  - EDR 사각지대로 공격에 매우 취약함
  - 호스트 침해 시 수백 VM 손실 가능
  - 기업 핵심 운영이 즉시 중단될 수 있음

ICS/OT 공격 증가

- 산업 제어 시스템(OT) 공격 증가
  - IT 시스템 침해가 OT 운영 중단으로 이어짐
  - 공장·전력·물류 등 핵심 인프라가 표적이 됨
  - 피해 발생 시 경제적 영향이 매우 큼

OT 보안 전략

- OT 환경 보호 위한 분리·제어 체계 필요
  - MFA·제로트러스트 기반 접근 관리 필수
  - 오프라인 백업이 랜섬웨어 대응 핵심
  - OT는 탐지보다 회복 전략이 더 중요함

AI 시대 보안전략

- AI 중심 보안체계 필요
  - AI 데이터 보호·권한 통제가 가장 중요함
  - AI 에이전트 오남용 방지가 핵심
  - AI 공격·방어 속도 차이가 위험을 결정함

조직 보안체계 재편

- AI 기반 자동화 중심으로 보안 구조 변화
  - SOC 운영방식·프로세스·인력 구조 전면 재편 필요
  - AI 전문 인력 확보가 조직 경쟁력 요소가 됨
  - 데이터·접근 통합 관리가 필수

전사적 대응 로드맵

- AI 리스크 평가·모델링 기반 전략 필요
  - RAG·LLM 서비스 보호가 필수 요건이 됨
  - AI 에이전트 활동 로그·감사 규칙 수립 필요
  - 데이터 보호·접근 제어 강화가 핵심

결론: 2026 핵심 방향성

- AI가 공격과 방어를 동시에 재편하는 시대
  - 공격 속도 증가에 대응한 자동화 방어 필요
  - 가상화·OT·Web3 등 신흥 공격면 대비 필수
  - AI 기반 위협 대응능력이 조직 생존을 결정함

참고문헌

- Cybersecurity Forecast 2026, Google Cloud Security, 2025