한국보안정책개발원 자료

2025년 07월

1. 서비스형 랜섬웨어(RaaS) 등장 원인은?

▷ **경제적 이익 분배 모델**: RaaS는 랜섬웨어 개발자가 자신의 악성코드를 직접 배포관리하지 않고, 제휴 해커(affiliate)에게 판매하여 수익의 일부를 나눠 갖는 구조입니다.

이로써 개발자는 지속적인 업데이트와 기능 개선에 집중하고,

유통은 제휴자가 담당해 양쪽 모두 수익 극대화를 꾀할 수 있습니다.

▷ **낮은 기술 진입장벽**: 서비스형 모델로 악성코드를 구매만 하면 누구나 공격자가 될 수 있어, 전통적 해커보다 기술력이 낮은 범죄자도 진입할 수 있습니다. 이로 인해 공격 조직이 폭발적으로 늘어나고 추적이 더욱 어려워졌습니다.

▷ **디지털 지하경제 활성화**: 암호화폐 결제와 다크웹 기반 시장이 성숙하면서, 범죄자 간 신뢰 기반 거래가 용이해졌습니다.
개발자?유통자?피해자 구조가 완전한 '사이버 범죄 생태계'를 형성하고 있습니다.

2. 피해 예방 5대 방법

▷ **정기적 오프라인 백업**

핵심 데이터는 주기적으로 백업하고, 백업本은 네트워크에서 물리적으로 분리하여 보관해야 합니다.

▷ **최신 패치 및 취약점 관리**

운영체제(OS)와 주요 애플리케이션의 보안 패치를 즉시 적용하고, 취약점 스캔을 정기 수행해야 합니다.

▷ **네트워크 분리(세분화) 및 접근 통제**

중요 시스템은 별도 VLAN 또는 서브넷으로 분리해 확산을 차단하고, 불필요한 포트프로토콜 접근을 제한해야 합니다.

▷ **보안 솔루션 도입 및 모니터링**

EDR(엔드포인트 탐지대응), XDR, AI 기반 위협 탐지 솔루션 등으로 의심 행위를 실시간 파악하고 자동 대응 체계를 구축합니다.

▷ **피싱스미싱 대응 교육**

직원 대상 정기적인 모의 피싱 훈련과 보안 인식 교육을 실시해, 악성 이메일첨부파일 실행을 원천 차단합니다.

3. 정부기관이 주의해야 할 事案

▷ **통합 가이드라인 보급 및 준수 강제화**

KISA의 '랜섬웨어 대응 가이드라인' 등을 기반으로 공공민간 기관의 의무적 이행을 법제화하고, 이행 여부를 정기 점검해야 합니다.

▷ **CISO 지정 및 정보보안 관리체계(ISMS) 확대**

주요 기관에 CISO(정보보호최고책임자) 지정을 의무화하고, ISMS 인증 대상을 확대해야 합니다.

▷ **사이버 위협 정보 공유(C-TAS) 활성화**

공격 징후와 IoCs(침해 지표)를 실시간 공유하는 체계를 고도화해, 전염병처럼 확산되는 사이버 위협을 조기에 억제해야 합니다.

▷ **국제 공조 및 법제도 정비**

RaaS 제작 유통 주체에 대한 국제 공조 수사와 제재를 강화하고, 암호화폐 익명 거래 근절을 위한 관련 법제도를 정비해야 합니다.

4. 해외 + 국내 피해 사례

▷ **국내 사례**

· **예스24**: 2025년 6월, 서비스형 랜섬웨어 공격으로 주요 시스템이 암호화되어 장시간 복구 지연이 발생

· **SGI서울보증**: 2025년 7월, 주택담보대출 전세대출 휴대폰 할부 개통 시스템 마비 사태를 초래

▷ **해외 사례**

· **미국 캔자스주 병원**: 2025년 1분기, 환자 22만 명 이상의 정보 유출 후 200만 달러(약 28억 원) 요구

· **영국미국프랑스 교육기관**: 2025년 1분기 학교들에 대한 공격이 160% 이상 급증, 등교 중단 및 개인정보 대량 유출

· **미국 CMS 계약업체**: 2023년 랜섬웨어 공격으로 280만 명의 메디케어메디케이드 정보 노출, 무료 신용 모니터링 제공 후 복구