2025년 사이버 위협 동향 및 2026년 전망 보고서

안랩이 '2025년 사이버 위협 동향 & 2026년 전망' 보고서를 발간했다. 이 보고서는 안랩의 위협 인텔리전스 플랫폼 AhnLab TIP를 통해 제공되는 보안 콘텐츠를 기반으로, 2024년 4분기부터 2025년 3분기까지의 다양한 보안 이슈 및 트렌드를 살펴보고 2026년 사이버 보안 위협을 조망한다.

▶보고서 다운로드

본 보고서의 구성은 다음과 같다.

Part 1. 2025년 사이버 위협 동향

2025년 사이버 위협 동향에서는 ▲국내외 주요 보안 사건 ▲공격 그룹 트렌드 ▲랜섬웨어 트렌드 ▲기타 주요 위협 트렌드 ▲공격 통계를 살펴본다.

1. 국내외 주요 보안 침해 사건

올해 국내에서 이슈가 되었던 통신사 해킹, 금융사 랜섬웨어 감염 등 주요 사건들과 미국 통신사-정부 연계 공격, 일본 아사히 그룹 랜섬웨어 공격 등 해외에서 발생한 보안 사건들을 시간 순서대로 분석한다.

2. 공격 그룹 트렌드

다크웹에서 확인한 공격 그룹 동향 Top 9과 북한, 중국, 러시아 등 6개 국가의 주요 APT 그룹의 상세한 공격 트렌드를 살펴본다.

3. 랜섬웨어 트렌드

먼저, 지난 1년 간 랜섬웨어 생태계에서 나타난 특징을 알아본다. 그리고, 랜섬웨어 그룹 활동 Top 10과 주요 피해 산업군 및 국가에 관한 분석 내용을 통계 자료와 함께 소개한다.

4. 기타 주요 위협 트렌드

악성코드, 공격 기법, 취약점, 모바일 위협 등 주요 위협 중 주목해야 할 트렌드 들을 주제 별로 분석한다.

5. 공격 통계

유행했던 공격 유형과 산업군 별 공격 동향을 통계 자료와 함께 살펴본다.

Part 2. 2026년 전망

2026년 예상되는 위협 동향 Top 5와 분석 내용을 소개한다. 2026년 전망 5개는 다음과 같다.

1. AI 기반 사이버 공격의 전방위 확산

AI를 활용한 맞춤형 공격과 AI 모델을 겨냥한 공격 기법이 고도화될 전망이다.

2. 랜섬웨어 공격 확대 및 피해 심화

소규모 랜섬웨어 조직이 다수 운영되는 파편화 및 카르텔화가 지속되고, 특히 중소기업을 노린 공격이 증가할 것으로 예상된다.

3. 오픈소스 생태계를 이용한 공급망 공격

공격자들은 오픈소스 생태계를 지속적으로 공략하고, 소프트웨어, 클라우드, 하드웨어 등 도메인을 가리지 않고 공급망 공격을 감행할 전망이다.

4. 국가 핵심 인프라에 대한 위협 확대

지정학적 갈등 심화로 국가 핵심 인프라 타격이 늘어날 것으로 보이며, IT와 OT를 아우르는 CPS(Cyber-Physical System) 보안이 더 중요해질 것이다.

5. 증가하는 리눅스 위협

주요 비즈니스 데이터들이 저장된 리눅스 서버는 2026년에도 공격자들의 표적이 될 것이다. 특히, 국가 핵심 인프라 타격 증가가 전망되는 가운데, 리눅스 위협도 그 연장선에 있다.

자세한 내용은 보고서 전문을 통해 확인할 수 있다.

▶보고서 다운로드

AhnLab

ASEC