과학기술정보통신부 | 보도자료 | 대체불가 대한민국

보도시점 2026. 7. 30.(목) 12:00 (2026. 7. 31.(금) 조간) 배포 2026. 7. 30.(목) 09:00

2026년 상반기 사이버위협 동향 발표

- 상반기 침해사고 1,236건 발생, 전년 동기대비 19.5% 증가 -
- 생성형 AI 확산에 따른 보안위협과 소프트웨어 공급망 공격 고도화 -
- DDoS, 랜섬웨어, API·계정 탈취 등 주요 침해사고 동향 분석 -

과학기술정보통신부(부총리 겸 과학기술정보통신부 장관 배경훈, 이하 '과기정통부')와 한국인터넷진흥원(원장 이상중, 이하 'KISA')은 국내 기업들이 **갈수록 고도화되고 있는 사이버위협에 선제적으로 대응**하고, **사이버침해사고로 인한 피해를 최소화**할 수 있도록 지원하기 위해서 **"2026년도 상반기 국내 사이버위협 동향"**을 발표했다.

과기정통부(KISA)는 올해 상반기에 **KISA에 접수된 침해사고 통계**를 분석하고, **국내 및 글로벌 정보보안 전문가**와 협력 네트워크*를 구성하여 상반기 침해사고 **핵심 유형**을 분류한 **상반기 사이버위협 동향과 함께 전문가 기고문**을 보고서에 담았다.

*(국내, 8개사) 안랩, 지니언스, 이글루코퍼레이션, NSHC, S2W, SK쉴더스, 플레인비트, 엔키, (글로벌, 7개사) Cisco Talos, Google, Microsoft, Trend Micro, Zscaler, Palo Alto Networks, Kaspersky 15개 기업

< 2026년 상반기 사이버 위협 동향 보고서 구성 >

신고 통계	2026년 상반기에 KISA에 신고 접수된 침해사고 신고 통계
'26년 상반기 사이버 위협 동향	① 생성형 AI 확산에 따른 보안 위협
	② 오픈소스 생태계를 노린 개발자 계정 탈취와 소프트웨어 공급망 공격의 고도화
	③ 국제 핵티비스트의 국내 대상 DDoS 공격 증가와 서비스 가용성 위협
	④ 랜섬웨어 공격의 지속적인 고도화와 데이터 유출을 결합한 이중 갈취 확산
	⑤ API 및 계정 탈취를 악용한 개인정보 유출 위협 지속
전문가 기고	① 판도라의 상자 '미토스'가 열어젖힌 취약점 연구의 새 흐름
	② 장악된 파이프라인: 오픈소스 공급망을 노린 TeamPCP 연쇄 침해 분석
	③ 국가망 보안체계(N2SF)로 보안패러다임 변화
	④ 법제도 변화에 따른 보안기업 보안실무의 실질적인 변화와 잔존 한계점 (기업의 정보보호 거버넌스 관점에서)

※ 보고서 원문은 7월30(목) 12:00시 기준 보호나라(www.boho.or.kr) 게시

< 침해사고 통계 >

2026년 **상반기에는 KISA에 1,236건의 침해사고가 신고·접수**되어 2025년 상반기보다 **19.5% 증가**했고, **신고·접수가** 가장 많았던 **2025년 하반기보다는 8.4% 감소했다**. 국내 민간 전문가들은 이와 같은 침해사고 신고 추세에 대해 작년 **통신 3사 침해사고**('25.4월, 9월, 10월)를 계기로 **침해사고 신고에 대한 기업 인식 개선**이 **'25년 하반기 침해사고 신고에 반영**되어 가장 높은 침해사고 신고 건수를 기록했을 것이라는 의견을 제시했다.

침해사고 유형별로는 분산서비스거부 공격(DDoS, Distribute Denial of Service)**과 랜섬웨어 감염** 신고가 큰 증가세를 보였다. ①**서버 해킹**은 조사 대상 전체 기간 중 **가장 큰 비중을 차지**하고 있으며, 신고 건수는 **2025년 상반기 531건에서 2026년 상반기 487건으로 8.3% 감소**했다. 반면, ②**DDoS 공격은 2025년 상반기에 238건에서 2026년 상반기 373건으로 56.7% 큰 증가세**를 보여주고 있다. ③**랜섬웨어** 신고는 145건으로 **악성코드 감염 신고 201건의 72.1%**를 차지했다. 이는 **2025년 상반기 82건보다 63건(76.8%) 증가를 나타낸다.**

< 최근 3년간 반기별 침해사고 신고접수 현황 >

구 분 \ 연 도		2024 (상반기)	비율	2024 (하반기)	비율	2025 (상반기)	비율	2025 (하반기)	비율	2026 (상반기)	비율
침해사고 신고	DDoS 공격	153	17.0%	132	13.4%	238	23.0%	350	25.9%	373	30.2%
	악성코드	106	11.8%	123	12.4%	115	11.1%	239	17.7%	201	16.3%
	(랜섬웨어)	(92)	(10.2%)	(103)	(10.4%)	(82)	(7.9%)	(192)	(14.2%)	(145)	(11.7%)
	서버 해킹	504	56.1%	553	56.0%	531	51.4%	522	38.7%	487	39.4%
	기타	136	15.1%	180	18.2%	150	14.5%	238	17.6%	175	14.1%
합 계		899		988		1,034		1,349		1,236	

< 2026년 상반기 사이버위협 동향 >

과기정통부(KISA)는 **국내 및 글로벌 정보보안 전문기업 15개 社 전문가들**과 함께 올해 상반기 사이버 침해사고 중 **핵심 유형 5가지를 도출**하였다. 이를 유형별로 분류하여 **사고원인 분석, 기술적 특징 및 기업 정보보호 관리체계에 반영해야할 사항들**을 제시함으로써 **국내 기업들이 자율적으로 자체 정보보호 역량을 강화할 수 있도록 지원**하였다.

① 생성형 AI 확산에 따른 보안 위협

인공지능(AI)은 취약점 탐지, 악성코드 분석, 코드 검토, 보안 이벤트 요약 등 방어 업무의 생산성을 높이고 있다. 그러나 **공격자들이 AI를 활용하면, 공격 대상의 취약점 탐색, 패치 전후 코드 비교, 공격 코드 초안 작성, 정찰 결과 정리, 반복 실험이 빨라질 수 있다.** 모든 공격이 완전히 자동화되는 것은 아니더라도, **공격 준비에 드는 시간과 비용이 줄어들면 기존보다 더 많은 대상을 짧은 시간에 분석**할 수 있다.

특히, AI 에이전트는 **이메일, 코드 저장소, 클라우드 서비스, 협업 플랫폼 등 외부 시스템과 연결돼 자율적으로 업무를 수행하면 공격 표면을 크게 넓힐** 수 있다. 특히, **악성 지시문 주입**(Prompt Injection), **권한 오남용**, **민감정보 유출, 악성 도구 호출, 잘못된 자동 실행**이 발생할 수 있다.

< 보안주의 사항 >

- ▲ AI 서비스와 에이전트가 사용하는 응용프로그램 인터페이스(API), 키, 토큰, 서비스 계정을 중앙에서 관리하고 장기 자격증명 사용을 최소화
- ▲ 민감정보를 프롬프트에 입력하지 않도록 데이터 분류·필터링·마스킹 정책을 적용하고, AI 입력·출력·도구 호출 이력을 감사 로그로 보관
- ▲ AI가 생성한 코드, 보안 분석 결과, 자동 조치 명령은 담당자가 검증한 뒤 반영하도록 승인 절차를 마련하고 문서화하여 관리
- ▲ AI 서비스의 공격 표면과 연결 관계를 공격 경로 관리를 위해 자산 목록을 통해 구성요소, 지원 종료 여부, 외부 노출 범위, 내부 연결 관계를 상시 식별
- ▲ 「AI 기반 사이버 공격 대비 기업 대응 요령」('26.5, KISA 보호나라)이 제시한 AI 기반 방어, 거버넌스 정비, 오픈소스 식별·관리, 보안 기본기 집중, 대외 정보 공유 및 협력

② 오픈소스 생태계를 노린 개발자 계정 탈취와 소프트웨어 공급망 공격의 고도화

공격자들은 **정보탈취형 악성코드(Infostealer)를 개발자 단말과 클라우드 개발환경에 무단으로 설치**하고, 소프트웨어 소스코드 개발 관리(GitHub), 자바스크립트 개발 관리(npm) 및 파이썬 개발 관리(PyPI) 환경의 **계정 비밀번호, 개인 접근 토큰(PAT, Personal Access Token), 클라우드 접근 키를 주요 표적**으로 삼고 있다. 탈취된 계정정보, 토큰 및 접속 키 등 **자격증명은 정상 프로젝트의 유지관리 권한을 악용하거나, 지속적 통합·지속적 배포**

(CI/CD, Continuous Integration/Continuous Delivery) **파이프라인을 통해 악성 패키지를 배포하거나 기업 정보를 탈취**하는데 직접 사용되고 있다.

공급망 공격은 개발자 한 명의 피해로 끝나지 않는다. 정상 패키지를 신뢰한 다수 기업과 기관의 빌드 서버, 개발자 단말, 운영환경으로 악성코드가 연쇄 확산될 수 있다. 특히, 자동화 계정과 빌드 파이프라인은 사람의 확인 없이 광범위한 배포를 수행하기 때문에 **하나의 토큰 노출이 수백 개 저장소와 서비스의 침해 및 정보유출**로 이어질 수 있다.

< 보안주의 사항 >

▲ 소프트웨어 구성요소 분석(SCA, Software Composition Analysis)과 소프트웨어 자재명세서(SBOM, Software Bill of Materials)를 활용하여 사용 중인 소프트웨어의 구성요소와 버전을 식별·관리
▲ 개발자와 유지관리자 계정에는 다중인증(MFA, Multi-Factor Authentication)을 적용하고, PAT·npm·PyPI 토큰은 최소 권한과 최소 유효기간을 원칙으로 발급·관리
▲ CI/CD 환경에서 코드 서명, 커밋·아티팩트 무결성 검증, 승인된 배포자 확인, 보호 브랜치와 이중 승인 절차를 적용
▲ 엔드포인트 탐지 및 대응 솔루션(EDR, Endpoint Detection and Response)을 개발자 단말과 빌드 서버에 적용하고, 비정상적인 저장소 접근, 토큰 사용, 패키지 배포 행위를 탐지·관리
▲ 비밀정보는 소스코드와 환경변수에 장기간 저장하지 말고, 전용 시크릿 관리 시스템을 통해 관리하고, 일회성·단기 자격증명을 사용하며, 이런 모든 관리 절차는 문서화 관리

③ 국제 핵티비스트의 국내 대상 DDoS 공격 증가와 서비스 가용성 위협

국제 핵티비스트(Hacktivist) 그룹이 국내 공공기관과 민간기업을 공격 대상으로 지목하면서 분산 서비스 거부 공격(DDoS, Distributed Denial of Service)에 대한 경계가 높아졌다. RipperSec 해킹조직은 텔레그램 채널 등을 통해 우리나라 기업 등을 공격 대상으로 언급하고 국내 기관에 대한 공격을 예고하거나 공격을 실제 수행했다고 주장한 사례를 소개하기도 하였다.

이들 공격의 주된 목적은 **기밀정보 탈취보다 대외 서비스의 가용성**을 떨어뜨려 사회적 혼란을 유발하고, 조직의 존재감을 과시하는 데 있다. 공격 성공 여부와 장애 화면을 사회관계망서비스(SNS, Social Networking Service)와 메신저에 게시해 대상 기관의 심리적 부담과 대외적 혼란을 키우는 것을 목적으로 한다.

기업들은 평상시에 인터넷 서비스 제공 사업자(ISP, Internet Service Provider), 클라우드 서비스 제공 사업자(CSP, Cloud Service Provider) 및 한국인터넷진흥원(KISA) 등과 비상 대응 절차를 협의하고, 대응할 수 있는 체제를 갖추어야 한다.

중소기업들은 KISA에서 제공하는 'DDoS 사이버대피소'를 무료로 이용할 수 있다. **KISA 보호나라 웹사이트를 통해 사전입주를 신청할 수 있으며, 실제 공격을 받아 서비스가 마비되는 긴급 상황이라면 국번 없이 118 KISA 상담센터, 사이버대피소 담당자 직통 02-405-4769 또는 help@ddos.or.kr로 연락하여 사이버대피소 서비스 지원을 신청**하거나 상담받을 수 있다.

< 보안주의 사항 >

▲ 콘텐츠 전송 네트워크(CDN, Content Delivery Network), 웹방화벽(WAF, Web Application Firewall), 클라우드 DDoS 방어 서비스를 연계해 네트워크·애플리케이션 계층을 함께 보호

▲ 요청 빈도 제한(Rate Limiting), 행동 기반 탐지, IP 평판, CAPTCHA, 캐시 정책을 각 기업별 서비스 특성에 맞게 적용

▲ 공격 전환 기준, 우회 회선 적용, 긴급 차단, 고객 공지, 대외 커뮤니케이션, 로그 보존 절차를 포함한 플레이북을 마련하고 정기적으로 훈련

▲ 서비스별 정상 트래픽 기준선을 수립하고, 응답시간·오류율·동시접속·원본 서버 부하를 통합 모니터링

④ 랜섬웨어 공격의 지속적인 고도화와 데이터 유출을 결합한 이중 갈취 확산

랜섬웨어는 제조, 물류, 유통, 정보기술(IT, Information Technology) 서비스 등 산업 전반의 핵심 위협으로 지속되고 있다. 공격자는 시스템을 암호화하기 전에 중요 데이터를 외부로 빼낸 뒤, **복호화 대가와 데이터 비공개 대가를 동시에 요구하는 이중 갈취 방식을 사용**하고 있다. 내부망에 장기간 잠복해 자료를 수집한 후 암호화를 수행하면 업무 중단, 정보 유출, 법적 책임, 평판 훼손이 동시에 발생하게 된다.

서비스형 랜섬웨어(RaaS, Ransomware-as-a-Service)와 초기 접근 브로커(IAB, Initial Access Broker)의 분업 구조가 정착되면서 전문 공격자가 아니어도 침해된 계정이나 원격접속 권한을 구매해 공격에 참여할 수 있게 되었다. 협력업체와 공급망 계정을 우회 경로로 이용하는 사례가 늘면서, 대기업뿐 아니라 중소·중견기업과 협력사도 직접적인 표적이 되고 있다.

랜섬웨어 대응은 악성 파일 차단에 국한해서는 안 된다. 초기 침투부터 권한 상승, 내부망 이동, 데이터 수집·압축·외부 전송, 백업 훼손, 대량 암호화까지 공격 전 과정을 탐지하고 복구할 수 있어야 한다.

< 보안주의 사항 >

▲ 중요 데이터는 운영망과 논리적·물리적으로 분리하고, 삭제·변조가 어려운 불변(Immutable) 백업 또는 오프라인 백업을 운영

▲ 백업 성공 여부만 확인하지 말고, 평상시에도 정기 복구 훈련을 통해 실제 복구 시간과 서비스 재개 가능 여부를 검증

▲ 원격접속 자산에 다중인증(MFA, Multi Factor Authentication)와 최소 권한을 적용하고, 사용하지 않는 계정·포트·서비스를 제거해야할 필요

▲ 확장형 탐지 및 대응 솔루션(XDR, Extended Detection and Response)와 EDR을 활용해 권한 상승, 대량 파일 접근, 비정상 압축, 외부 전송, 백업 삭제 행위를 탐지·대응

▲ 사고 대응 절차, 의사결정 권한, 법률·홍보·고객 대응, 신고·복구 연락망을 사전에 수립해놓고, 협력사까지 포함해 정기적인 훈련 실시

⑤ API 및 계정 탈취를 악용한 개인정보 유출 위협 지속

개인정보 탈취 공격은 전통적인 데이터베이스(DB, Database) 서버 침해에서 **외부 API와 사용자 계정을 악용하는 방식으로 확대**되고 있다. 공격자는 **인증 우회, 객체별 권한 검증 미흡, 과도한 데이터 반환, 예측 가능한 식별자 등 API 설계상의 취약점을 이용**한다.

또한, **다크웹이나 과거 유출 사고에서 확보한 계정정보**를 자동화 도구로 대량 대입하는 **‘계정정보 재사용 공격’**(크리덴셜 스터핑, Credential Stuffing)을 수행한다. 이러한 요청은 **정상 서비스 이용과 형태가 유사**해 **기존 네트워크 보안장비만으로 비정상 행위를 구분하여 대응하기 어렵다.**

< 보안주의 사항 >

▲ 모든 대외 API에 대해 인증(Authentication)과 인가(Authorization)를 구분해서 점검하고, 사용자·객체·기능별 권한 검증을 서버 측에서 수행

▲ API 보안 솔루션과 WAF를 활용해 비정상 호출 빈도, 대량 조회, 순차 식별자 탐색, 비정상 지역·단말의 접근을 탐지·차단

▲ MFA 적용, 비밀번호 재사용 방지, 위험 기반 로그인, 유출 계정 모니터링, 자동화 로그인 방어를 적용

▲ 개인정보 처리 시스템에는 최소 권한, 중요정보 암호화, 접근기록 보존·점검, 이상 조회 경보를 적용해야 한다.

▲ API별 데이터 반환 항목을 최소화하고, 개발·테스트 환경에 실제 개인정보를 사용하지 않도록 가명·샘플 데이터를 적용

과기정통부 **최우혁 정보보호네트워크정책실장**은 **"AI 기반 사이버위협이 현실로 다가오고, 클라우드 환경 취약점을 대상으로 하는 지능화된 공격이 지속적으로 나타나고 있다."** 고 강조하며,

"이에 대비할 수 있도록 기업들의 정보보호역량 강화를 당부하며, 정부는 AI 기반의 예방·대응체계를 구축·운영하고, 선제적 취약점 발굴 조치를 통해 국민이 안심할 수 있는 사이버 환경을 조성해나가겠다" 고 밝혔다.

담당 부서	정보보호네트워크정책관실 사이버침해조사팀	책임자	팀 장	김우철 (044-202-6490)
		담당자	사무관	김성환 (044-202-6491)
관련 기관	한국인터넷진흥원 위협분석단	책임자	단 장	김광연 (02-405-4800)
		담당자	팀 장	김도원 (02-405-4810)