2025. 11

AhnLab

2025년 사이버 위협 동향
2026년 전망

개요

목차

개요

보고서 소개

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 전망한다.

AhnLab TIP는 여러 출처로부터 악성코드, 침해사고, 위협행위자, 취약점, 침해지표(IoC), 보안 뉴스 등 다양한 위협 정보를 수집, 분석 및 분류한다. 이를 통해, 고객이 위협 인텔리전스를 바탕으로 보안 전략을 수립하고 의사결정을 내릴 수 있도록 지원한다.

AhnLab TIP에 대한 자세한 내용은 안랩 공식 홈페이지와 AhnLab TIP 포털에서 확인할 수 있다.

→ 안랩 홈페이지 바로가기

→ AhnLab TIP 포털 바로가기

[그림] AhnLab TIP 대시보드

개요

숫자로 보는 안랩의 위협 인텔리전스

2,258개
위협 인텔리전스 게시글

AhnLab TIP의 "Intelligence" 게시판에는 최근 1년간 2,258개 콘텐츠가 게시됐다. 콘텐츠 종류는 다음과 같다.

- **ASEC Notes**: 위협 정보를 가장 신속하게 전달
- **Dark Web Notes:** 딥웹/다크웹 위협과 고위험 정보 제공
- **ASEC Blog**: 최신 위협을 빠르게 분석
- **동향 보고서**: 악성코드, 피싱, 취약점, 다크웹 등 다양한 동향 분석
- **분석 보고서**: APT 그룹, 공격 기법, 침해 사례 등 심층 분석

661개
보안 권고문

보안 권고문은 소프트웨어 취약점과 조직의 보안을 위협하는 이슈에 대해 신속한 정보와 대응 가이드를 제공한다.

매일 수천 ~ 수만개 IoC
30% - 안랩만의 IoC

악성 파일, URL, IP, 도메인 등 매일 수천 - 수만 건에 달하는 IoC를 제공해 고객이 위협 대응에 활용하도록 한다.

안랩은 국내 최대 규모의 위협 탐지 & 대응 센서 네트워크를 보유하고 있다. 이에, 안랩의 IoC 중에는 OSINT에서 확보가 어려운 독점적인 정보가 약 30%를 차지한다.

404개 – 위협 행위자
1,051개 – 악성코드 패밀리

안랩은 위협 행위자 및 악성코드 패밀리를 지속적으로 추적하고, 분석 정보를 AhnLab TIP를 통해 제공하고 있다.

Threat Actors 게시판에는 위협 행위자 상세 정보 외에도 연관 TTPs, IoC, 최신 기사 등을 파악할 수 있도록 한다.

Malware Families 게시판에는 악성코드 특징, 기법, 제작자 등을 기반으로 분류한 악성코드 군 정보를 제공한다.

2,216개
뉴스 클리핑

국내외 주요 언론 매체 및 벤더에서 발행한 보안 뉴스와 기술 문서를 제공한다. 각 뉴스에는 연관 IoC 정보를 포함해 기업 보안 담당자가 대응에 활용할 수 있도록 한다.

2,970개 – 외부 보고서
19,679개 – 소셜미디어 포스팅

국내외 주요 보안 기업과 전문가의 분석 리포트, X(구 Twitter) 등 소셜 미디어에서 선별한 최신 위협 동향 정보를 제공한다. 콘텐츠에는 연관 IoC가 함께 포함되어 있어, 고객이 빠르게 위협을 식별하고 대응 전략을 수립할 수 있도록 지원한다.

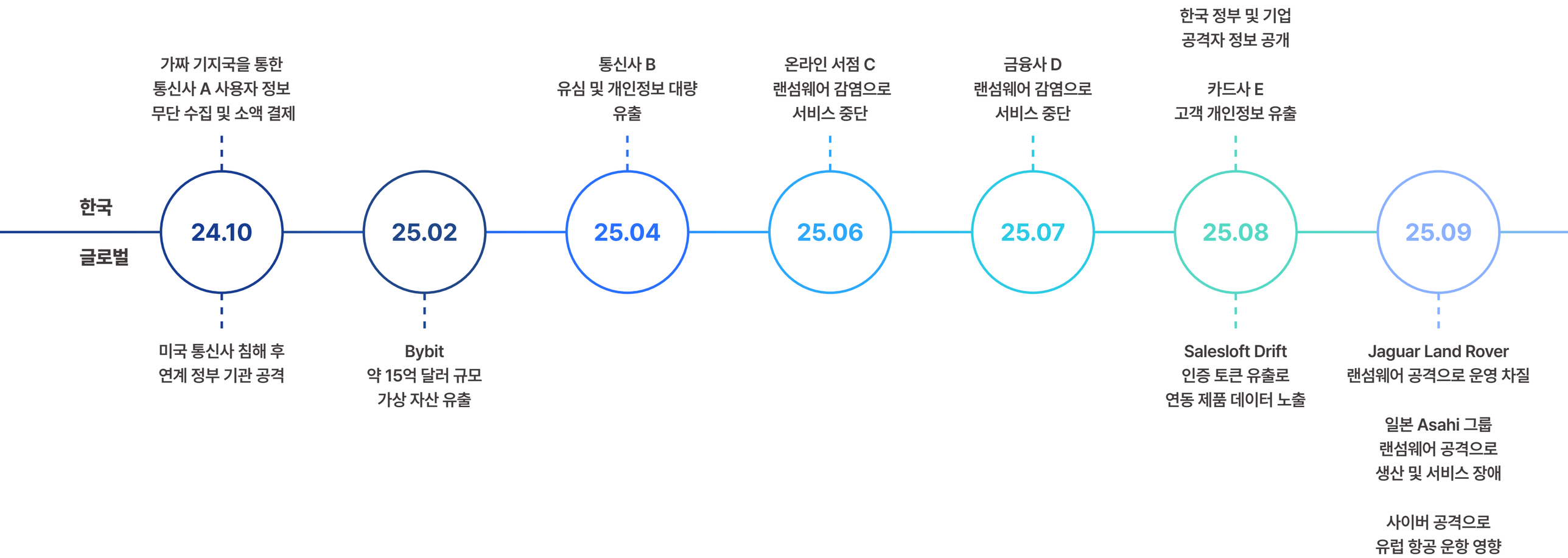
2025년 사이버 위협 동향

AhnLab

2025년 사이버 위협 동향 & 2026년 전망

2025년 사이버 위협 동향

주요 사건



2025년 사이버 위협 동향

주요 사건: 한국

2024.10. 통신사 A, 가짜 기지국을 통한 사용자 정보 무단 수집 및 소액 결제 피해

통신사 A 일부 사용자 대상 가짜 기지국 기반 해킹 사건이 발생했다. 약 2만 2천명의 개인정보가 노출되고, 368명에게 수억 원 규모의 무단 소액 결제 피해를 입었다.

공격자는 2024년 10월부터 가짜 기지국으로 피해자 휴대폰을 자동 접속시킨 뒤 IMSI 등 가입자 식별 정보를 탈취했다. 이후 복제폰 제작, 인증 절차 우회 등을 통해 소액 결제를 수행한 것으로 보인다.

경찰은 일부 범인을 검거하고 장비 일부를 확보했다. 정부는 민관합동조사단을 구성해 원인 규명에 나섰다. 해당 통신사는 신규 펨토셀 차단, 소액 결제 한도 축소, 유심 보호 서비스 확대, 피해자 환불 및 보상 조치를 시행 중이다.

2025.04. 통신사 B, 유심 및 개인정보 대량 유출

통신사 B는 약 2,300만 명의 고객 개인정보가 유출되는 대규모 해킹 사고를 겪었다. 유출 정보에는 가입자 전화번호, IMSI, IMEI, 유심 인증키(K값) 등 유심 핵심 식별 정보가 포함되었다. 이로 인해, SIM 스와핑, 명의 도용 등 2차 피해 우려가 제기되었다.

공격에는 리눅스 기반 BPFDoor 백도어가 사용되었다. 이 백도어는 커널 단 패킷 필터를 활용해 탐지를 회피하고, 특정 매직 패킷 수신 시에만 활성화된다. 공격자는 웹셸 및 원격 코드 실행(RCE) 취약점을 통해 내부 시스템에 침투했다. 이후, HSS 서버에 BPFDoor를 설치하고 유심 정보를 탈취한 것으로 확인됐다.

2025.06. 온라인 서점 C, 랜섬웨어 감염으로 서비스 중단

한국 1위 온라인 서점이자 티켓 플랫폼 C사는 **랜섬웨어 공격으로 웹사이트와 모바일 앱이 4일간 마비**됐다. 공격자는 주요 내부 파일과 관리자 계정을 암호화해 시스템 전체를 잠근 뒤 금전을 요구했다.

약 2,000만 명의 사용자가 도서 구매, 공연 예매, 커뮤니티 이용 등에 큰 불편을 겪었으며, 콘서트 및 팬미팅이 취소되거나 연기되기도 했다.

Key Point

- 통신사 A, 가짜 기지국 기반 해킹 피해 - 피해자 휴대폰 자동 접속 후 가입자 식별 정보 탈취
- 통신사 B, 고객 2,300만명 개인정보 유출 – 리눅스 기반 BPFDoor 악성코드 사용
- 온라인 서점 C, 랜섬웨어 감염 – 웹사이트와 모바일 앱 4일 간 마비

2025년 사이버 위협 동향

주요 사건: 한국

2025.07. 금융사 D, 랜섬웨어 감염으로 서비스 중단

금융사 D는 건라(Gunra) **랜섬웨어에 감염되어 전산 시스템이 마비**되는 대규모 사이버 공격을 당했다. 공격자는 SSL VPN 장비 SSH 포트에 로그인 시도를 통해 내부망에 침투했다. 이후 관리자 권한을 획득해 랜섬웨어를 배포했다.

이 랜섬웨어는 ChaCha8 + RSA 암호화 알고리즘을 사용해 주요 파일을 조건 별로 정교하게 암호화하고 .ENCRT 확장자를 붙였다. 랜섬웨어 감염으로 전세 자금 보증, 휴대폰 개통, 대출 보증 등 실제 금융 서비스가 중단되었다. 일부 지점은 수기 업무로 대응하기도 했다. 다행히, **금융보안원이 복구 도구를 제작해 시스템 복구에 성공**했다.

2025.08. 한국 정부 및 기업 공격자 'APT Down' 정보 공개

글로벌 해킹 컨퍼런스 DEF CON 33에서 공개된 보고서 'APT Down: The North Korea Files'는 한국을 공격한 APT 그룹의 실체를 드러냈다. 보고서는 해커 워크스테이션에서 추출한 8.9GB 분량 데이터를 기반으로, **한국 정부기관·선관위·언론·통신사 장기 침투 정황**을 담고 있다.

공격자는 피싱, 인증서 탈취, 내부망 측면 이동(Lateral Movement) 등 고도화된 기법을 사용했다. 또한, 북·중 합작 공격 정황도 확인되었다. 한국 정부는 일부 기관을 통해 대응에 나섰다. **안랩은 해당 공격을 분석한 Larva-25010 – APT Down 공격자 PC 분석 보고서를 공개했다.**

2025.08. 카드사 E, 고객 개인정보 유출 피해

카드사 E는 **297만 명의 고객 개인정보가 유출되는 대규모 보안 사고를 겪었다.** 이 중 28만 명은 카드번호, 유효기간, CVC, 비밀번호 등 결제에 직접 사용 가능한 민감 정보까지 유출되었다.

공격자는 온라인 결제 서버에 악성코드와 웹셸을 심어 데이터를 탈취했다. 총 200GB의 정보가 외부로 반출된 것으로 확인되었다.

E사는 피해 고객 카드 재발급, 연회비 면제, 무이자 할부, 전액 보상 등의 조치를 시행했고, 향후 5년간 1,100억 원 규모의 보안 투자를 약속했다.

Key Point

- 금융사 D, Gunra 랜섬웨어 감염 – 금융 서비스 중단 겪었으나 복구 도구로 복구 성공
- 공격 그룹 APT Down의 한국 기업/기관 장기 침투 정황 - 안랩 분석 보고서 발간
- 카드사 E, 297만 명 고객 개인정보 유출 – 총 200GB 정보 외부 반출

2025년 사이버 위협 동향

주요 사건: 글로벌

2024.10. 미국 통신사 침해 후 연계된 정부기관 대상 공격 발생

해킹 그룹 Salt Typhoon이 미국 주요 통신사 최소 8곳을 침해하여, 수사 기관의 감청 시스템과 민감한 통신 인프라에 접근했다.

이들은 Ivanti VPN(CVE-2023-46805, CVE-2024-21887), Fortinet EMS(CVE-2023-48788), Sophos Firewall(CVE-2022-3236), Microsoft Exchange ProxyLogon 등 취약점을 악용해 침투했다. 침해된 통신망을 통해 미국 정부 기관의 통신을 감청하거나, 법원 명령에 따른 감청 데이터에 접근한 정황도 확인되었다.

공격자는 GhostSpider, SnappyBee, Masol RAT 등 고도화된 백도어를 사용해 은밀하게 장기간 내부에 머물렀다. 일부 정부 웹사이트도 공격을 받은 것으로 알려졌다.

2025.02. Bybit, 약 15 억 달러 규모 가상 자산 유출

두바이 가상 자산 거래소 **바이비트(Bybit)는 약 15억 달러 상당의 암호화폐를 탈취당하는 해킹 피해를 입었다. 이 공격은 라자루스(Lazarus) 소행으로 추정**된다.

공격자는 콜드 월렛(cold wallet)에서 핫 월렛(hot wallet)으로 자금을 이체하는 과정을 노렸다. 내부 개발자 시스템을 해킹하거나 세이프 월렛(safe wallet) 플랫폼 서명 인터페이스를 조작해 다중 서명(Multisig) 지갑의 트랜잭션을 위조했다. 이 과정에서 악성 자바스크립트(JavaScript) 코드를 서명 호스트에 삽입했고, 정상 주소 위장한 뒤 실제로는 공격자 지갑으로 자산을 전송했다. 탈취된 자산은 이더리움(ETH), 스테이킹 이더리움(stETH) 등이었다. 바이비트는 보상 프로그램 등을 시행했다.

2025.08. Salesloft Drift, 인증 토큰 유출로 연동 제품 데이터 노출

세일즈로프트(Salesloft)의 Drift AI 챗봇 통합 기능이 해킹 당해 OAuth 토큰이 유출됐다. 세일즈포스(Salesforce) 포함 **700여 개 기업의 고객 데이터가 탈취**되었다.

공격자는 먼저 세일즈로프트의 깃허브(GitHub) 계정을 침해해 내부 코드를 확보했다. 이후, Drift의 AWS 환경으로 이동해 OAuth 토큰을 수집했다. 이 토큰을 이용해 세일즈포스 인스턴스에 접근해 고객 정보, 계정 등을 추출했다. 공격자는 AWS 키, 비밀번호, Snowflake 토큰 등도 수집한 것으로 알려졌다. 세일즈포스와 세일즈로프트는 Drift 앱을 AppExchange에서 제거하고, 모든 연결을 차단했다. 그리고, 피해 기업 알림 및 토큰 무효화를 진행했다.

Key Point

- Salt Typhoon, 미국 통신사 침해 후 수사 기관 감청 시스템 및 통신 인프라 접근
- 두바이 소재 바이비트(Bybit), 약 15억 달러 상당 암호화폐 탈취 피해 – Lazarus 소행 추정
- Salesloft의 Drift AI 챗봇 해킹 및 OAuth 토큰 유출, 700여개 기업의 고객 데이터 탈취

2025년 사이버 위협 동향

주요 사건: 글로벌

2025.09. 일본 Asahi 그룹 랜섬웨어 피해

일본 대표 식음료 기업 아사히(Asahi) 그룹은 **킬린(Qilin) 랜섬웨어의 공격을 받아 전국 30개 공장의 생산 및 물류 시스템이 마비**되는 사태를 겪었다.

공격자는 아사히의 일본 내 IT 인프라의 시스템을 암호화하고, 일부 데이터를 외부로 유출한 뒤 금전을 요구했다. Asahi Super Dry, Draft Beer, Dry Zero 등 주요 제품의 생산과 출하가 중단되었으며, 콜센터와 주문 시스템도 오프라인 상태가 지속되었다. 킬린 랜섬웨어 그룹은 Golang과 Rust 기반 고도화된 랜섬웨어를 사용하는 서비스형 랜섬웨어(RaaS) 조직으로, 이중 갈취(double extortion) 수법을 활용한다. 아사히 그룹은 외부 전문가와 협력해 복구를 진행 중이다. 일부 공장은 10월 초부터 부분적으로 가동을 재개했다.

2025.09. 영국 Jaguar Land Rover 랜섬웨어 피해

재규어랜드로버(Jaguar Land Rover, JLR)는 Scattered Spider 및 Lapsus$ 연계 조직으로 추정되는 조직의 랜섬웨어 공격을 받아 전 세계 생산이 중단되었다.

공격자는 **JLR의 내부 IT 시스템을 마비시켜 영국 내 주요 공장과 글로벌 생산 라인을 5주 이상 마비**시켰다. 3만 명 이상의 직원과 20만 명 규모의 공급망 인력이 영향을 받았다. 총 피해액은 약 19억 파운드(약 3.3조 원)로 추산된다.

JLR는 고객 데이터 유출은 없다고 밝혔으나, 생산 중단과 납기 지연, 부품 공급 차질로 인한 경제적 여파가 컸다. 영국 정부는 15억 파운드 규모의 긴급 대출 보증을 제공하며 산업 안정화에 나섰다.

2025.09. 사이버 공격으로 유럽 공항 장애 발생

유럽 공항들이 **콜린스 에어로스페이스(Collins Aerospace)의 MUSE 소프트웨어에 대한 랜섬웨어 공격으로 인해 대규모 장애**를 겪었다.
소프트웨어는 공항의 전자 체크인, 수하물 처리, 탑승권 발급 등을 담당한다.

이번 공격으로 인해 런던 히드로, 브뤼셀, 베를린, 더블린 공항 등에서 수백 편의 항공편이 지연되거나 취소되었다.

공격자는 콜린스 에어로스페이스의 유럽 데이터센터를 통해 침투한 것으로 추정된다. 일부 시스템은 복구 도중 재감염되며 복구가 지연되었고, 수천 명의 승객이 수동 체크인과 장시간 대기로 불편을 겪었다.

Key Point

- 일본 아사히 그룹, Qilin 랜섬웨어 공격 받아 30개 공장의 시스템 마비
- 재규어랜드로버, 랜섬웨어 공격으로 영국과 글로벌 생산 라인 5주 이상 마비 – 피해액 약 19억 파운드 추산
- 콜린스 에어로스페이스, 랜섬웨어 공격 당해 유럽 주요 항공편 지연 및 취소

2025년 사이버 위협 동향

공격 그룹 트렌드 - 다크웹 Top 9

안랩은 다크웹에서 사이버 위협 관련 이슈를 모니터링 및 분석해 AhnLab TIP에서 콘텐츠로 제공한다. 다음은 최근 1년 간 다크웹 동향을 통해 파악한 공격 그룹 관련 인사이트다.

1. 랜섬웨어 생태계 파편화와 소형 그룹 증가

2025년 랜섬웨어 생태계는 근본적인 구조 변화를 겪었다. 록빗(LockBit) 등 대형 그룹들이 수사 기관의 집중 단속으로 크게 위축되고, 랜섬허브(RansomHub)가 내부 갈등으로 공식 활동을 중단한 것이다.

그 반작용으로 40개 이상의 소형·신생 그룹이 대거 등장했다. 과거 소수 대형 그룹 체제가 Akira, Qilin, Play, Gunra 등으로 재편된 것이다. 소형 그룹들은 기존 유출된 LockBit 3.0, Conti 소스코드 등을 재활용하면서 독자 브랜드로 활동한다. 이들은 대형 공격 그룹보다 더 공격적이고 예측 불가능한 협상 전략을 구사한다. 일부는 복호화 도구조차 제공하지 않아 피해가 가중되고 있다.

랜섬웨어 생태계는 **중앙집중형에서 탈중앙화된 형태로 진화**하고 있다. 전통적인 IoC 기반 탐지가 한계에 부딪힌 가운데, **기존 방어 전략도 전면적인 재편이 필요**하다.

2. 한국 기업 및 금융기관 공격 급증

2025년 한국은 아시아에서 집중적인 사이버 공격을 받은 국가 중 하나였다. **2024년 인도와 일본에 대한 공격이 많았던 반면, 올해는 한국에 대한 선택적 공격 패턴이 보였다.**

앞서 다룬 통신사 2,700만 고객 정보 유출, 온라인 서점 랜섬웨어 공격, 금융사 랜섬웨어 공격 등 대형 침해사고가 연이어 발생했다. 특히, 금융 분야는 중소 자산 운용사까지 공격 대상이 되어 금융 생태계 전반이 위협받고 있다. **한국에 공격이 집중되는 이유는 높은 IT 의존도, 디지털 자산 가치, 글로벌 평균 대비 낮은 정보보호 투자 비율, 랜섬웨어 협상 비용 지불에 대한 인식, 미국 외 지역 공격 시 FBI 등 수사 기관 감시 회피 등이 있다.**

3. RaaS·화이트라벨 기반 랜섬웨어 카르텔

2025년 랜섬웨어 생태계의 가장 큰 변화는 화이트라벨 모델 기반 '랜섬웨어 카르텔'의 등장이다. 이 모델에서 **중앙 플랫폼은 암호화 도구, 데이터 유출 인프라 및 협상 도구를 제공하고, 계열사들은 자체 브랜드로 공격을 수행하며 수익의 20%만 납부**한다. 이는 기존 RaaS의 30 ~ 40% 수익 배분보다 훨씬 유리한 조건이다. 이 모델은 Global Group, Anubis 등 랜섬웨어 생태계 전반으로 확산되었다.

공격자들은 **기술적 전문성이나 인프라 구축 부담 없이 '프랜차이즈' 형태로 공격 수행**이 가능해 진입 장벽이 낮아졌다. 그 결과, 공격 빈도와 다양성이 늘어났고, 공격자의 브랜드만으로는 공격 그룹 특정이 어려워졌다.

Key Point

- 랜섬웨어 생태계 파편화 - LockBit 등 대형 랜섬웨어 그룹 위축은 여러 소형 그룹 등장으로 이어져
- 2025년, 한국을 타깃한 공격 다수 발생 – 높은 IT 의존도, 낮은 보안 투자 비율 등 다양한 원인
- 화이트라벨 모델 기반 랜섬웨어 카르텔 – 계열사에 유리한 수익 배분, 손 쉬운 프랜차이즈 형태 공격 수행

2025년 사이버 위협 동향

공격 그룹 트렌드 - 다크웹 Top 9

4. 국가 배후 APT와 랜섬웨어 생태계 융합

2025년, **국가 배후 APT 그룹들이 민간 랜섬웨어 생태계에 본격 합류**했다. 국가 차원 사이버 스파이 활동과 금전적 사이버 범죄의 경계가 무너졌음을 의미한다.

Microsoft는 북한 APT 그룹 Moonstone Sleet이 자체 랜섬웨어 FakePenny 대신 러시아계 Qilin 랜섬웨어를 배포하기 시작했다고 밝혔다. 북한 배후 그룹 안다리엘(Andariel)이 Dtrack 백도어 설치 후 Play 랜섬웨어를 배포한 사건도 있었다. **APT 그룹이 초기 침투를 담당하고 RaaS 계열사가 갈취를 맡는 분업 구조**가 확인된 것이다.

APT 그룹의 고도화된 침투 기술과 RaaS의 효율적 갈취 메커니즘이 결합되면 공격 성공률과 피해 규모를 확대할 수 있다. 방어자의 분석은 어려워지고, 국제 사회의 제재국들이 체계적인 수익원으로 활용할 위험도 커진다.

5. 국제 공조 수사와 랜섬웨어 생태계 재편

2025년 수사 기관 간 국제 공조는 사이버 범죄 생태계에 큰 타격을 가했다. **일명 엔드게임 작전(Operation Endgame)은 2024년 5월 시작되어 2025년 5월 2단계로 확대되었고, DanaBot, Qakbot, Trickbot 등 주요 악성코드 인프라를 집중 타격했다.**

2025년 5월에만 300개 서버와 650개 도메인을 차단했다. 사이버 범죄자 20명에 대한 국제 체포영장을 발부했고, 약 405만 달러의 암호화폐 압수하면서 총 압수액은 약 2,453만 달러를 기록했다.

BreachForums 운영자 5명과 XSS 포럼 관리자를 체포하는 등 다크웹 인프라에도 타격을 가했다. 이는 **LockBit, RansomHub 등 대형 공격 그룹의 붕괴**로 이어졌다.

6. 랜섬웨어 그룹 내부 분열

2025년 랜섬웨어 생태계는 내부 신뢰가 무너지며 큰 타격을 받았다. 대표적인 사건은 5월 발생한 **LockBit 관리자 패널 해킹이다. 비트코인 지갑 주소 6만개, 피해자-계열사 협상 대화 기록 208개 및 계열사 계정 정보가 유출**된 것이다. Qilin과 Black Basta의 내부 도구와 채팅 로그가 유출되어 운영 방식이 경쟁자들에게 노출되기도 했다.

또한, 피해 기업들이 몸값을 지불하고도 제대로 작동하지 않는 복호화 도구를 받거나 아예 받지 못하는 경우도 많아졌다. 이로 인해, 랜섬웨어 계열사들의 운영자 불신이 고조되면서 독립적으로 활동하거나 경쟁 그룹으로 이동해 내부 정보를 유출하는 배신이 일상화되었다. 이러한 내부 분열이 소형 그룹 난립의 원인이 되었다.

Key Point

- 국가 배후 APT와 랜섬웨어 연합 – APT 그룹이 초기 침투, 랜섬웨어 그룹이 갈취 담당
- 국제 수사 기관 공조로 사이버 범죄 생태계 집중 타격 – LockBit, RansomHub 등 붕괴
- 랜섬웨어 그룹 간 해킹 및 내부 분열, 소형 그룹 난립으로 이어져

2025년 사이버 위협 동향

공격 그룹 트렌드 - 다크웹 Top 9

7. 공급망 공격 고도화 및 확대

2025년 공급망 공격은 2024년 대비 정교해지고 규모도 커졌다. **소프트웨어를 넘어 클라우드 서비스, MSP, 보안 솔루션 제공업체까지 확대**되고 있다. 가장 대표적인 사례는 공격 그룹 클롭(CLOP)의 Cleo MFT 플랫폼 제로데이 취약점 악용이다. 지난 1월, 단 한 번의 공격으로 182개 기업을 동시에 침투하는 대규모 공격을 감행한 바 있다. 또한, 클롭에 의한 Oracle EBS 취약점 악용도 증가했다. CISA는 Oracle Cloud 자격 증명 유출로 인한 연쇄 침해 위험을 공식 경고했다.

공격 그룹 DragonForce와 Scattered Spider는 클라우드 MSP를 직접 노렸다. SimpleHelp 취약점을 악용하고, 소셜 엔지니어링 기법으로 IT 관리자를 속여 원격 접근 권한을 확보했다. 그 결과, **하나의 MSP 침해로 수십 개 고객사가 동시에 피해를 입는 '연쇄 공급망 공격'이 실현**됐다.

8. 다크웹 생태계 불안정성 심화

2025년 다크웹 생태계는 전례 없는 불안정성을 겪었다. 기존 수사 기관 대 범죄 조직 구도에서 범죄 조직 간 공격까지 일상화되면서 생태계 자체가 혼돈에 빠졌다.

지난 3월, **공격 그룹 DragonForce는 경쟁 그룹 RansomHub의 데이터 유출 사이트(Data Leak Site, DLS)를 해킹**했다. 4월에는 BlackLock과 Mamona의 DLS도 디페이스(deface)하고 내부 채팅 로그와 백엔드 설정을 유출했다. 연구자들은 DragonForce가 경쟁 그룹의 AI 생성 백엔드 코드 취약점을 악용했다고 밝혔다. 흥미로운 점은 Everest와 LockBit 사이트가 동일한 메시지 "Don't do crime CRIME IS BAD xoxo from Prague"로 디페이스 되었다는 것이다. 이는 공격 그룹에 대한 조직적 공격 가능성을 시사한다.

9. 지정학적 갈등 연계 핵티비스트 활동 급증

2025년에는 지정학적 갈등의 사이버 공간 확산이 격화되었다. 친러시아 공격 그룹 NoName057(16)은 NATO 국가들을 지속적으로 공격했다. Dark Storm Team은 NATO 전력 인프라를 공격하여 물리적인 영향을 가했다. 반대 진영에서는 IT Army Ukraine이 러시아 통신사 UIS에 디도스 공격을 감행해 72시간 동안 서비스 장애를 일으켰다.

중동에서는 이란-이스라엘 전쟁이 심화되면서 핵티비스트 활동이 증가했다. Holy League와 313 Team 등의 공격 그룹이 이스라엘 병원과 중앙은행을 공격했다. #OpIsrael 2025 캠페인은 대규모 사이버 공격을 예고했으며, 실제 의료 기관들이 디도스 공격을 받기도 했다. 이 밖에, 인도-파키스탄 갈등 국면에서도 Indian Cyber Force가 파키스탄 은행과 경찰청 해킹을 주장하기도 했다.

Key Point

- 공급망 공격, 소프트웨어를 넘어 클라우드, MSP 등으로 확대 – 하나의 기업 침해로 수 많은 고객사 타격
- DragonForce, 경쟁 그룹 RansomHub의 DLS 해킹 – 공격 그룹 간 조직적 공격 가능성
- 러시아 vs 우크라이나+NATO, 이란-이스라엘, 인도-파키스탄 등에서 핵티비스트 활동 급증

2025년 사이버 위협 동향

공격 그룹 트렌드 – APT: 전체 동향

2025년은 지난해와 마찬가지로 **북한 APT 그룹들의 활동이 활발**했다. 가장 많이 언급된 그룹은 라자루스(Lazarus)로 총 31 건의 정보가 공개되었다. 이 그룹은 여러 하위 그룹이 있어 언급이 많았고, 하위 그룹을 구분할 경우 횟수는 달라질 수 있다. 다음으로 김수키(Kimsuky)가 27건, TA-RedAnt가 17건 언급되었다.

중국과 러시아 APT 그룹의 활동도 활발했다. Mustang Panda 11건, APT28 10건, Gamaredon이 10건의 정보 공개가 있었다. 인도와 파키스탄 APT 그룹의 활동도 꾸준했는데, **지정학적 갈등 고조** 때문으로 보인다. 파키스탄 Transparent Tribe가 17건으로 두드러졌다.

같은 기간 APT 그룹 활동을 국가 별로 집계한 결과, 북한이 86건으로 선두를 기록했다. 중국이 27건, 러시아와 인도가 18건, 파키스탄이 17건으로 뒤를 이었다. 이란은 9 건으로 비교적 적었다. 이 주요 국가들 외 공격 그룹들도 32건이 있었다. 글로벌 위협 환경에서 다양한 국가 기반 그룹이 활발히 활동하고 있음을 알 수 있다.

보고서 공개 횟수가 적다고 해서 활동이 적다고 단언할 수 없다. 은밀하게 활동하는 APT 그룹들은 관련 정보가 확인되지 않는 경우도 있다. 또한, 정부 기관에 대한 공격은 정책적으로 공개하지 않기도 한다.

배후	APT 그룹	10월	11월	12월	1월	2월	3월	4월	5월	6월	7월	8월	9월
북한 (86건)	Andariel	2		1	1	1							
	Kimsuky	3	4	6	2	2	2			2	2	2	2
	Konni	2					2	1	1				
	Lazarus	5	2	2	4	3	4	1		2	2	4	2
	TA-RedAnt	2	1		2	1	4		1		2	3	1
중국 (27건)	APT41	1	1					1	1	1	1	1	
	MirrorFace		2		1		1	1					
	Mustang Panda				2	2		3		1			3
	Salt Typhoon		1			1			1	1			
러시아 (18건)	APT28	2	1						3	1	2		1
	Gamaredon			4			1	1			1	1	
이란 (9건)	Charming Kitten		2	1					1				
	MuddyWater		1			1					1	1	1
인도 (18건)	Bitter	1	1	1					1	1		1	
	SideWinder	1					1		2			1	2
	Viceroy Tiger	1	1		1	1					1		
파키스탄 (17건)	Transparent Tribe		1	1			1	1	4	4	2	3	

[표] 국가별 APT 그룹 월별 활동 건수 (2024년 10월 ~ 2025년 9월)

2025년 사이버 위협 동향

공격 그룹 트렌드 – APT: 전체 동향

APT 그룹들은 지정학적 갈등 지역을 중심으로 활동한다. 한국-북한, 인도-파키스탄, 중국-동남아시아, 러시아-우크라이나, 이스라엘-중동 등에서 사이버 공격이 집중되는 이유다. **정부, 군, 외교, 방산, 금융, 에너지, 통신, 교육, NGO 등 고가치 조직을 표적**으로 삼는다.

초기 침투 방식은 이메일 기반 스피어 피싱이 여전히 주를 이룬다. LNK, ISO, MSC, PDF, CHM, ZIP 등 다양한 포맷의 악성 첨부파일이 사용된다. 사회공학 기법을 활용해 가짜 채용, 정책 문서, 보안 알림, 공문 등으로 위장하며, 맞춤형 미끼 문서와 이벤트를 사용한다.

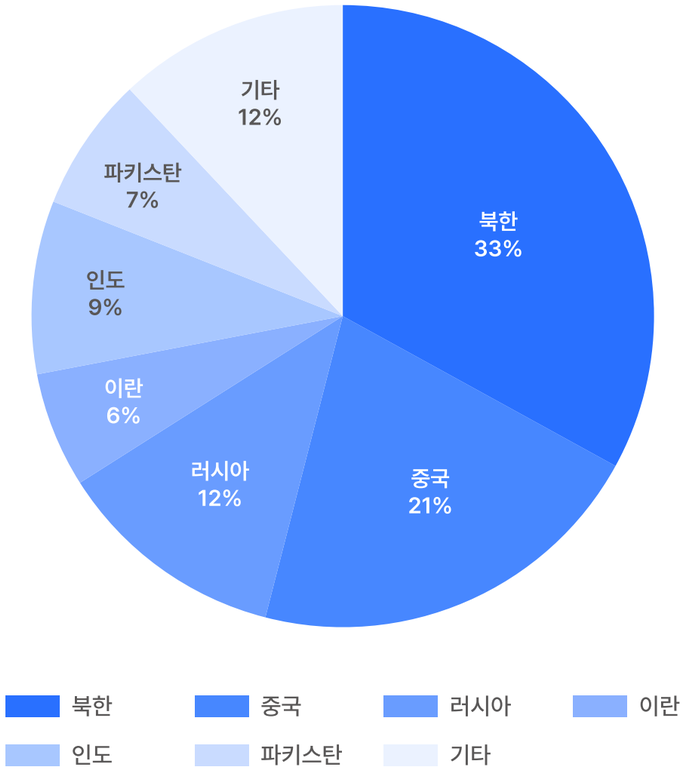
여기에, **다양한 악성코드와 정상 도구를 사용**한다. 악성코드는 주로 원격 제어, 백도어, 키로거, 정보 탈취형 악성코드를 활용한다. PowerShell, VBS, Batch 스크립트, 오픈소스 도구(Sliver, Mimikatz 등)도 공격 과정에 포함된다. 멀티 플랫폼 캠페인을 위해 윈도우, 리눅스, macOS, 안드로이드용 악성코드를 상황에 맞춰 활용한다.

또한, 이들은 지속성 유지, 탐지 회피 등 고도화된 기법으로 무장하고 있다. 다음은 APT 그룹들이 주로 사용하는 공격 기법이다.

- 작업 스케줄러/레지스트리 등록
- 서비스/객체 모델(COM) 하이재킹
- UAC(User Account Control) 우회
- 파일리스 실행
- DLL 사이드로딩
- JPEG 스테가노그래피
- VM/샌드박스 탐지 회피
- 로그 삭제

GitHub, Dropbox, Google Drive, Telegram, Cloudflare, Outlook 등 정상 서비스와 클라우드 인프라를 활용해 C2 통신 및 데이터 유출을 수행하기도 한다. 그리고, DNS/DoH, TOR, VPN 등을 활용해 공격 활동을 은닉한다.

이들의 최신 공격 기법 트렌드로는 AI를 이용한 딥페이크, MFA 우회(AiTM, OTP 탈취), 공급망 공격, 워터링 홀, IoT 장비 침투, 공격 자동화 및 대량화, 정상 서비스 위장 등이 있다. 공개된 도구와 자체 개발 악성코드를 혼합해 사용하고 있다.

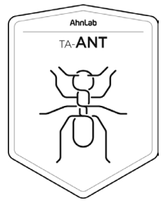


[그림] 국가별 APT 그룹 활동 비중 (2024년 10월 ~ 2025년 9월)

2025년 사이버 위협 동향

공격 그룹 트렌드 – APT: 북한

북한 APT 그룹은 정치·외교·금융·암호화폐 등 다양한 산업을 대상으로 금전적 이익과 정보 수집을 노린다. 스피어 피싱, 공급망 공격, 멀티 플랫폼 악성코드, 권한 상승, MFA 우회 등 고도화된 공격 기법을 활용하는 것이 특징이다.



북한

Kimsuky

2025년, Kimsuky 그룹은 한국을 중심으로 다양한 국가와 산업을 겨냥한 고도화된 사이버 공격을 수행했다. **강연 의뢰서나 인터뷰 요청을 위장한 스피어 피싱을 통해 ISO, LNK, MSC 등 다양한 파일을 유포**했다. MSC 파일을 활용한 구글 드라이브 기반 피싱과 VbsEdit 서명 악용이 특징적이었다.

이메일 피싱은 ▲mail.ru ▲내도메인.한국 등을 활용해 위장했다. ISO 파일과 악성 한글 문서를 통한 공격도 지속했다. 깃허브, 페이스북, 텔레그램 등 다양한 채널을 활용한 다단계 공격과 AI 기반 위조 신분증 사용도 새롭게 확인되었다. 아울러, PebbleDash, RDP Wrapper, Proxy 악성코드를 통해 원격 제어를 강화했다. 일본 대상 공격에서는 AsyncRAT 변종을 사용하기도 했다.

Kimsuky는 여러 하위 그룹이 존재한다. Larva-24005는 Kimalogger를 이용해 사용자 키 입력 내용을 수집했다. Larva-24009는 한국 사용자 대상 LNK 기반 공격을 수행했고 QuasarRAT, UltraVNC 등을 활용했다. Larva-25001는 정상 문서로 위장한 LNK 파일로 HttpSpy, Memload 등의 악성코드를 감염시켰다.

Andariel

Andariel 그룹은 미국과 한국을 대상으로 금전적 목적의 공격을 지속하고 있다. 2024년 미국 법무부의 기소 이후에도 활동을 멈추지 않았다. 미국 민간 기업을 대상으로 Preft 및 Nukebot 백도어를 활용한 침투를 수행한 바 있다. Sliver, Chisel, PuTTY 등 오픈소스 도구와 키로거, Mimikatz를 활용한 자격 증명 탈취 기법을 활용했다. Play 랜섬웨어 인프라를 통해 랜섬웨어를 배포하기도 했다.

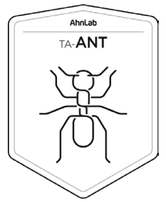
한국에서는 자산 관리 및 문서 중앙화 솔루션을 대상으로 ModeLoader 및 SmallTiger 악성코드를 배포했다. RDP 접근 및 숨김 계정 생성을 통해 장기적인 침투 기반을 마련했다. Apache Tomcat 취약점을 이용한 웹셸 설치, Advanced Port Scanner를 통한 네트워크 탐색 등도 확인되었다. 특히, RID 하이재킹 기법을 통해 낮은 계정 권한을 관리자 권한으로 상승시키고, CreateHiddenAccount 도구를 활용해 백도어 계정을 추가한 것은 주목할만한다. PsExec를 통한 원격 명령 실행, REGINI를 활용한 SAM 레지스트리 조작 등 정교한 내부 침투 기술도 사용했다. 한국 보안 기업 S사의 인증서를 탈취해 악성코드에 서명하는 방식으로 신뢰 기반을 악용하기도 했다.

Key Point

- Kimsuky, 스피어 피싱을 통해 다양한 악성코드 유포, 위장 도메인 및 악성 한글 문서 활용 지속
- Kimsuky는 여러 하위 그룹을 두고 있어 더 다양한 사이버 공격 감행
- Andariel, 한국 자산 관리 및 문서 중앙화 솔루션을 대상으로 ModeLoader 및 SmallTiger 악성코드 배포

2025년 사이버 위협 동향

공격 그룹 트렌드 – APT: 북한



북한

Konni

Konni는 작년 말부터 2025년까지 한국과 우크라이나를 포함한 고가치 표적을 대상으로 **LNK 파일 기반 스피어 피싱 공격을 집중적으로 수행**했다. 공격은 세무·시장 분석 등 한국어 키워드를 활용한 사회공학적 기법과 함께 PowerShell 및 AutoIt 스크립트를 통해 악성 페이로드를 은밀히 실행하는 방식으로 구성되었다. 특히, ZIP 압축파일 내부에 위장된 바로가기 파일을 삽입해 사용자가 실행할 때 다단계 로딩되도록 하여 악성코드를 배포했다.

Konni는 **워드프레스(WordPress) 기반 C2 인프라를 활용해 Konni RAT, Amadey, Lilith RAT, AsyncRAT 등 다양한 원격 제어형 악성코드를 배포**했다. 감염 지속성 유지를 위해 Avast 백신 탐지 우회, 시작 디렉터리 자동 실행, 숨김 디렉터리 생성, 레지스트리 키 등록 등의 기법을 사용했다. 또한, 대량의 악성 샘플을 자동 생성해 다양한 시점에 배포하고, 탐지 회피를 위해 난독화와 암호화를 결합한 페이로드를 사용했다.

사회공학적 측면에서는 한국 정부 사칭 이메일과 우크라이나 정부 대상 공격이 확인됐다. PHPMailer를 활용해 발신자 정보를 위장하고, 정상 문서와 악성 스크립트를 결합해 피해자가 신뢰하도록 했다. Konni는 단순 정보 탈취를 넘어 시스템 제어, 자격 증명 수집, 네트워크 정찰을 수행하고, 장기 침투를 위한 지속성 확보 전략을 강화했다. 이러한 활동은 북한 연계 사이버 작전의 일환으로 보이며, 향후 더 정교한 공격이 확산될 가능성이 높다.

Lazarus

Lazarus 그룹은 2024년부터 2025년까지 암호화폐, 금융, IT, 국방 등 다양한 산업을 대상으로 공격을 확대했다. 특히 **macOS와 리눅스까지 지원하는 멀티 플랫폼 악성코드를 다수 개발**했다. Electron과 Tauri 프레임워크를 활용한 새로운 백도어 및 정보 탈취 도구를 선보이기도 했다. 주요 악성코드는 InvisibleFerret, BeaverTail, OtterCookie, CookiePlus, FrostyFerret 등이 있다. 해당 악성코드들은 키로깅, 클립보드 감시, 브라우저 캐시 및 암호화폐 지갑 정보 탈취 기능을 포함한다. 공격 기법은 공급망 공격과 워터링 홀 기법이 두드러졌다.

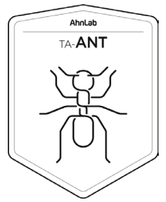
한국에서는 **소프트웨어 취약점을 악용한 Operation SyncHole 캠페인을 통해 최소 6개 산업 조직을 침해했다.** 또한, npm, PyPI, GitHub 등 오픈소스 생태계를 통해 악성 패키지를 배포하여 개발자와 기업을 감염시켰다. 사회공학적 기법도 진화하여 ClickFix & ClickFake Interview 등 가짜 면접 캠페인과 고도의 심리 전술로 피해자를 유인했다. 기술적으로는 다단계 난독화, VMProtect·Confuser 난독화, 확장 속성(xattr) 은닉, JPEG 스테가노그래피, 파일리스 실행, DLL 사이드 로딩, TxF 기반 Process Doppelganging 등 탐지 회피 및 지속성 확보 기술이 눈에 띄었다. 또한, MFA 우회, OTP 탈취, 클라우드 인프라 악용 등도 주요 변화로 나타났다.

Key Point

- Konni, LNK 파일 기반 스피어 피싱 공격 집중 수행
- 워드프레스 기반 C2 인프라를 활용해 다양한 원격 제어형 악성코드 배포
- Lazarus, macOS와 리눅스까지 지원하는 멀티 플랫폼 악성코드 다수 개발
- 한국에서 소프트웨어 취약점 활용 Operation SyncHole 캠페인을 통해 최소 6개 산업 조직 침해

2025년 사이버 위협 동향

공격 그룹 트렌드 – APT: 북한



북한

TA-RedAnt

TA-RedAnt는 2024년부터 2025년까지 한국 포함 동아시아, 남아시아, 중동, 유럽 등 다양한 지역으로 공격을 확대했다. 해당 지역에서 **정치·외교·국방·금융·의료·에너지·교육 등 다양한 산업을 표적**으로 삼았다. TA-RedAnt 역시 ScarCruft(APT37), SideWinder, Transparent Tribe(APT36), UNC3886(Fire Ant) 등 여러 하위 그룹을 포함한다.

스피어 피싱, 워터링 홀, 채용 위장, 악성 문서(HWP, PDF, ISO, LNK 등), 악성 설치파일 및 압축파일(EGG, ZIP), 클라우드 링크, Github/Dropbox 기반 C2 등 다양한 공격 기법을 사용한다. 특히, JPEG 이미지에 악성코드를 숨기는 스테가노그래피, 파일리스 실행, DLL 사이드로딩, TxF 기반 Process Doppelganging, Transacted Hollowing 등 고도화된 은폐 및 지속성 확보 기술을 새롭게 도입했다.

새롭게 확인된 내용으로는 Rust 기반 백도어(Rustonotto, CHILLYCHINO), VCD 랜섬웨어, PubNub/Ably 메시징 C2, LLM 기반 악성코드(LAMEHUG), MFA 우회(AitM, OTP 탈취), AI 이미지·음성 변조, Python 코드 난독화 등이 있다. 또한 .desktop 파일을 활용한 리눅스 공격, WebSocket 기반 C2, 구글 드라이브를 통한 페이로드 전달 등 멀티 플랫폼 공격이 증가한 것도 특징이다.

이들의 사회공학 기법도 진화를 거듭하고 있다. 실존 인물 사칭, 학술행사 및 뉴스레터 위장, 메신저 단톡방 활용, 링크 없는 이메일 등으로 의심을 최소화한다. 공격 자동화와 탐지 회피 능력도 강화했다. 정상 문서·앱·서명 프로그램 위장, 클라우드·정상 서버 기반 C2 구축, 다단계 복호화·난독화, 자가 삭제 및 임시 폴더 은닉 등의 기술도 사용한다.

TA-RedAnt는 다양한 악성코드와 도구를 활용해 자격 증명, 시스템 정보, 암호화폐, 문서, 오디오, USB/MTP 데이터 등을 탈취했다. **일부 피해 조직에는 랜섬웨어를 감염시켜 금전적 피해**를 입히기도 했다. 앞으로도, 지속적으로 공격 기법을 진화 시키며 주요 글로벌 위협으로 자리매김할 전망이다.

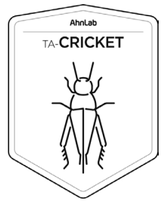
Key Point

- 정치, 외교, 국방, 에너지 등 다양한 산업 표적
- 스피어 피싱, 악성 설치파일, 클라우드 기반 C2 등 다양한 공격 기법 사용
- JPEG 스테가노그래피, 파일리스 실행, DLL 사이드로딩 등 은폐 및 지속성 확보 기술 고도화
- 일부 피해 조직에는 랜섬웨어를 감염시켜 금전적 피해를 입힌 사례 존재

2025년 사이버 위협 동향

공격 그룹 트렌드 – APT: 중국

중국 APT 그룹은 정부 기관, 외교, 군사, 산업 분야를 대상으로 장기/전략적인 정보 수집 및 감시를 수행한다. 제로데이 취약점, 공급망 공격, 멀티 플랫폼 악성코드, 클라우드 인프라 악용 등 고도화된 기술을 활용하고, 탐지 회피 능력을 강화한다. 사회공학 기법과 AI 기반 자동화 도구를 결합해 맞춤형 피싱 및 공격 캠페인을 대량 실행하고 지정학적/경제적 이익을 동시에 추구한다.



중국

APT41

APT41은 지난 1년 간 글로벌 정부 기관 및 산업을 대상으로 고도화된 공격을 지속했다. Google Calendar를 악용한 TOUGHPROGRESS 캠페인, ClickOnce 기반 OneClik 공격, RunnerBeacon 백도어, Anatsa(TeaBot) 트로이 목마 등 다양한 기법을 활용해 정부 기관, 에너지·석유·가스 산업, 금융 기관을 집중 공격했다. 또한, 일본 기업을 대상으로 정찰 도구와 암호화된 웹셸을 배포하고, 아프리카 정부 IT 인프라를 겨냥한 공격도 병행했다. 특히 2024년 7월에는 **Fortinet VPN 클라이언트(FortiClient) 인증 후 메모리에 남은 자격 증명을 추출하는 제로데이 취약점을 악용**한 바 있다.

워드프레스(WordPress) 기반 C2 인프라, 암호화된 HTTPS 트래픽, TLS 프로토콜 위장을 통해 탐지를 회피했다. 또한, 공격 자동화를 위해 대량의 악성 샘플을 생성해 여러 시점에 걸쳐 배포했다. 공급망 공격과 모바일 플랫폼 침투를 동시에 수행하는 것이 특징이다. 특히, iOS와 안드로이드 기기에서 정보 탈취를 위한 맞춤형 악성 앱을 배포하고, 클라우드 서비스 계정을 탈취해 기업 내부망으로 공격을 확산시킨다. 공격 대상의 언어와 문화적 특성을 반영한 사회공학 기법을 사용하며, AI 기반 자동화 도구를 활용해 피싱 콘텐츠를 대량 제작하는 정황도 포착했다.

MirrorFace

MirrorFace는 2024년 6월 이후 일본을 중심으로 대만, 인도, 유럽 외교 기관까지 공격 대상을 확장했다. **초기 침투는 스피어 피싱 이메일과 OneDrive 링크를 통한 ZIP 파일 유포 방식**으로 이루어진다. ZIP 내부에는 매크로 문서(ROAMINGMOUSE), 바로가기 파일, SFX 실행 파일 등이 포함된다. SSL VPN 및 파일 저장 서비스의 제로데이 취약점(CVE-2023-28461, CVE-2023-27997 등)을 악용해 초기 접근을 시도하고, MirrorStealer, Lodeinfo, Cobalt Strike를 통해 자격 증명 탈취 및 AD(Active Directory) 서버 침투를 수행한다. 악성코드는 ANEL 백도어 최신 버전과 NOOPDOOR, NOOPLDR 등 신규 악성코드를 활용했다. 공격 자동화를 위해 PowerShell 스크립트와 WMI 기반 명령 실행을 결합하기도 했다. 그리고, Base64/HEX 인코딩, WMI 실행, UAC 우회, 샌드박스 회피 등 탐지 회피 기법도 강화했다.

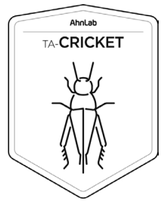
일본 내 정치인 및 언론인을 대상으로 한 맞춤형 피싱 캠페인도 진행했다. 공격 인프라로 클라우드 서비스와 CDN(Content Delivery Network)을 활용해 정상 트래픽으로 위장했다. 일본 경찰은 이들의 활동이 조직적 정보 수집 시도일 가능성이 높다고 경고했다.

Key Point

- APT41, FortiClient 자격 증명을 추출하는 제로데이 취약점 악용 사례 보고
- 워드프레스 기반 C2, 암호화된 HTTPS 트래픽, TLS 프로토콜 위장 등을 통해 탐지 회피
- MirrorFace, 스피어피싱 등으로 초기 접근 및 제로데이 취약점 활용으로 침투 시도
- 일본을 중심으로 정치인 및 언론인 대상 맞춤형 피싱 캠페인 진행

2025년 사이버 위협 동향

공격 그룹 트렌드 – APT: 중국



중국

Mustang Panda

Mustang Panda는 2024년부터 2025년까지 동남아시아, 동북아시아, 유럽, 남미 등 다양한 지역의 정부, 외교, 군사, NGO, 학계 등을 대상으로 공격을 확대했다. **스피어 피싱 이메일과 악성 문서(LNK, CHM, OneNote, PDF, HTML, ISO 등)를 활용해 초기 침투를 시도했다. HTML Smuggling, USB 웜(SnakeDisk), 클라우드 기반 피싱 등 다양한 공격 기법**을 도입했다.

악성코드는 PlugX, TONESHELL, Bookworm, PUBLOAD, MQsTTang, CCoreDoor, ShadowPad 등 다양한 백도어와 RAT를 사용했다. StarProxy, PAKLOG/CorKLOG, SplatCloak, Yokai 등 신규 도구도 다수 확인되었다. 이들은 측면 이동, 키로깅, EDR 우회, USB 전파 기능을 갖추고 있다. 탐지 회피 기법도 고도화 했다. 정상 프로세스(MAVInject.exe 등)를 통한 DLL 인젝션, WriteProcessMemory 기반 반사 DLL 인젝션(Reflective DLL Injection), FakeTLS 및 TLS-like 헤더를 활용한 C2 트래픽 은닉, Cloudflare CDN·Google Drive·Box 등 클라우드 인프라를 통한 페이로드 전달이 주요 특징이다. 사회공학적 기법도 강화했다. 대만 대선, 몽골 홍수, ASEAN 회의, 티베트 행사 등 지역 이슈를 활용한 맞춤형 미끼 문서를 사용했다. WebSocket C2, AES/DES 기반 다단계 암호화, Kavach OTP 탈취를 통한 MFA 우회 등도 새롭게 등장한 기법이다.

Salt Typhoon

Salt Typhoon은 2024년부터 2025년까지 미국, 아시아, 중동, 아프리카 지역 통신사·정부·군사·NGO를 대상으로 장기적인 감시 및 정보 수집 활동을 수행했다. **공개된 서버 및 네트워크 장비 취약점(CVE-2018-0171, CVE-2023-20198 등)을 악용해 초기 접근을 확보했다.** 내부에서는 WMIC.exe, PSEXEC.exe를 활용한 측면 이동을 수행했다. 공격자는 AD 환경 권한 상승을 위해 Kerberos 티켓 조작과 Pass-the-Hash 기법을 사용했다. 그리고, **탐지 회피를 위해 정상 관리 도구를 악용하는 Living-off-the-land(LOTL) 전략을 강화했다.**

악성코드는 GHOSTSPIDER, SNAPPYBEE, MASOL RAT를 주로 사용했다. 특히, GHOSTSPIDER는 모듈형 설계와 TLS 암호화를 통해 분석을 어렵게 했다. 또한, SNAPPYBEE는 클라우드 API 호출을 통해 데이터 유출을 수행하고, MASOL RAT는 파일리스 실행과 PowerShell 난독화를 결합해 탐지를 회피했다. 2025년 5월에는 Commvault Metallic SaaS 플랫폼의 제로데이 취약점(CVE-2025-3928)을 악용해 Microsoft 365 환경을 침해했다. 이 밖에, ShadowPad·SoftEther VPN을 통한 C2 은닉, CAB 파일을 활용한 DEMODEX Rootkit 설치 방식 개선, 그리고 정상 프로세스 인젝션을 통한 지속성 확보 기법을 도입했다. 공격 인프라는 CDN과 클라우드 스토리지를 활용해 정상 트래픽으로 위장했다. 공격 자동화를 위해 Python 기반 스크립트와 AI 생성 피싱 콘텐츠를 결합한 정황도 포착되었다.

Key Point

- MustangPanda, 스피어 피싱 이메일과 악성 문서를 활용해 초기 침투. HTML Smuggling 등 다양한 공격 기법 도입
- 기존 도구와 인프라를 재활용하면서 새로운 악성코드와 은닉 기술을 도입해 정교함 강화
- Salt Typhoon, 공개된 서버 및 네트워크 장비 취약점을 활용해 초기 접근 확보
- 탐지 회피를 위한 LOTL 전략 강화, 악성코드 개발, 트래픽 위장, 공격 자동화 등 다양한 전술 고도화 진행

2025년 사이버 위협 동향

공격 그룹 트렌드 – APT: 러시아

러시아

러시아 APT 그룹은 지정학적 갈등을 활용해 정부, 군사, 외교, 전략 기관을 대상으로 장기적/조직적인 공격을 수행한다. 이메일 피싱, 공개 취약점 악용, 클라우드 인프라 기반 C2 은닉, 파일리스 실행 등 고도화된 기법을 사용하며, 탐지 회피 능력이 탁월하다. 심리전과 정치적 영향력 확대를 위해 맞춤형 캠페인을 전개하며, 정보 탈취를 넘어 기반 시설 공격까지 도모한다.

APT28

APT28은 우크라이나, NATO, 동유럽을 중심으로 정부, 군사, 방위 산업, 기술 분야 대상 공격을 지속했다. 지정학적 갈등을 활용해 맞춤형 피싱 캠페인을 전개했으며, **러시아-우크라이나 전쟁 및 NATO 정상회의 관련 문서를 미끼**로 사용했다. 초기 침투는 이메일 피싱과 취약점(CVE-2023-38831, CVE-2023-23397 등) 악용이 두드러졌다. Outlook, Roundcube, Zimbra 등 이메일 서버 취약점도 적극 활용했다.

LLM 기반 악성코드(LAMEHUG)를 도입해 명령 자동 생성과 정보 수집을 시도했다. MFA 우회(AiTM), COM Hijacking, UAC 우회 등 지속성 확보 기술을 강화했다. 또한, Google Drive 등 클라우드 인프라를 활용해 C2 통신을 은닉하고, 정상 트래픽으로 위장해 탐지를 회피했다. Python 스크립트와 PowerShell 난독화를 결합해 악성 샘플을 대량 생성하는 방식으로 공격을 자동화했다. 주요 악성코드는 HeadLace, GooseEgg, MASEPIE가 확인되었다. 이들은 자격 증명 탈취, 네트워크 정찰, 측면 이동 기능을 포함한다. 또한, Cobalt Strike, Sliver 등 오픈소스 공격 프레임워크를 활용해 공격 체인을 고도화했다. 최근에는 HTML Smuggling, 파일리스 실행, JPEG 스테가노그래피를 통한 페이로드 은닉 기법도 도입했다.

Gamaredon

Gamaredon 그룹은 우크라이나 및 러시아어권 사용자를 대상으로 고도화된 스피어 피싱과 정보 수집 활동을 수행한다. 초기 침투는 LNK, HTA, XHTML 파일을 활용한 피싱 캠페인을 통해 이루어졌다. 파일 실행 시, PowerShell 기반 악성코드가 로드되어 시스템 정보를 수집하고 추가 페이로드를 다운로드했다. Cloudflare Tunnels, DNS over HTTPS(DoH) 등 외부 인프라를 이용해 C2 탐지를 회피했다. 그리고, 공격 자동화를 위해 Python 스크립트와 PowerShell 난독화를 결합했다. **신규 악성코드인 GammaDrop, GammaLoad, GammaSteel은 난독화, 레지스트리 은폐, USB 드라이브 무기화 등 정교한 기법을 사용**했다. 특히, GammaSteel은 파일리스 실행과 다단계 암호화를 통해 분석을 어렵게 했다.

모바일 플랫폼 공격도 강화했다. BoneSpy, PlainGnome 등 **안드로이드 감시 악성코드를 통해 러시아어권 사용자를 타깃했다.** 일부는 삼성 녹스(Knox)로 위장해 기업에 침투했다. 악성 앱은 통화 기록, 메시지, 위치 정보를 수집하고 카메라·마이크를 원격 제어했다. 2025년에는 우크라이나 주둔 서방 군사를 대상으로 PowerShell 기반 정보 탈취를 수행했다. 이들은 단순 스파이 활동을 넘어 군사·외교 정보 수집과 심리전 목적의 공격을 병행한다. 러시아 연방보안국(FSB) 산하 제18정보보안센터와의 연계도 추정된다.

Key Point

- APT28, 피싱 캠페인 전개, 러시아-우크라이나 전쟁 및 NATO 정상회의 관련 문서를 미끼로 사용
- LLM 기반 악성코드(LAMEHUG)를 도입해 명령 자동 생성과 정보 수집 시도
- Gamaredon, 난독화, 레지스트리 은폐, USB 드라이브 무기화 등 정교한 기법을 수행하는 악성코드 사용
- 모바일 플랫폼 공격 강화, 안드로이드 감시 악성코드를 통해 러시아어권 사용자 타깃

2025년 사이버 위협 동향

공격 그룹 트렌드 – APT: 이란

이란 APT 그룹은 중동과 유럽을 중심으로 외교, 언론, 인권 단체 및 정부 기관 대상 장기 공격을 수행한다. 스피어 피싱, HTML Smuggling, 파일리스 실행, MFA 우회, OTP 탈취 등 고도화된 기법을 사용한다. 클라우드 인프라와 스테가노그래피를 통해 탐지 회피 능력도 강화했다. 안드로이드 악성코드와 AI 기반 피싱 콘텐츠를 결합해 모바일 기기까지 공격 범위를 확대했다.

이란

Charming Kitten

Charming Kitten은 중동과 유럽을 중심으로 외교, 언론, 인권 단체를 표적으로 공격을 수행했다. 초기 침투는 사회공학 기법 기반 피싱과 악성 문서 배포를 활용했다. **LNK 파일과 PowerShell을 결합한 다단계 로딩 방식도 새롭게 추가**했다. JPEG 이미지 내 스테가노그래피를 통한 악성코드 은닉과 탐지 회피를 위해 파일리스 실행 기법을 적극 활용했다.

Charming Kitten은 **MFA 우회와 OTP 탈취 기술을 통해 인증 체계를 무력화**하고, AiTM(Adversary-in-the-Middle) 기반 피싱 사이트를 운영해 실시간으로 세션을 하이재킹 했다. 클라우드 기반 C2 통신은 Dropbox, Google Drive, Telegram API를 활용해 정상 트래픽으로 위장했다. 그리고, TLS 암호화와 DNS over HTTPS(DoH)를 결합해 네트워크 탐지를 회피했다. 악성코드는 POWERSTATS, NokNok, CharmPower를 주로 사용했고, 키로깅, 브라우저 쿠키 탈취, 시스템 정보 수집 기능이 포함된다.

MuddyWater

MuddyWater는 중동, 유럽, 남아시아 지역 정부, 외교, 통신, 산업 조직을 대상으로 공격을 지속했다. 이들은 **Living-off-the-land(LOTL) 기법을 적극 활용해 PowerShell, MSHTA 등 정상 도구로 초기 침투와 명령 실행을 수행**했다. 스피어 피싱 이메일을 통해 악성 LNK 파일을 배포하고 정상 문서와 악성 스크립트를 결합해 탐지를 회피했다. 또한, Ligolo, SimpleHelp, Venom Proxy 등 **오픈소스 도구를 활용한 C2 통신을 확대했다. VPN과 원격 관리 도구(RMM)를 통한 내부 확산**도 확인되었다. 특히, BugSleep(MuddyRot) 백도어를 사용해 기존 Atera RMM을 대체했고, 공격 자동화를 위해 Python 기반 스크립트와 PowerShell 난독화를 결합했다. 파일리스 실행과 메모리 내 악성코드 로딩 방식도 이들 공격의 주요 특징이다. 탐지 회피는 정상 프로세스 인젝션과 UAC 우회 기법을 사용했다.

주요 악성코드는 MuddyC2Go, BugSleep, SimpleHelp RAT가 확인되었다. 이 악성코드들은 자격 증명 탈취, 키로깅, 네트워크 정찰 기능을 포함한다. 또한, DNS over HTTPS(DoH)와 TLS 암호화를 활용해 C2 트래픽을 은닉하고, 클라우드 서비스(Google Drive, Dropbox)를 통해 페이로드를 전달했다. 공격 인프라의 경우, CDN과 정상 웹사이트를 악용한 워터링 홀 기법을 사용했다.

Key Point

- Charming Kitten, 사회공학 기법 기반 피싱과 악성 문서 배포 - LNK 파일과 PowerShell을 결합한 다단계 로딩 방식 새롭게 추가
- MFA 우회와 OTP 탈취 기술을 통해 인증 체계 무력화
- MuddyWater, LOTL 기법을 활용해 정상 도구로 초기 침투와 명령 실행
- 오픈소스 도구를 활용한 C2 통신 확대 및 VPN과 원격 관리 도구를 통한 내부 확산

2025년 사이버 위협 동향

공격 그룹 트렌드 – APT: 인도

인도

인도 APT 그룹은 남아시아와 중동 지역 정부, 군사, 외교 기관 대상 장기적인 공격을 수행한다. 스피어 피싱, HTML Smuggling, PowerShell 난독화, DLL 사이드 로딩 등 고도화된 기법을 활용하며, 클라우드 인프라와 스테가노그래피를 통해 탐지를 회피한다. 안드로이드 악성코드를 사용해 멀티 플랫폼 공격을 수행하고, AI 기반 피싱 콘텐츠 결합 등을 통해 사회공학적 기법도 고도화하고 있다.

Bitter

Bitter는 남아시아와 중동 지역 정부, 군사, 외교 기관을 지속적으로 공격했다. 초기 침투는 악성 문서와 LNK 파일을 활용한 이메일 공격을 통해 이루어졌다. **HTML Smuggling과 PowerShell 기반 악성코드를 새롭게 사용해 탐지 회피 능력을 강화**했다. 정상 문서와 악성 스크립트를 결합해 피해자의 신뢰를 확보하고, 다단계 로딩 방식으로 페이로드를 은닉했다.

Bitter는 **안드로이드 악성코드를 활용해 모바일 기기까지 공격 범위를 확대했다. 이들의 악성 앱은 금융 정보, 메시지, 위치 데이터를 탈취하고 카메라·마이크를 원격 제어하는 기능도 포함**했다. 클라우드 기반 C2 통신은 Google Drive, Dropbox, Telegram API를 활용해 정상 트래픽으로 위장했다. TLS 암호화와 DNS over HTTPS(DoH)를 결합해 네트워크 탐지를 회피했다. AiTM(Adversary-in-the-Middle) 기반 피싱 사이트와 OTP 탈취를 통해 MFA를 우회했다. 악성코드는 AridViper 변종, BitterRAT, VajraSpy를 주로 사용했다. 이들은 키로깅, 브라우저 쿠키 탈취, 시스템 정보 수집 기능을 제공한다. Python 스크립트와 PowerShell 난독화를 결합해 대량의 악성 샘플을 생성하여 공격을 자동화했다. 사회공학 기반 맞춤형 미끼 문서도 다양화했다. 특히, 정부 정책 문서, 외교 협상 자료, 군사 보고서를 위장한 이메일이 다수 발견되었다.

Sidewinder

SideWinder 그룹은 남아시아, 동남아시아, 중동 지역 정부, 군사, 외교, 에너지, 교육 기관을 대상으로 공격을 확대했다. **WarHawk 계열 악성코드를 중심으로 USB 웜, 키로거, 정보 탈취 기능을 포함한 다양한 모듈을 개발**했다. 다단계 로딩과 파일리스 실행을 결합해 탐지 회피 능력도 강화했다. 초기 침투는 스피어 피싱 이메일을 통한 악성 LNK 파일 배포 및 HTML Smuggling 기법을 활용했다.

PowerShell 난독화, DLL 사이드로딩, TxF 기반 Process Doppelganging 등 고도화된 기법으로 탐지를 회피했다. 또한, Cloudflare CDN과 Google Drive를 활용해 C2 통신을 은닉하고, TLS 암호화와 DNS over HTTPS(DoH)를 결합해 네트워크 탐지를 회피했다. WarHawk, SideWinder RAT, SplatCloak 악성코드를 주로 사용했고, 이들은 키로깅, 브라우저 쿠키 탈취, 시스템 정보 수집, USB 전파 기능을 제공한다. **사회공학 기법은 실존 인물 사칭, 학술 행사 위장, 단체 메시지 방 활용 등으로 진화**했다. 공격자는 피해자와 신뢰 관계를 형성하기 위해 다단계로 이메일을 교환했다. 또한, 공격 자동화를 위해 Python 기반 스크립트와 AI 생성 피싱 콘텐츠를 결합한 정황도 포착했다.

Key Point

- Bitter, HTML Smuggling과 PowerShell 기반 악성코드를 새롭게 사용해 탐지 회피 능력 강화
- 안드로이드 악성 앱, 금융 정보, 메시지, 위치 데이터 탈취및 카메라·마이크 원격 제어
- SideWinder, WarHawk 계열 악성코드를 중심으로 USB 웜, 키로거, 정보 탈취 기능 포함 다양한 모듈 개발
- 실존 인물 사칭, 학술 행사 위장, 단체 메시지 방 활용 등 사회공학 기법 진화

2025년 사이버 위협 동향

공격 그룹 트렌드 – APT: 파키스탄 및 기타

파키스탄 APT 그룹은 인도, 파키스탄, 중동, 아프리카 정부·군사·교육·NGO 대상 장기 공격을 수행한다. 여러 악성코드를 활용해 윈도우, 리눅스, 안드로이드 환경을 동시에 공격한다. MFA 우회 및 WebSocket 기반 C2 통신으로 탐지를 회피한다. 클라우드 인프라와 스테가노그래피로 악성 페이로드를 은닉하고, 맞춤형 피싱, AI 기반 콘텐츠 생성 등 사회공학 기법을 고도화한다.

파키스탄

Transparent Tribe

Transparent Tribe는 인도, 파키스탄, 중동, 아프리카 지역 정부, 군사, 교육, NGO 대상 공격을 지속했다. 이들은 CapraRAT, CrimsonRAT, ObliqueRAT 등 **다양한 RAT을 활용하며 윈도우, 리눅스, 안드로이드 환경을 동시에 공격**했다. 특히 리눅스 환경에서는 ".desktop" 파일 기반 공격을 새롭게 선보였다. WebSocket을 이용한 C2 통신으로 탐지 회피 능력을 강화하고, Kavach OTP 탈취를 통해 MFA를 우회했다. AiTM 기반 피싱 사이트를 활용해 실시간 세션 하이재킹도 수행했다.

Transparent Tribe는 클라우드 기반 인프라를 적극 활용했다. Google Drive, Slack, Telegram API를 통한 C2 통신을 확대하고, TLS 암호화와 DNS over HTTPS(DoH)를 결합해 네트워크 탐지를 회피했다. 주요 악성코드는 CrimsonRAT, CapraRAT, ObliqueRAT 외에도 안드로이드 악성 앱도 확인되었다. 공격자는 정상 앱으로 위장한 악성 앱을 배포하고, APK 파일에 스테가노그래피를 적용해 악성 페이로드를 은닉했다. 그리고, 맞춤형 미끼 문서로 사회공학 기법을 다양화했다. 외교 협상 자료, 학술 행사 초청장 등을 위장한 이메일이 다수 발견되었고, 피해자와 신뢰 관계를 형성하기 위해 다단계 이메일 교환을 수행했다. 또한, 공격 자동화를 위해 Python 기반 스크립트와 AI 생성 피싱 콘텐츠를 결합한 정황도 포착되었다.

기타

기타로 분류된 APT 그룹들은 국가 기반 분류가 어려울 정도로 활동 양상이 복잡다단하다. 정부, 국방, 금융, 통신, 교육, NGO 등 다양한 산업을 표적으로 삼으며, 아시아, 중동, 유럽, 미주 등 전 세계에서 활동한다. 이들은 **공통적으로 사회공학 기반 스피어 피싱과 다양한 문서 포맷을 활용한 초기 침투 방식을 사용**한다. 그리고, PowerShell 등 스크립트 기반 악성코드를 다단계로 로딩한다. 클라우드 서비스와 오픈소스 인프라를 적극적으로 활용하고, 특히 GitHub, Dropbox, Google Drive, Telegram 등을 C2로 활용하는 경우가 많다. 또한 Rust, Go, Python 등 **다양한 언어로 개발된 악성코드를 통해 윈도우, 리눅스, macOS, 안드로이드 등 멀티 플랫폼을 동시에 공격**한다.

고도화된 탐지 회피 기술을 사용한다. 난독화, 암호화, 파일리스 실행, DLL 사이드로딩, COM Hijacking, 로그 삭제, 타임 스탬프 조작 등 다양한 방식이 확인되었다. 특히, LLM 기반 악성코드(LAMEHUG), ClickFix, HTML Smuggling 등 최신 사회공학 기법과 MFA 우회, 세션 쿠키 탈취 등 인증 체계 무력화 기술을 새롭게 선보였다. 일부 그룹은 타 그룹의 인프라를 장악하거나 위장 기만(False Flag) 전략을 통해 혼란을 야기한다.

Key Point

- Transparent Tribe, 다양한 RAT 활용 및 윈도우, 리눅스, 안드로이드 환경 동시 공격
- 클라우드 인프라를 활용해 C2 통신 확대 및 네트워크 탐지 회피
- 기타 그룹들은 공통적으로 사회공학 기반 스피어 피싱과 다양한 문서 포맷을 활용한 초기 침투 방식 사용
- 다양한 언어로 개발된 악성코드를 통해 윈도우, 리눅스, macOS, 안드로이드 등 멀티 플랫폼을 동시에 공격

2025년 사이버 위협 동향

랜섬웨어 트렌드

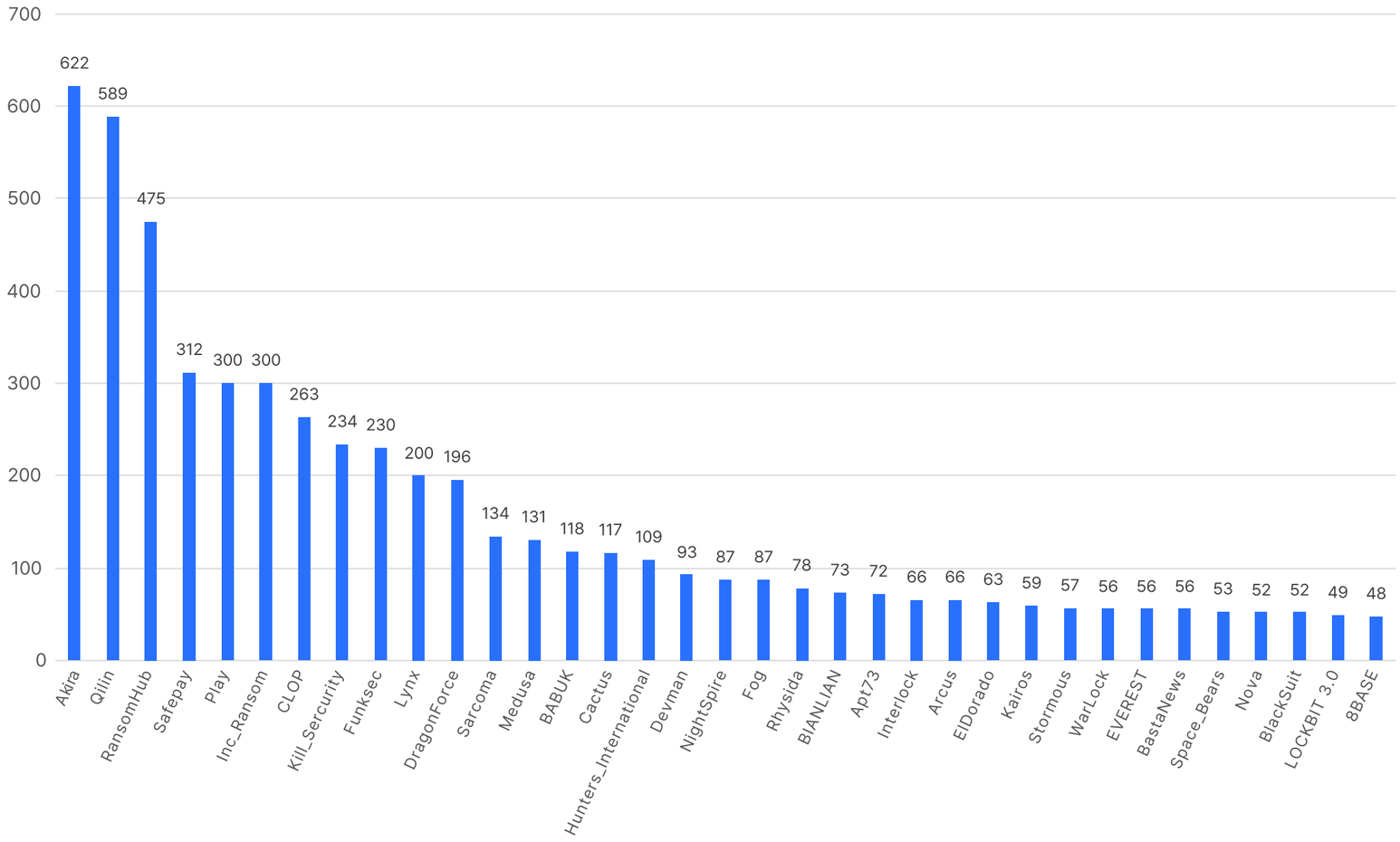
개요 및 동향

2025년 **랜섬웨어 생태계는 전년 대비 38% 확대**되며 폭발적으로 성장했다. 단속 등으로 주요 조직들이 피해를 입었지만 활동 그룹 수는 96개로 26% 증가했다. 생태계 파편화가 가속화된 것이다.

공격 그룹 순위에도 큰 변화가 있었다. 622건의 피해 사례를 발생 시킨 **Akira는 전년 4위에서 1위로 올랐다.** Qilin은 589건으로 11위에서 2위로 급부상했다. CLOP도 43위에서 7위로 올랐다. 반면, 2024년 1위였던 LockBit은 Operation Cronos 여파로 30위권 밖으로 밀려났다.

북한 배후 Andariel과 Moonstone Sleet이 Play 및 Qilin 랜섬웨어를 배포하면서 **국가 지원 공격 그룹들이 RaaS에 편입되며 카르텔화** 되는 모습을 보였다. 금전적 이익과 국제 제재 회피를 위한 새로운 모델을 제시했다.

2025년 랜섬웨어 그룹별 피해 기업 게시 건수



2025년 사이버 위협 동향

랜섬웨어 트렌드

수사 기관의 단속과 한계

올해, 수사 기관의 랜섬웨어 대응이 강화되었으나 효과는 제한적이었다. Operation Cronos로 타격을 입은 LockBit은 2025년 9월, LockBit 5.0을 발표하며 부활을 선언했다. 특히, 원자력·화력 발전소 등 주요 인프라 공격을 명시적으로 허용하여 더욱 공격적 전술로 회귀했다.

RansomHub의 올해 4월 갑작스러운 활동 중단을 선언했다. 2024년 공격 횟수 1위였던 조직이 완전히 사라진 것이다. DragonForce가 흡수를 주장했으나 RansomHub는 DragonForce의 법 집행기관 협력 의혹을 제기하며 분열하는 모습을 보였다.

RansomHub 제휴자들은 Qilin, DragonForce, Lynx로 이동하면서 생태계가 재편됐다. RaaS 생태계의 높은 회복력과 적응력을 다시 한 번 볼 수 있었다.

주요 공격 전술

랜섬웨어 공격 기법은 '삼중 갈취 전술'로 진화했다. 데이터 암호화·유출에 더해 피해 조직의 고객과 파트너에게 연락해 추가 압박을 가하는 방식이다. 의료·금융 분야에서 평판 손상 극대화를 위해 집중적으로 사용되었다.

랜섬웨어 공격 기법은 '삼중 갈취 전술'로 진화했다. 데이터 암호화·유출에 더해 피해 조직의 고객과 파트너에게 연락해 추가 압박을 가하는 방식이다. 의료·금융 분야에서 평판 손상 극대화를 위해 집중적으로 사용되었다.

제로데이에서 1-Day 취약점 공격으로 전환한 것도 주목할 변화다. CLOP은 Cleo MFT 제로데이 취약점으로 400개 조직을 침해했고, Akira는 소닉월 SSL VPN 취약점을 집중 공격했다. MFT 플랫폼과 VPN 장비가 새로운 핵심 공격 벡터로 부상했다.

대응 방안 및 전망

랜섬웨어는 AI 기반 자율 공격 시스템과 LLM을 활용한 전술이 고도화되고, 암호화 없는 데이터 전용 공격이 증가할 것으로 예상된다. 북한 사례를 시작으로 국가 후원 해커와 사이버 범죄 조직 협력이 강화될 전망이다.

이러한 **랜섬웨어 대응을 위해서는 다층적 방어 체계를 구축**해야 한다. 제로 트러스트 아키텍처 도입, VPN과 RDP에 대한 다중 인증(MFA) 적용, Vmware ESXi 등 하이퍼바이저 환경 보호와 네트워크 마이크로 세그먼테이션을 통한 피해 확산 방지도 중요하다.

위협 인텔리전스 기반 24/7 모니터링으로 IAB(Initial Access Broker) 판매와 실제 공격 간 18일 시간차를 활용한 조기 탐지가 필요하다. 물리적 분리된 오프라인 백업과 불변 백업도 필수다.

Key Point

- 대형 랜섬웨어 그룹들이 위축되었으나 RaaS 생태계는 높은 회복력 보여
- 랜섬웨어 공격 기법은 삼중 갈취 전술로 진화 – 데이터 유출 협박에 더해 고객과 파트너까지 압박
- 진화하는 랜섬웨어 대응을 위해서는 다층적 방어 체계 필요 – 제로 트러스트, MFA, TI 기반 모니터링 등

2025년 사이버 위협 동향

랜섬웨어 트렌드 - 주요 그룹 활동 분석 Top 10

1. Gunra - 한국 금융권 침투

Gunra는 2025년 4월 처음 발견된 신규 랜섬웨어 그룹으로 대한민국, 일본, 브라질, 튀르키예, 대만을 주요 타깃으로 삼았다. 피해 국가 중 미국이 없는 것이 특징이다. Conti v2 소스코드를 기반으로 제작된다.

가장 큰 특징은 5일이라는 극단적으로 짧은 협상 기한으로, 피해 조직에 심리적 압박을 가한다. 다크웹에서는 메신저 '왓츠앱(WhatsApp)' 스타일의 협상 포털을 운영하며 매니저 역할을 두는 등 체계적으로 운영한다.

Gunra 랜섬웨어는 **윈도우와 리눅스 모두 공격**할 수 있다. 특히, 최대 100개 동시 암호화 스레드를 지원하는 고성능 리눅스 변종을 보유했다. 리눅스 버전은 ChaCha20 암호화를 사용하며, 구현 과정에서 암호화 약점이 발견되었다. 이에, 국내 보증보험사는 금융보안원의 도움으로 복호화에 성공할 수 있었다.

2. Qilin - 압도적 지배력 확립

2024년 대한민국과 일본에서 보고된 공격이 단 한 건도 없었던 Qilin은 2025년 수십 건의 공격을 기록하며 양국에서 가장 활발한 활동을 보였다. RansomHub가 사라진 공백을 신속하게 메우며, 표류하던 제휴자(affiliate)들을 대거 흡수했다. **한국에서는 'Korean Leak' 캠페인으로 IT 공급망 침해를 통해 29개 중소 자산운용사들을 공격**했다.

특히, **북한 배후 Moonstone Sleet이 2월부터 Qilin 랜섬웨어를 배포하며 국가 후원 위협 그룹으로 진화**했다. 9월에는 DragonForce, LockBit과 카르텔을 형성하며 시장 지배를 위한 협력 체제를 구축했다.

3. Play - 북한 Andariel과 결합

Play 랜섬웨어는 2024년 10월 북한 배후 Andariel과 협력한 것이 확인되었다. **국가 배후 그룹이 RaaS 인프라를 활용한 첫 사례**였다. Andariel은 5월 피해 조직에 침투한 뒤 Sliver C2 프레임워크와 DTrack 백도어를 배포하며 잠복했고, 9월 Play 랜섬웨어를 최종 배포했다.

2025년 상반기, FBI는 약 900개 조직이 Play 랜섬웨어의 피해를 입었다고 발표했다. 북한은 WannaCry 이후 랜섬웨어를 자금 조달 수단으로 활용해왔으며, Play와의 협력은 국제 제재를 우회하는 새로운 전략으로 평가된다.

Key Point

- Gunra 랜섬웨어, 윈도우와 리눅스 모두 공격 가능 - 리눅스 버전은 암호화 구현 과정에서 약점 발견
- 북한 배후 Moonstone Sleet이 2월부터 Qilin 랜섬웨어를 배포하며 국가 후원 위협 그룹으로 진화
- Play 랜섬웨어, 북한 Andariel과 협력 - 국가 배후 그룹이 RaaS 인프라를 활용한 첫 사례

2025년 사이버 위협 동향

랜섬웨어 트렌드 - 주요 그룹 활동 분석 Top 10

4. Akira – SSL VPN 공격

Akira는 2025년 꾸준한 성장률을 유지하며 **공격 횟수 1위**에 올랐다. 2024년 산발적인 대량 데이터 유출 패턴에서 벗어나 2025년 1분기부터는 정기적인 소량 유출로 전술을 변경했다.

가장 주목할 만한 사건은 7월부터 시작된 소닉월 SSL VPN 장비 집중 공격이다. CVE-2024-40766 취약점을 악용해 전 세계적으로 공격을 감행했다. 8월에는 미국 조직에서 네트워크 스캐닝, 측면 이동, 권한 상승, 데이터 유출이 연쇄적으로 관찰되었다.

Vmware ESXi 가상화 환경 공격에도 특화되어 있어 클라우드 인프라를 광범위하게 암호화할 수 있는 능력을 보유했다. Rust 기반 새로운 변종(Akira v2)을 개발해 고급 난독화 기법을 적용했다. 또한, PowerTool 악용, 로그 삭제 등 다양한 EDR 회피 기법을 구사했다. 제조업, 교육, 의료 분야를 주요 표적으로 2025년 상반기 수십 개 조직을 공격하며 대표적인 공격 그룹으로 자리매김했다.

5. Lynx - 제조업 집중 공격

Lynx는 2024년 7월, INC 랜섬웨어 코드를 리브랜딩해 등장했다. 2025년 피해자 수가 96개(1월)에서 300개(8월)로 급증했다. 6월부터 Sinobi라는 이름으로 복수 브랜드 전략을 구사하기 시작했다. **제조업과 건설업을 주요 표적으로 하고, 미국이 전체 피해 국가의 60%를 차지**했다.

1월 미국 법무법인을 공격해 고객 민감 정보를 탈취했고, 12월에는 루마니아 에너지 공급사를 마비시켰다. 윤리적 해킹을 표방했으나, 실제로는 이중 갈취 전술을 사용하며 기회주의적이고 무차별적인 공격을 감행한다.

6. LockBit – 버전 5.0으로 부활

LockBit은 2024년 2월 'Operation Cronos' 이후 심각한 타격을 입었다. 그 후 2025년 9월, 설립 6주년을 맞아 LockBit 5.0으로 부활을 선언했다. **새 버전은 윈도우, 리눅스, VMware ESXi를 동시에 노리는 크로스 플랫폼 전략을 강화**했다. 또, DLL 리플렉션 로딩, ETW 패칭 등 고도화된 안티 분석 기법을 적용했다.

가장 주목할만한 것은 제휴자들에게 그간 대외적으로 자제해왔던 원자력 발전소, 화력 발전소 등 주요 인프라 공격을 명시적으로 허용한 점이다.

Key Point

- Akira 랜섬웨어, 소닉월 SSL VPN 장비 취약점을 활용해 전 세계적인 공격 감행
- Lynx 랜섬웨어, 제조업과 건설업을 주요 표적으로 공격 – 미국이 전체 피해 국가의 60% 차지
- LockBit 5.0, 윈도우, 리눅스, VMware ESXi를 동시에 노리는 크로스 플랫폼 전략 강화

2025년 사이버 위협 동향

랜섬웨어 트렌드 - 주요 그룹 활동 분석 Top 10

7. DragonForce - 카르텔 전략

2023년 말 등장한 DragonForce는 2025년 3월 '랜섬웨어 카르텔'을 선언하며 생태계 재편을 시도했다. **제휴자들이 자체 브랜드로 활동하면서 DragonForce 인프라를 활용할 수 있는 화이트라벨 모델을 도입**했다. 수익의 80%를 제휴자에게 배분하고, 페타바이트급 스토리지, 24시간 모니터링, 블로그 및 파일 서버를 제공했다. 2025년 4월, RansomHub 인프라를 흡수했다고 주장했다. 다만, RansomHub 측은 DragonForce가 수사기관과 협력하고 있다고 맞불을 놓으며 갈등이 표면화되었다.

8. CLOP - Cleo MFT 공격

CLOP은 2025년 1분기 극적으로 복귀했다. 그 중심에는 **Cleo MFT 솔루션의 두 가지 제로데이 취약점(CVE-2024-50623, CVE-2024-55956) 활용 공격**이 있었다. 10월 Cleo가 첫 번째 취약점을 패치했으나, CLOP은 11월 패치 우회에 성공했고, 12월 두 번째 제로데이를 발견해 공격을 지속했다. 약 400개 조직이 침해되었다.

CLOP은 지난 2023년 2천개 이상 조직을 침해한 MOVEit 공격 경험을 살려 MFT 플랫폼 취약점 공략에 특화된 전문성을 보였다. 1월부터 알파벳 순서로 피해자 명단을 공개했고, 최종 피해 규모는 수백 건이 넘었다.

9. RansomHub – 최강자의 흥망성쇠

RansomHub는 90%라는 파격적인 제휴자 수익 배분율과 210개 이상 조직 침해로 2025년 1분기까지 최다 활동을 이어갔다. 그러나 4월 1일, 갑작스럽게 활동이 완전히 중단되었다.

RansomHub의 몰락은 수백 명의 제휴자들이 Qilin, DragonForce, Lynx 등으로 이동하는 대규모 생태계 재편을 촉발했다. 이는 2024년 LockBit의 'Operation Cronos' 이후 가장 큰 구조적 변화였으며, 랜섬웨어 생태계의 불안정성과 역동성을 다시 한번 입증했다.

10. 일본 기업 표적 공격 증가

일본은 2024년 10월 ~ 2025년 9월에 간 **전년 동기 대비 217% 증가한 랜섬웨어 공격**을 당했다. 공격 횟수는 Qilin이 최다였고, Lynx, Nightspire, RansomHub, Akira 등도 보안이 취약한 중소기업 대상 공격을 감행했다.

신규 공격 그룹 Kawa4096는 6월 말 등장 직후 두 개 조직을 침해했다. 이 그룹의 KaWaLocker 랜섬웨어는 Salsa20 암호화, 멀티 스레딩, 파일명 해싱 기능을 갖췄고, 7월 출시한 2.0 버전에서 기능을 강화했다. 제조업이 가장 큰 타격을 받았고, 중소기업이 피해의 다수를 차지했다.

Key Point

- DragonForce, 제휴자들이 자체 브랜드로 활동하면서 DragonForce 인프라를 활용할 수 있는 화이트라벨 모델 도입
- CLOP 랜섬웨어, Cleo MFT 솔루션의 제로데이 취약점 공략 – 약 400개 조직 침해
- 일본을 향한 랜섬웨어 공격 217% 증가 - 제조업이 가장 큰 타격을 받았고, 중소기업 피해도 다수

2025년 사이버 위협 동향

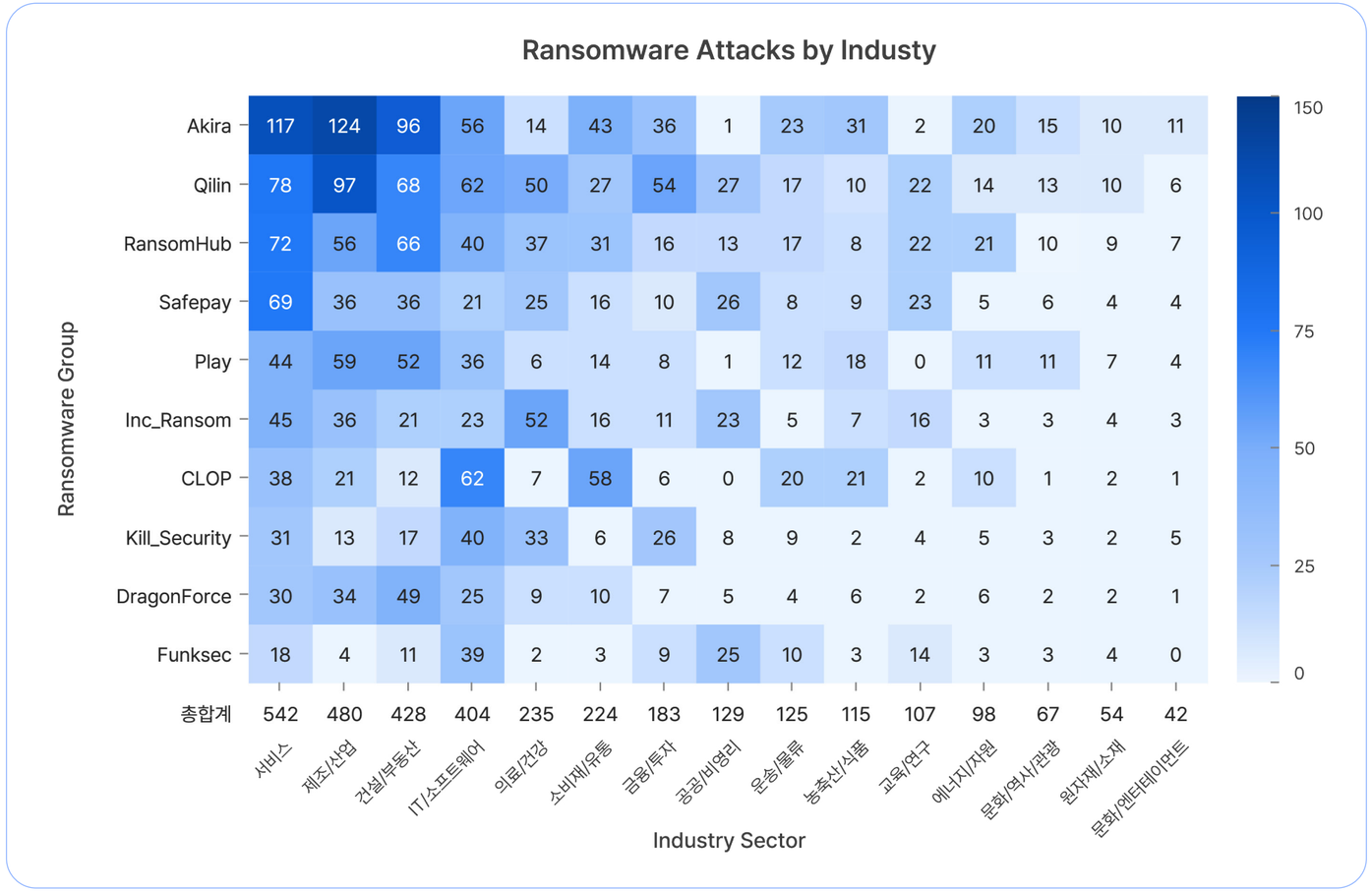
랜섬웨어 트렌드 – 주요 피해 산업군

2025년 랜섬웨어 공격 그룹별 주요 피해 산업군 데이터 분석 결과, 서비스, 제조/산업, 건설/부동산, IT/소프트웨어 분야가 주요 공격 대상이었다. **가장 주목할 만한 변화는 서비스 산업이 최다 피해 산업군이 된 것**이다. 코로나19 이후 디지털 전환으로 서비스 산업의 IT 의존도가 높아졌고, 시스템 중단 시 매출 손실 등 즉각적인 피해를 입기 때문이다.

제조/산업과 건설/부동산은 여전히 주요 표적이었다. 제조업은 스마트 팩토리와 공급망 관리 시스템의 확대로 공격 표면이 넓어졌다. 생산 라인 중단 시 큰 손실이 발생해 복구 비용 지불 가능성도 높다. 건설/부동산은 프로젝트 일정 지연에 따른 위약금과 법적 분쟁 위험이 크기 때문에 복구 압박이 크다. IT/소프트웨어 산업도 대규모 고객 데이터를 보유하고 있어 공격자들이 지속적으로 노리고 있다.

가장 우려스러운 변화는 의료/건강 분야의 공격 증가다. 이 분야는 암묵적으로 공격이 금기 시 되어 왔는데 2025년 완전히 무너졌다. 일례로, BlackCat은 2024년 수사기관 작전으로 와해된 후 부활하며 병원 공격 금지령을 해제하고 공격을 장려했다. 환자 생명과 직결되어 빠른 복구가 필수적이고 민감 의료 정보 유출 시 법적·윤리적 책임이 커, 공격자들이 선호하는 고수익 표적이 되었다.

반면, 농축산/식품, 문화/역사/관광 등은 공격 빈도가 적었다. 디지털 의존도가 낮고 전통적인 운영 방식을 추구해 공격자들이 주요 타깃으로 삼지는 않는 것으로 풀이된다.



[그림] 랜섬웨어 그룹별 산업군 공격 현황 (2024년 10월 ~ 2025년 9월)

2025년 사이버 위협 동향

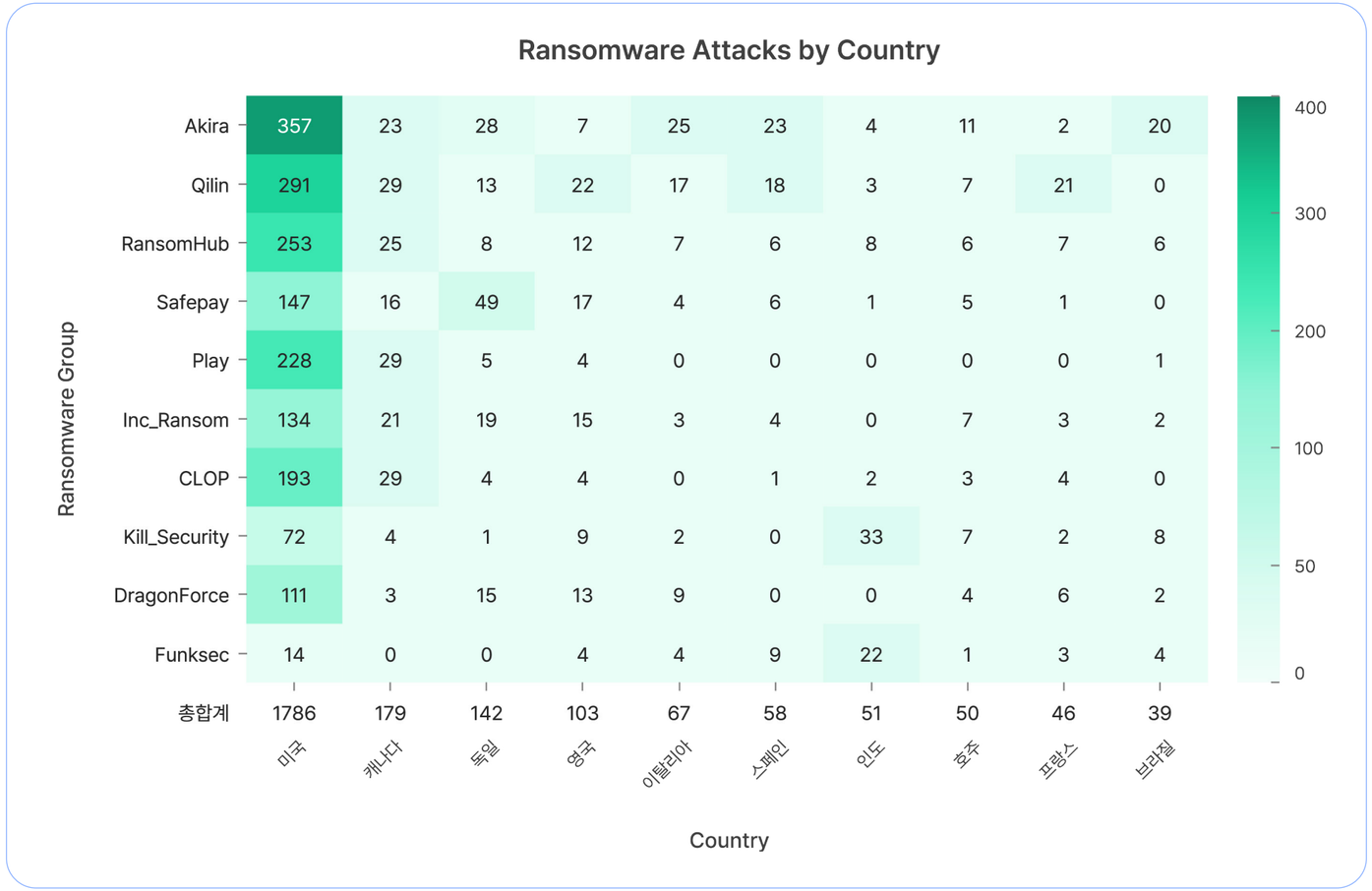
랜섬웨어 트렌드 – 주요 피해 국가: 전세계

2025년 통계에 따르면, 미국은 여전히 가장 많은 랜섬웨어 공격을 받고 있다. **Akira와 Qilin은 꾸준히 공격을 지속했고, RansomHub는 4월 활동 중단 전까지 미국 기업/기관을 표적**으로 삼았다. 미국은 세계 최대 경제 대국으로서 제조, IT, 의료, 금융 등 고부가 산업이 밀집해 있고, 디지털 의존도가 높아 사이버 위협에 노출되기 쉬운 구조적 특성을 갖고 있다. 대규모 고객 데이터와 민감 정보가 클라우드에 집중되어 있어, 데이터 유출과 이중·삼중 갈취의 주요 타깃이 된다.

유럽과 아시아 지역의 공격 패턴 다변화도 주목할만 했다. 독일은 Safepay와 Akira의 집중 공격을 받으며 전년 대비 피해가 증가했다. 특히, 데이터 유출 압박형 공격이 두드러졌다. 프랑스와 영국도 지속적인 타격을 입었다. **아시아에서는 인도가 Kill_Security와 Funksec의 거점으로 부상하며 새로운 공격 대상**으로 자리잡았다. 캐나다는 미국과 인접한 지리적 특성과 유사한 경제 구조로 인해 여전히 피해가 많았다.

스페인, 이탈리아, 브라질 등도 주요 피해국으로 나타났다. 유럽에서는 Qilin과 Akira가 스페인과 이탈리아를 지속적으로 공격했다. 남미에서는 브라질이 Akira의 집중 공격을 받았다. 아태 지역은 호주와 일본이 주요 피해국으로 확인됐다.

미국 정부와 동맹국들은 랜섬웨어 생태계에 대해 국제 공조를 통한 수사와 제재로 적극 대응하고 있다. 다만, 공격자들은 법적 관할의 틈을 이용해 해외 인프라를 기반으로 공격을 수행하며 제재를 피하고 있다.



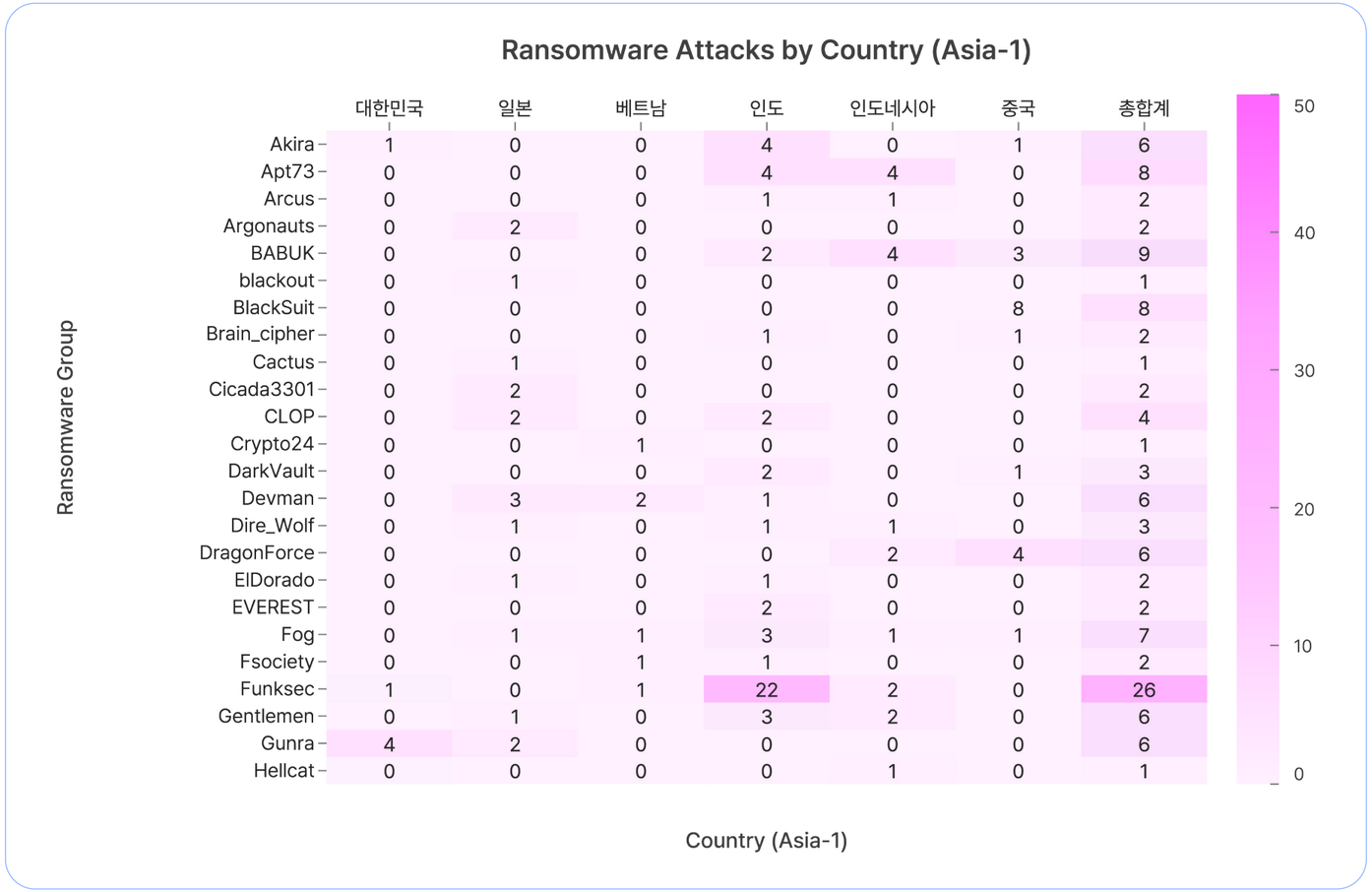
[그림] 국가별 랜섬웨어 공격 피해 현황 (2024년 10월 ~ 2025년 9월)

2025년 사이버 위협 동향

랜섬웨어 트렌드 – 주요 피해 국가: 아시아 (1)

2025년 아시아 국가별 랜섬웨어 피해 분석 결과, **인도가 일본을 제치고 주요 타깃으로 급부상**했다. 이 밖에, 대만, 대한민국, 일본이 비슷한 수준의 피해 횟수를 기록했다. 전체 사건 수는 전년도 대비 급격한 증가세를 보였다.

흥미로운 점은 국가별 위협 집중도에 차이가 있다는 것이다. **대한민국과 중국은 소수의 강력한 그룹 편중**이 두드러진다. 반면, 일본과 인도네시아는 상대적으로 분산형 위협 구조를 보였다. 이 경우, 다양한 공격 그룹이 사용하는 침투 전술에 대비해야 한다.



Ransomware Group	대한민국	일본	베트남	인도	인도네시아	중국	총합계
Akira	1	0	0	4	0	1	6
Apt73	0	0	0	4	4	0	8
Arcus	0	0	0	1	1	0	2
Argonauts	0	2	0	0	0	0	2
BABUK	0	0	0	2	4	3	9
blackout	0	1	0	0	0	0	1
BlackSuit	0	0	0	0	0	8	8
Brain_cipher	0	0	0	1	0	1	2
Cactus	0	1	0	0	0	0	1
Cicada3301	0	2	0	0	0	0	2
CLOP	0	2	0	2	0	0	4
Crypto24	0	0	1	0	0	0	1
DarkVault	0	0	0	2	0	1	3
Devman	0	3	2	1	0	0	6
Dire_Wolf	0	1	0	1	1	0	3
DragonForce	0	0	0	0	2	4	6
ElDorado	0	1	0	1	0	0	2
EVEREST	0	0	0	2	0	0	2
Fog	0	1	1	3	1	1	7
Fsociety	0	0	1	1	0	0	2
Funksec	1	0	1	22	2	0	26
Gentlemen	0	1	0	3	2	0	6
Gunra	4	2	0	0	0	0	6
Hellcat	0	0	0	0	1	0	1

[그림] 아시아 주요 국가 랜섬웨어 그룹별 공격 현황 (2024년 10월 ~ 2025년 9월, 연속 이미지 P33-P34)

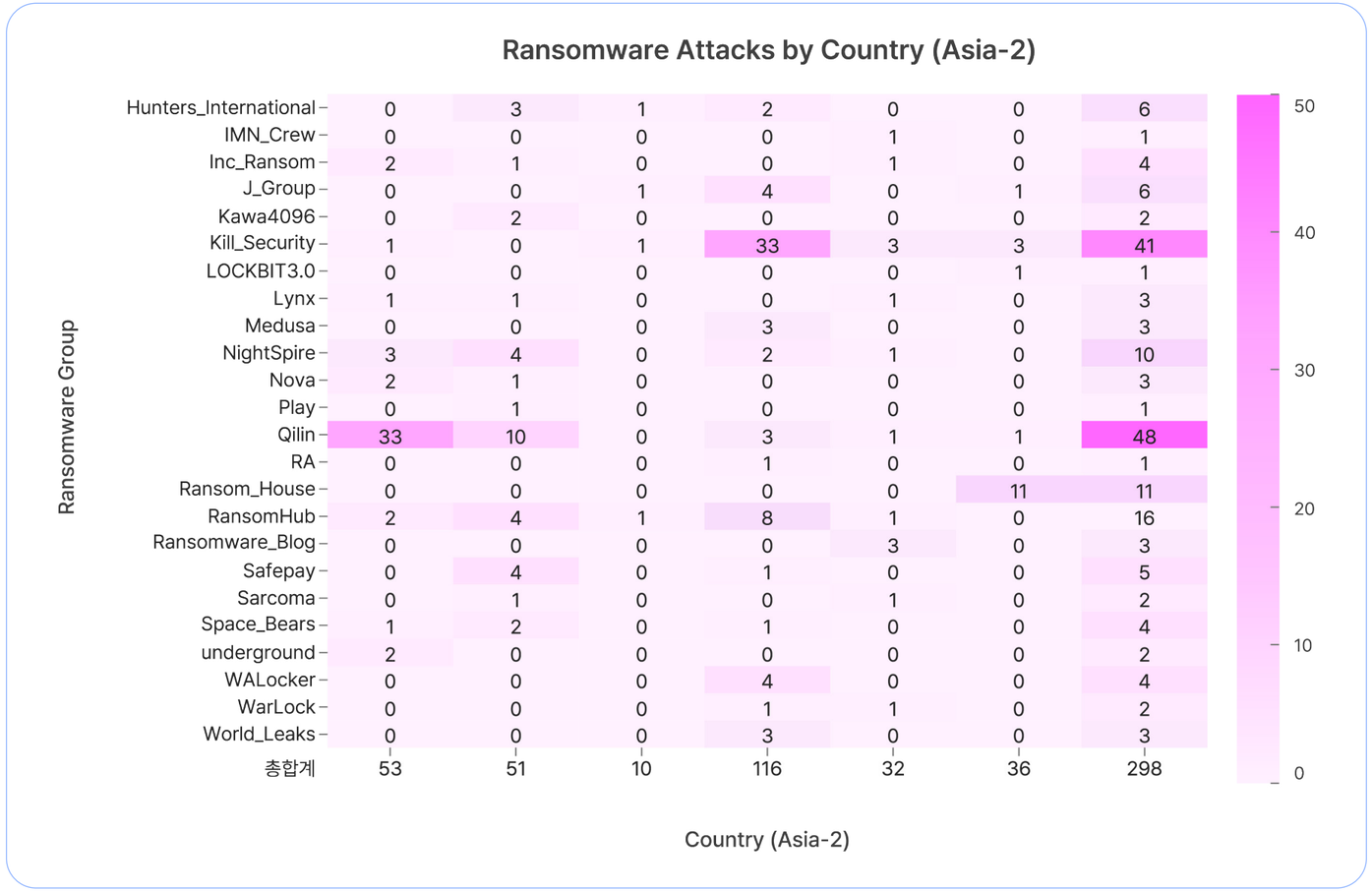
2025년 사이버 위협 동향

랜섬웨어 트렌드 – 주요 피해 국가: 아시아 (2)

공격 그룹 활동을 보면, **Qilin이 올해 아시아권에서 가장 활발한 움직임**을 보였다. 특히 대한민국과 일본에서 집중적인 활동이 확인되었다. Qilin은 대한민국에서의 활동이 급증했는데, IT 서비스 공급업체를 침투해 해당 업체가 관리하는 여러 자산 관리 회사를 동시에 타격하는 공급망 공격을 수행했기 때문이다. 그 뒤를 잇는 Kill_Security는 인도에 강한 편중을 보였다.

2025년 아시아권 랜섬웨어 공격은 ▲피해 횟수 증가 침해 ▲공격 대상 이동(일본 → 인도) ▲ 국가별 위협 그룹 집중도 차이로 요약할 수 있다.

대한민국, 인도, 일본을 비롯한 아시아 국가들에 다양한 공격이 지속되고 있어, 지속적인 모니터링과 강화된 보안 체계가 요구된다. 또한, RansomHub 와해 이후 재편된 Qilin, Kill_Security 등 주요 공격 그룹의 전술 변화를 신속하게 반영해 대응 방안을 수립해야 한다.



[그림] 아시아 주요 국가 랜섬웨어 그룹별 공격 현황 (2024년 10월 ~ 2025년 9월, 연속 이미지 P33-P34)

2025년 사이버 위협 동향

주요 위협 트렌드 - 악성코드 Top 9

2025년, 다양한 유형의 악성코드가 보고되었고, 통신·금융·리눅스 인프라를 겨냥한 공격이 두드러졌다. 랜섬웨어와 인증 구조를 악용한 악성코드가 활발히 유포되었고, USB 기반 전파나 SNS 광고를 통한 정보 탈취 등 기법도 다양해졌다.
북한 APT 그룹 관련 새로운 악성코드가 발견되고 기존 악성코드도 꾸준히 유포되고 있다.

1. BPFDoor 악성코드 통신사를 노린 은밀한 침입자

BPFDoor는 리눅스 시스템을 대상으로 동작하는 백도어 악성코드다. 네트워크 필터링 기술 BPF를 악용해 보안 장비의 감시를 우회해 시스템 내부에 은밀하게 접근한다.

이 악성코드는 특정 패킷 수신 시에만 활성화된다. 다양한 통신 프로토콜을 활용해 외부 명령을 수신하고, 내부 정보를 유출한다. 실행 과정에서 정상적인 시스템 프로세스로 위장하고, 파일을 복제한 뒤 원본을 삭제해 흔적을 최소화한다. /dev/shm 경로로 메모리 기반 실행을 시도한다.

2025년, **국내 통신사 해킹 사건에서 해당 악성코드가 사용**되었다. 특히, 가입자 인증 서버를 겨냥한 공격이 보고되면서, 산업 전반의 보안 점검 필요성이 제기되었다.

2. Qilin 랜섬웨어 자산 운용사를 노린 이중 협박자

Qilin은 RaaS 방식으로 운영되는 랜섬웨어다. 대부분 C언어로 작성되는 기존 랜섬웨어와 달리 **Rust 언어로 개발되며 윈도우와 리눅스 환경 모두 지원**한다. 일반 랜섬웨어가 보통 파일을 한 번만 암호화하지만, Qilin은 리눅스 환경에서 동일 파일을 세 번 암호화한다. 백업 삭제 및 복구 방해 기능도 포함한다. 공격자에게 법률·홍보 지원까지 제공하는 조직적인 운영 구조를 갖추고 있다.

2025년, **국내 자산 운용사**를 공격했다. 여러 자산 운용사가 공유하던 전산 관리 업체 클라우드 서버가 감염되어, 고객 정보와 내부 문서가 다크웹에 유출되었다.

3. Gunra 랜섬웨어 협상 없이 복구한 사례

Gunra 랜섬웨어 역시 RaaS 형태로 운영된다. Conti 랜섬웨어의 소스코드를 기반으로 제작된 것으로 알려져 있다. 윈도우와 리눅스 환경을 모두 지원하고, 운영체제에 영향을 주는 파일은 제외한 채 기업의 핵심 자산만 선별적으로 암호화하는 방식으로 피해를 극대화하는 특징이 있다.

2025년, **대한민국 금융 기관 및 제조 업체를 연이어 공격했다.** 피해 기업의 내부 문서와 고객 정보가 다크웹에 유출되면서 산업 전반에 불안감이 확산되었다. 다만, 리눅스 버전에서는 암호화 키 생성 방식에 구조적 결함이 발견되었다. 이에, 국내에서 복호화 키를 추출해 데이터를 복구했다.

Key Point

- BPFDoor, 국내 통신사 해킹에 사용 – 특정 패킷 수신 시에만 활성화되어 내부 정보 유출
- Qilin 랜섬웨어, Rust 언어로 개발되며 윈도우와 리눅스 환경 지원 – 국내 자산 운용사 공격
- Gunra 랜섬웨어, 국내 기업 다수 공격 – 리눅스 버전 암호화키 구조적 결함으로 복호화 가능

2025년 사이버 위협 동향

주요 위협 트렌드 - 악성코드 Top 9

4. Plague 악성코드 리눅스 인증 구조를 노리다

Plague 악성코드는 **리눅스 시스템의 로그인 절차를 가로채 사용자 계정 정보를 탈취**한다. 시스템이 부팅될 때 자동으로 실행되며, 사용자가 SSH나 터미널을 통해 로그인할 때 입력하는 ID와 비밀번호를 수집한다.

리눅스는 PAM이라는 인증 모듈을 통해 로그인 정보를 확인하는데, Plague 악성코드는 LD_PRELOAD 기법을 활용해 시스템이 원래 실행해야 하는 인증 기능 대신 자신이 먼저 작동하도록 설정한다.

즉, 사용자가 로그인할 때 Plague 악성코드가 몰래 끼어들어 정보를 가로채는 방식이다. 로그인 기록을 삭제하고 시스템 설정을 변경해 재부팅 이후에도 계속 작동할 수 있도록 구성되어 있다. 최근에는 탐지 회피와 은폐 기능이 강화된 형태로 진화하고 있다.

5. USB로 퍼지는 채굴 악성코드

USB를 통한 악성코드 전파는 물리적 접근이 가능한 환경에서 여전히 효과적인 수단으로 활용되고 있다. 최근 **국내에서도 USB를 매개로 암호화폐 채굴 악성코드가 유포된 사례**가 있었다.

공격자는 감염된 USB에 바로가기(.lnk) 파일을 숨겨두고, 사용자가 이를 실행하면 PowerShell 스크립트를 통해 채굴 프로그램인 XMRig를 설치한다. 단순 설치에 그치지 않고, PostgreSQL 데이터베이스와 직접 연결되어 명령을 주고 받는 방식으로 작동한다. 일반적인 악성코드보다 더 정교한 통신 구조를 갖추고 있어, 외부에서 채굴 활동을 제어하거나 상태를 모니터링할 수 있도록 한다. 또한, GitHub를 통해 악성 파일을 다운로드 하고, 윈도우 레지스트리의 Run 키를 이용해 재부팅 후에도 자동 실행되도록 설계되어 있다. 이에, 지속적인 채굴이 가능하다.

6. 가짜 거래소 광고로 유포되는 인포스틸러

공격자는 바이낸스 등 **유명 거래소를 사칭한 페이스북 광고를 노출하고, 사용자가 이를 클릭하면 가짜 거래소 사이트로 유도한 뒤 installer.msi 파일을 다운로드하도록 유도**한다. 파일은 실행 즉시 악성 행위를 시작하지 않으며, 피해자가 가상 환경이 아니고 공격자가 설정한 조건에 해당하는 경우에만 악성 스케줄러를 등록하고 이후 인포스틸러 악성코드를 내려받아 실행한다.

단순 악성코드 유포 주소에 접속하는 것만으로는 감염되지 않으며, 비대상 사용자의 경우 정상 사이트로 리다이렉션되어 탐지를 회피한다. 악성코드는 PowerShell을 통해 추가 페이로드를 받아오며, 시스템 정보, 브라우저 저장 데이터, 화면 캡처, 텔레그램 계정 등 민감한 정보를 수집한다.

Key Point

- Plague 악성코드, 리눅스 시스템의 로그인 절차를 가로채 사용자 계정 정보 탈취
- 국내에서 USB를 매개로 암호화폐 채굴 악성코드가 유포된 사례 발생
- 가짜 거래소 광고 - 유명 거래소 사칭 페이스북 광고 > 가짜 거래소 사이트로 유도 > 악성파일 다운로드

2025년 사이버 위협 동향

주요 위협 트렌드 - 악성코드 Top 9

7. Proxyware 악성코드의 은밀한 침투 내 PC가 몰래 대역폭을 공유한다면?

Proxyware는 사용자가 자신의 인터넷 대역폭을 외부에 공유하고 수익을 얻는 합법적인 프로그램이다. 최근에는 이를 악용한 악성코드가 보안 위협이 되고 있다.

공격자는 **사용자의 동의 없이 Proxyware를 설치해 네트워크 자원을 몰래 공유**하게 한다. 이를 통해 금전적 이득을 취하는 Proxyjacking이 국내에서도 다수 확인되었다. Mimo 코인 마이너와 함께 유포되거나, 프리웨어 설치 과정 중 광고 페이지를 통해 자동 설치되는 방식이 사용된다. 피해자는 시스템 성능과 네트워크 속도 저하를 겪게 된다.

Proxyware는 외부 서버와 지속적으로 통신하며, 공격자가 설정한 방식에 따라 자원을 활용하기 때문에 감염 사실을 인지하기 어렵다. Cryptojacking과 유사하지만 CPU 대신 네트워크 대역폭을 활용한다는 점에서 차별화되며, 백신 탐지를 우회하는 방식으로 은밀하게 작동한다.

8. BeaverTail & Tropidoor 악성코드 라자루스의 채용 이메일 위장 공격

BeaverTail과 Tropidoor는 북한의 지원을 받는 것으로 알려진 '라자루스(Lazarus)'가 사용하는 악성코드로 채용을 위장한 피싱 이메일을 통해 유포된다. 공격자는 실제 기업명을 사칭해 개발자나 IT 종사자에게 접근한다. 악성 프로젝트가 포함된 Bitbucket 링크를 이메일에 담아 유포하는 방식으로 감염을 시도한다.

악성코드 BeaverTail은 브라우저에 저장된 로그인 정보와 암호화폐 지갑 데이터를 수집하는 인포스틸러 기능을 갖추고 있다. Tropidoor는 메모리 기반 백도어로 시스템 정보 수집, 명령 실행, 화면 캡처 등 다양한 기능을 통해 장기적인 침입을 가능하게 한다. 대부분의 공격은 해외에서 발생했지만, 국내에서도 감염 로그가 일부 확인된 바 있다.

9. EndRAT, Kimsuky의 새로운 악성코드

EndRAT은 북한의 지원을 받는 것으로 알려진 '김수키(Kimsuky)'가 2025년 7월부터 활용하기 시작한 AutoIt 기반 새로운 RAT(Remote Access Trojan) 악성코드다.

EndRAT는 서버와의 통신에 사용되는 고유 문자열 "endServer9688" 및 "endClient9688"을 포함하고 있으며, 해당 식별자를 기반으로 명명되었다. 일반적으로 LNK 파일 실행을 유도하는 방식으로 유포된다. 2025년 9월에는 '스트레스 클리어'라는 프로그램으로 위장된 MSI 인스톨러를 통해 배포된 사례도 확인되었다. AutoIt 스크립트를 기반으로 제작된 점, 실행 조건 및 통신 구조에 특정 문자열을 사용하는 방식은 기존 악성코드와 차별화 된다.

Key Point

- 사용자의 동의 없이 Proxyware를 설치해 네트워크 자원을 몰래 공유하는 공격 방식
- Lazarus, 개발자나 IT 종사자에 접근해 BeaverTail 및 Tropidoor 악성코드 배포
- Kimsuky 그룹, 새로운 RAT(Remote Access Trojan) 악성코드 'EndRAT' 사용 시작

2025년 사이버 위협 동향

주요 위협 트렌드 - 공격 기법 Top 10

1. 소프트웨어 공급망 공격

2025년 들어 소프트웨어 공급망 공격의 규모와 정교함이 확대되었다. **공격자들은 오픈소스 패키지 저장소(npm, PyPI 등)에 직접 침투하거나, 인기 라이브러리 및 개발 도구를 변조해 정상 업데이트 및 의존성 설치 과정을 통해 악성코드를 광범위하게 유포**했다. 이러한 공격은 개발 및 CI/CD 환경을 감염시켜 소스코드 탈취, 백도어 삽입, 자격 증명 수집 등으로 이어졌다. 그 결과, 금융, 암호화폐, 클라우드, 공공기관 등 다양한 산업이 연쇄 피해를 입었다. 특히, 2025년에는 정상 서명 및 자동 배포 체계를 악용한 공급망 공격이 다수 확인되면서, 오픈소스 생태계 전반의 신뢰성과 무결성에 심각한 위협이 제기되었다.

2. 도난 자격 증명 및 MFA 우회 (T1078)

2024년 하반기 이후, 스피어 피싱과 정보 유출을 통한 자격 증명 탈취가 급증했다. 공격자는 **유효 계정을 확보해 VPN, SSO, 클라우드 환경에 침투하고, MFA 우회를 위해 EvilProxy 등 프록시 기반 인증 중간자 공격 도구를 사용**하거나, 사용자 단말에 다수의 인증 요청을 반복 전송해 실수로 승인을 유도하는 방식도 활용한다. APT29, Scattered Spider 등은 이 기법으로 장기간 은닉과 내부망 거점 확대에 성공했다. 악성코드 없이 정상 계정만으로 침투해 탐지가 어렵고, 성공 시 권한 상승과 중요 자산 접근으로 이어져 조직에 중대한 위협이 된다.

3. 클라우드 환경 침해 및 리패트리에이션

클라우드 리패트리에이션(Cloud Repatriation)은 비용 최적화, 성능 개선, 규제 대응을 위해 핵심 데이터나 워크로드를 온프레미스로 이전하는 전략이다. 다만, CSP의 보안 기능 부재로 인해 보안 설정 누락, 구성 오류 등 리스크가 수반될 수 있다. 특히, 클라우드 환경에서는 Oauth 토큰 탈취, 자격 증명 남용을 통한 측면 이동, 권한 확장 등을 통한 침해가 늘어나고 있다. 이에, 인증, 권한, 가시성 강화와 함께 리패트리에이션 시 보안 정책 재정비가 요구된다.

4. AI/LLM 기반 공격 고도화

공격자는 **AI와 대형 언어 모델(LLM)을 활용해 악성코드 자동 생성, 탐지 회피, 정교한 피싱 문안 및 딥페이크 콘텐츠 제작 등을 자동화**하고 있다. 그 결과 공격의 정확성과 효율성이 크게 향상되고, 전통적인 위협 탐지 기법만으로는 차단이 점점 어려워지고 있다. 또한, 자동화된 도구를 이용해 대규모 표적화 공격을 신속하게 설계 및 전개하여, 방어자가 대응할 수 있는 시간도 줄어들고 있다. 이와 같은 흐름으로 AI 기반 공격은 더욱 다양해지고 고도화될 것으로 전망된다.

2025 공격 기법 Top 10

1. 소프트웨어 공급망 공격
2. 도난 자격 증명 및 MFA 우회
3. 클라우드 환경 침해 및 리패트리에이션
4. AI/LLM 기반 공격 고도화
5. 원격 접속 및 경계 보안 침투
6. MoTW 우회 및 압축 포맷 악용
7. 웹 서비스 및 클라우드 악용
8. 스피어 피싱 첨부 파일 악용
9. DLL Search Order Hijacking
10. OS 내장 도구 악용 – LOTL

2025년 사이버 위협 동향

주요 위협 트렌드 - 공격 기법 Top 10

5. 원격 접속 및 경계 보안 침투 (T1133)

RDP, VPN, VDI 등 외부 원격 접속 서비스를 활용한 침투 시도가 증가하고 있다. 특히, 네트워크 경계에 위치한 방화벽, VPN 등의 취약점은 주요 진입점이 된다. 공격자는 노출된 포트, 취약한 자격 증명 및 인증 구성을 통해 초기 침입을 수행한다. 이후, SSO 세션 탈취 및 인증 우회를 통해 내부망으로 측면 이동한다. Ivanti, Fortinet, Cisco ASA, Palo Alto Networks 장비의 제로데이 취약점은 APT 공격의 주요 공격 벡터로 활용되었고, 인증 우회 및 내부망 진입 사례가 다수 보고되었다.

6. MoTW 우회 및 압축 포맷 악용 (T1553.005)

공격자는 **윈도우의 보안 기능 MoTW(Mark of the Web)를 우회하는 공격을 지속**하고 있다. MoTW는 인터넷에서 다운로드된 파일에 Zone.Identifier 메타 데이터를 부여해 SmartScreen과 Office 보호 기능으로 검증한다. 공격자는 ISO, ZIP 등 압축 포맷을 활용해 MoTW가 내부 파일에 전달되지 않도록 하거나, LNK 파일 구조 조작 및 7-ZIP 취약점(CVE-2025-0411)을 이용해 MoTW를 제거하여 경고 없이 악성 파일을 실행시킨다. 사용자는 위험을 인지하지 못한 채 악성 파일을 열게 되고, 계정 탈취나, 랜섬웨어 감염 등 추가 피해를 겪게 된다.

7. 웹 서비스 및 클라우드 악용 (T1071.001)

공격자는 **탐지 회피를 위해 C2 통신에 GitHub, Dropbox, Google Drive, Telegram 등 정상적인 웹 서비스와 클라우드 플랫폼을 활용**한다. 네트워크 트래픽을 일반 사용자 활동처럼 위장해 방화벽이나 IDS로는 식별이 어렵다. 2024년에는 CloudSorcerer라는 공격 그룹이 GitHub에 암호화된 명령을 숨기고 Microsoft Graph API와 Yandex Cloud를 통해 피해 시스템과 통신한 사례가 있었다. Gamaredon, Kimsuky, PteroBox 등 APT 조직도 이 기법을 활용한다. 이제, 클라우드 기반 C2는 대표적인 은닉형 침투 전략으로 자리 잡았다.

8. 스피어 피싱 첨부 파일 악용 (T1566.001)

2024년 하반기 이후, 공격자는 **사회공학 기법 기반 스피어 피싱을 주요 침투 수단으로 활용**하고 있다. LNK, CHM, ZIP/RAR 파일 등이 지속적으로 사용되고 있다. 최근에는 첨부 파일 대신 악성 URL 및 QR 코드를 활용하는 방식도 활용한다. 그 외, 클릭픽스(ClickFix) 기법을 통해 사용자의 클릭, 인증 정보 입력, 악성 파일 설치를 유도하기도 한다. CrowdStrike 및 Microsoft 사례에 따르면 이와 같은 ClickFix 유형 공격은 내부망 접근과 자격 증명 탈취의 주요 경로로 활용된다. MuddyWater, Konni 등 APT 그룹이 초기 침투 이후 측면 이동에 활용한 정황이 보고되었다.

9. DLL Search Order Hijacking (T1574.001) DLL Side Loading (T1574.002)

DLL Search Order Hijacking은 **프로그램이 DLL을 로드할 때 윈도우 탐색 순서를 조작해 공격자가 만든 악성 DLL을 정상 DLL 대신 로드시키는 공격 기법**이다. 권한 상승, 원격 코드 실행 및 지속성 확보에 악용된다. 실제로, ShadowPad 연계 랜섬웨어 캠페인과 NI LabVIEW의 제어되지 않은 검색 경로 취약점(CVE-2025-2630) 등에 활용되었다. 흔히, 공격자들은 취약 경로에 악성 DLL을 배치하거나 설치·업데이트 프로세스 동작을 조작해 장기간 탐지를 회피하며 권한을 유지한다.

10. OS 내장 도구 악용 – LOTL (T1059)

공격자는 **악성코드 흔적 최소화를 위해 PowerShell, WMI, rundll32, mshta 등 윈도우 정상 파일을 사용하는 LOTL(Living Off The Land) 기법을 사용**한다. 이 기법은 백신, EDR 등의 방어 체계를 우회하고 정상 프로세스에 악성 행위를 은닉한다. Microsoft의 조사에 따르면 Volt Typhoon 등 중국계 APT 그룹은 미 국방·통신·에너지 인프라 대상 침투에서 wmic, netsh, PowerShell을 사용해 권한 획득, 자격 증명 수집, 내부망 정찰을 수행했다. LOTL은 탐지 우회와 장기 은닉에 효과적이며, 자격 탈취·권한 상승·데이터 유출까지 이어질 수 있다.

2025년 사이버 위협 동향

주요 위협 트렌드 – 취약점 Top 10

1. Ivanti Connect Secure VPN 취약점 (CVE-2024-21887, CVE-2025-22457 등)

APT 그룹들이 **최초 침투에 방화벽, SSL VPN 등 네트워크 보안 제품 취약점을 활용하는 사례가 많아지고 있다.** 특히 Ivanti Connect Secure VPN의 인증 우회 취약점(CVE-2023-46805)과 커맨드 인젝션 취약점(CVE-2024-21887)은 올해까지도 공격자들의 주요 표적이 되었다. 2025년 4월 공개된 버퍼 오버플로우를 통한 원격 코드 실행 취약점(CVE-2025-22457)은 중국계 APT 그룹 UNC5221이 사용했다. 취약점을 통해 웹셸 및 백도어를 배포해 정부 기관과 금융사에 침투한 것으로 확인된다.

2. Fortinet 제품 취약점 (CVE-2025-24472)

2025년 초 FortiOS와 FortiProxy 인증 우회 취약점(CVE-2025-24472)이 공개되었다. 공격자는 **이 취약점을 악용해 최고 관리(Super Admin) 권한을 획득해 네트워크 전체를 제어**할 수 있게 되었다. 초기 침투 단계에서 이 취약점을 활용한 사례가 보고되었고, 대기업과 금융 기관들이 심각한 피해를 입었다. 취약점 PoC가 공개된 이후 공격 시도가 급증했다.

3. Palo Alto Networks 방화벽 및 PAN-OS GlobalProtect 취약점 (CVE-2024-0012 등)

Palo Alto Networks의 PAN-OS 관리 웹 UI 인증 우회(CVE-2024-0012, CVE-2025-0108)를 발판으로 권한 상승(CVE-2024-9474)과 인증 후 파일 읽기(CVE-2025-0111)가 연계되어 **관리자 또는 루트 권한 장악과 구성 변조, 민감 정보 접근으로 이어지는 취약점 악용 사례**가 있었다. GlobalProtect 측면에서는 CVE-2024-3400 제로데이가 대표적인 취약점 사례다. 원격 셸 수립과 내부 네트워크 측면 이동이 확인되었다. 이에 관해, 미국 보건복지부(HHS)의 보안팀(HC3)은 헬스케어 산업군을 주요 표적 산업군으로 지목했다.

4. Cisco ASA/Firepower 취약점 (CVE-2025-20333, CVE-2025-20362 등)

Cisco ASA와 Firepower 장비에서 ArcaneDoor 계열 활동과 연관된 제로데이 및 N데이 취약점이 발견되었다. CVE-2025-20333은 VPN 웹 서버 취약점을 통해 원격 코드 실행을 가능하게 한다. CVE-2025-20362는 인증 없이 제한된 URL 접근을 허용한다. 두 취약점은 실제 공격에서 연쇄적으로 활용되었다. 미국 CISA는 연방 기관에 자산 식별, 포렌식 수집, 신속한 완화와 패치 적용을 요구했다. Cisco는 ROMMON과 부트 체인 조작을 통한 지속성 확보 전술도 확인했다. 이 사례는 방화벽이 단발성 침해를 넘어 장기간 거점으로 활용될 수 있음을 보여준다.

2025 취약점 Top 10

1. Ivanti Connect Secure VPN
2. Fortinet – FortiOS/FortiProxy
3. 팔로알토 – 방화벽/GlobalProtect
4. Cisco ASA/Firepower
5. 파일 전송 솔루션 (MOVEit, Cleo 등)
6. Sitecore RCE
7. 웹 브라우저 제로데이
8. 안드로이드 권한 상승
9. 압축 프로그램
10. 오픈소스 소프트웨어 공급망

2025년 사이버 위협 동향

주요 위협 트렌드 – 취약점 Top 10

5. 파일 전송 솔루션 취약점 (MOVEit, Cleo 등)

Cleo Harmony, VLTrader 등 MFT 제품에서 원격 코드 실행과 인증 우회 취약점이 확인되었다. CLOP 랜섬웨어가 이를 활용해 여러 조직에 피해를 입혔다. CVE-2024-50623은 무제한 파일 업로드·다운로드를 악용해 원격으로 코드를 실행한다. CVE-2024-55956은 Autorun 디렉터리 설정을 악용해 인증 없이 명령 실행을 허용했다. MOVEit Transfer의 CVE-2024-5806은 SFTP 인증 처리 문제로 인증 우회가 가능했다. Safe Wallet 프론트엔드 자산이 손상되고 자금 탈취가 발생했다. FBI는 이를 북한 공격 그룹 TraderTraitor의 활동으로 지목했다.

6. Sitecore RCE 취약점 (CVE-2025-534690)

Sitecore의 ViewState 역직렬화 취약점(CVE-2025-534690)은 사전 인증 없이 원격 코드 실행을 가능하게 한다. 오래된 배포 가이드에서 제공된 샘플 machineKey 재사용이 공격의 시발점으로 지적됐다. 2024년 말부터 악용 정황이 관측되었고, 2025년 9월 공식 권고가 나왔다. 공격자는 인터넷에 노출된 Sitecore 인스턴스를 통해 초기 접근을 확보한 뒤 원격 셸을 설치하고, 시스템 및 도메인 정찰, 자격 증명 수집 및 내부 측면 이동을 수행했다. 이후 설정 파일과 비밀 키 등 민감 정보를 탈취했다.

7. 브라우저 제로데이 취약점 (Google Chrome: CVE-2024-4947, Mozilla Firefox CVE-2024-9680)

웹 브라우저에서 발견된 제로데이 취약점이 실제 공격에 활용되었다. Chrome V8 엔진 취약점(CVE-2024-4947)은 **제작된 웹페이지 접속만으로 코드 실행이 가능하며, 라자루스 계열 공격 그룹이 금융 분야를 공격하는데 활용**했다. Firefox의 Use-After-Free(CVE-2024-9680)는 러시아 APT 그룹 RomCom이 유럽과 북미 스파이 캠페인에서 백도어를 설치하는데 활용했다. 이 취약점들은 자격 증명 탈취, 페이로드 실행, 지속성 확보로 이어지는 공격 흐름이 특징이다.

8. 안드로이드 권한 상승 취약점 (Android CVE-2025-38352)

Android CVE-2025-38352는 로컬 권한 상승을 통해 악성 앱이 기기 권한을 확대하는 데 사용되었다. 특히, 전체 공격 흐름에서 웹 브라우저 제로데이 취약점과 결합해 초기 기기 장악 후 자격 증명 탈취, 추가 페이로드 실행으로 이어지는 사례가 관찰됐다. 악성 앱은 권한을 확장해 시스템 설정 변경, 민감 데이터 접근, 보안 기능 비활성화까지 가능하다. 모바일 사용자를 겨냥한 표적 공격에서 금융 정보 탈취나 스파이 활동으로 연결될 위험이 있다.

9. 압축 프로그램 취약점 (CVE-2025-0411, CVE-2025-8088 등)

공격자들은 압축 프로그램도 공격 수단으로 활용하고 있다. 이와 관련, **개인과 기업 환경에서 널리 사용되는 7-Zip과 WinRAR 취약점을 악용한 공격 사례가 확인**되었다. 7-Zip의 MoTW 우회 취약점(CVE-2025-0411)은 러시아 공격 그룹이 우크라이나 정부 기관과 민간 조직을 대상으로 SmokeLoader를 배포하는 데 사용되었다. WinRAR에서는 경로 탐색 취약점(CVE-2025-6128, CVE-2025-8088)이 발견되었다. 특히, CVE-2025-8088은 RomCom이 유럽과 캐나다의 물류, 제조, 금융, 방산 기업을 공격하는 데 활용한 것으로 알려졌다.

10. 오픈소스 소프트웨어 공급망 취약점 (예: npm 패키지)

JavaScript npm 패키지 등 **널리 사용되는 오픈소스 라이브러리에서 유지보수 인원의 계정 탈취와 악성코드 주입이 결합된 공급망 공격**이 잇따랐다. 2025년 9월 npm에서 유지 보수 인원 피싱과 토큰 탈취로 인기 패키지 다수가 오염되었다. 같은 시기에 PyPI는 개발자 대상 이메일 피싱 캠페인을 공식적으로 경고하고 계정 탈취 위험을 공지했다. 컨테이너 영역에서는 XZ 백도어가 포함된 Docker Hub 이미지가 다수 남아 있다는 사실이 확인되고, 공급망 노출로 이어졌다. 이 밖에, Rust 생태계에서도 지갑 키를 훔치는 악성 크레이트가 발견되어 즉시 제거되었다.

2025년 사이버 위협 동향

주요 위협 트렌드 - 모바일 Top 6

1. 사회공학 기법 기반 모바일 범죄 고도화

2025년에는 사회공학 기법을 활용한 모바일 범죄가 더욱 고도화되었다. 주로 유포 시점의 사회적 이슈를 반영해 제작 및 배포된 것이 특징이다. **국내 통신사, AI 앱, 공공기관 등을 사칭해 피해자의 관심을 끄는 위장 앱들이 사용**된다. 또한, 급등주, 공모주 투자나 연인 관계를 빙자해 내적 친밀감을 형성한 후 투자로 유도하는 스캠 앱도 다수 발견되었다. 이 앱들은 고수익을 보장한다는 명목으로 피해자를 현혹하고, 악성 앱 설치를 요구한다.

피해자는 투자금을 입금한 후 앱을 통해 실시간으로 조작된 수익률을 확인하게 된다. 출금 요청 시에는 다양한 이유를 들어 투자금을 돌려주지 않고 잠적하는 사례가 다수 발생하고 있다. 이 외에도, 은밀한 대화를 할 수 있다는 명목으로 앱 설치를 유도한 뒤, 피해자의 연락처와 사진 등을 탈취하고 이를 기반으로 유포를 협박해 자금을 요구하는 몸캠 피싱 사례도 지속적으로 발견되고 있다.

2. 새로운 공격 기능이 탑재된 악성 앱

안드로이드의 HCE(Host Card Emulation)를 이용해 NFC 통신을 가로채는 기법을 활용한 악성 앱이 고도화되고 있다. NGate라는 이름으로 불리는 이 앱은 NFC 통신을 가로채는 기능 외에도 가짜 화면을 띄워 사용자 크리덴셜 정보를 탈취하는 기능도 포함한다.

이 앱들은 NFC 기반 장비와 접촉 시 발생하는 통신 정보를 공격자에게 전송한다. 공격자는 NFC 통신 정보를 바탕으로 ATM 무단 출금 등을 수행한다. 암호화폐 정보를 탈취하기 위해 OCR(광학 문자 인식) 라이브러리를 활용한 악성 앱도 새롭게 발견되었다. 이 앱은 사용자가 암호화폐 지갑 백업을 위해 사용하는 니모닉(Mnemonic) 관련 정보를 이미지로 저장하는 점을 악용했다. 공격자는 OCR 기술을 활용해 이미지 내에 포함된 니모닉 문구와 암호화폐 관련 정보를 자동으로 분석하고 추출 및 탈취한다.

3. 공식 스토어 내 악성 앱 유형 다양화

공식 앱 스토어에서도 다양한 유형의 악성 앱이 지속적으로 발견되고 있다. 최근에는 금융정보 탈취(Banker), 고금리 대출(SpyLoan), 암호화폐 정보 탈취(SparkCat, SparkKitty), 은닉 광고 실행(HiddenAds), 투자 사기(ScamFX) 등 다양한 앱들이 발견되고 있다.

특히, Banker 유형은 악성 기능을 포함할 경우 앱 스토어 보안 검사에 의해 탐지될 가능성이 높기 때문에, **정상 앱으로 위장해 등록한 후 설치한 뒤에 악성 페이로드를 외부에서 다운로드 받아 실행하는 방식으로 진화**했다. 일부 악성 앱은 사용자 환경에 따라 악성 기능을 조건부로 활성화하거나, 특정 국가 및 언어 설정에서만 악성 행위를 수행하는 등 지능적으로 동작하는 경우가 많다.

Key Point

- 모바일 사회공학 기법, 통신사, AI 앱, 공공기관 등을 사칭해 피해자의 관심을 끄는 위장 앱 활용
- 안드로이드의 HCE(Host Card Emulation)를 이용해 NFC 통신을 가로채는 악성 앱 등장
- 앱 스토어에 정상 앱으로 등록한 후 악성 페이로드를 외부에서 다운로드 받아 실행하는 방식으로 진화

2025년 사이버 위협 동향

주요 위협 트렌드 - 모바일 Top 6

4. 다양한 취약점 활용 공격

RCE(Remote Code Execution), 권한 상승(EoP) 등 **공개된 CVE 외에도, 등록되지 않은 미공개 취약점을 악용한 공격이 지속적으로 발견**되고 있다. 이러한 취약점은 보고되기 전까지 알려지지 않기 때문에, 공격자는 이를 '제로데이(Zero-Day)'로 활용해 악성 앱을 제작 및 유포한다. 피해자는 보안 패치가 적용되기 전까지 무방비 상태로 노출될 수 있다.

대표적으로 Pixnapping 취약점이 있다. 이 취약점을 악용하면 안드로이드 13~16 버전 특정 단말기에서 반투명 오버레이와 정밀한 타이밍을 이용해 픽셀 데이터를 추출할 수 있다. 이를 통해 MFA 인증코드 등 민감한 정보를 탈취한다. CVE-2024-43093 취약점은 ContactsDirectory를 악용해 사용자 상호 작용 없이 앱을 자동 실행할 수 있는 권한 상승 취약점이다. 사용자 몰래 악성 앱을 실행하거나 백그라운드에서 악성 기능을 활성화할 수 있다. 실제로 이러한 기능을 수행하는 악성 앱이 발견된 사례도 있다.

5. 북한 연계 사이버 공격 그룹 활동

북한 연계 공격 그룹이 대한민국을 대상으로 민감 정보를 탈취하기 위한 스파이 앱을 지속적으로 유포하고 있다. 주로 **파일 관리자, 소프트웨어 업데이트, 보안 문서 뷰어 등 유틸리티 앱으로 위장**해 사용자의 의심을 피하고, 정상 앱처럼 보이도록 UI와 기능을 정교하게 설계했다.

또한, 분석을 방해하기 위해 코드 난독화, 암호화, 동적 로딩, 조건부 실행 등 다양한 기법을 적용했다. C2 서버를 통해 명령을 수신하고 탈취한 정보를 외부로 전송하는 기능도 포함되었다. 일부 악성 앱의 C2 서버에서는 코인 피싱 사이트도 존재한다. 이는 암호화폐 관련 자산 탈취까지 범위를 확장하고 있음을 보여준다.

6. 악성코드 선탑재 장비 유포

최근, 안드로이드 OS 기반 스마트폰, 셋톱박스(set-top box) 등 **일부 장비가 제조사 출고 전부터 악성코드가 포함된 상태로 유통되는 사례가 발견**되었다. 이 장비들은 정상 제품보다 저렴한 가격을 내세워 소비자를 현혹한다. 장비 내부에는 디도스나 크리덴셜 스터핑 공격을 수행하는 Mirai 악성코드, 광고 수익을 노리는 HiddenAds 유형의 악성코드가 포함되어 있다. 악성코드는 사용자가 인지하지 못한 상태에서 장기간 동작한다. 네트워크 트래픽 증가, 배터리 소모, 개인정보 유출 등의 피해로 이어질 수 있다.

또한, USB 케이블을 통한 해킹 사례도 지속적으로 보고되고 있다. 내부에 데이터 전송 기능을 악용한 악성 칩셋이 포함되어 있고, 연결 기기에서 파일 접근, 명령 실행, 정보 탈취 등이 가능하도록 설계되어 있다.

Key Point

- 공개된 CVE 외에도, 등록되지 않은 미공개 취약점을 악용한 모바일 공격 지속적으로 발견
- 북한 연계 그룹 - 주로 파일 관리자, 소프트웨어 업데이트, 보안 문서 뷰어 등 유틸리티 앱으로 위장
- 스마트폰, 셋톱박스 등 일부 장비가 제조사 출고 전부터 악성코드가 포함된 상태로 유통되는 사례 발견

2025년 사이버 위협 동향

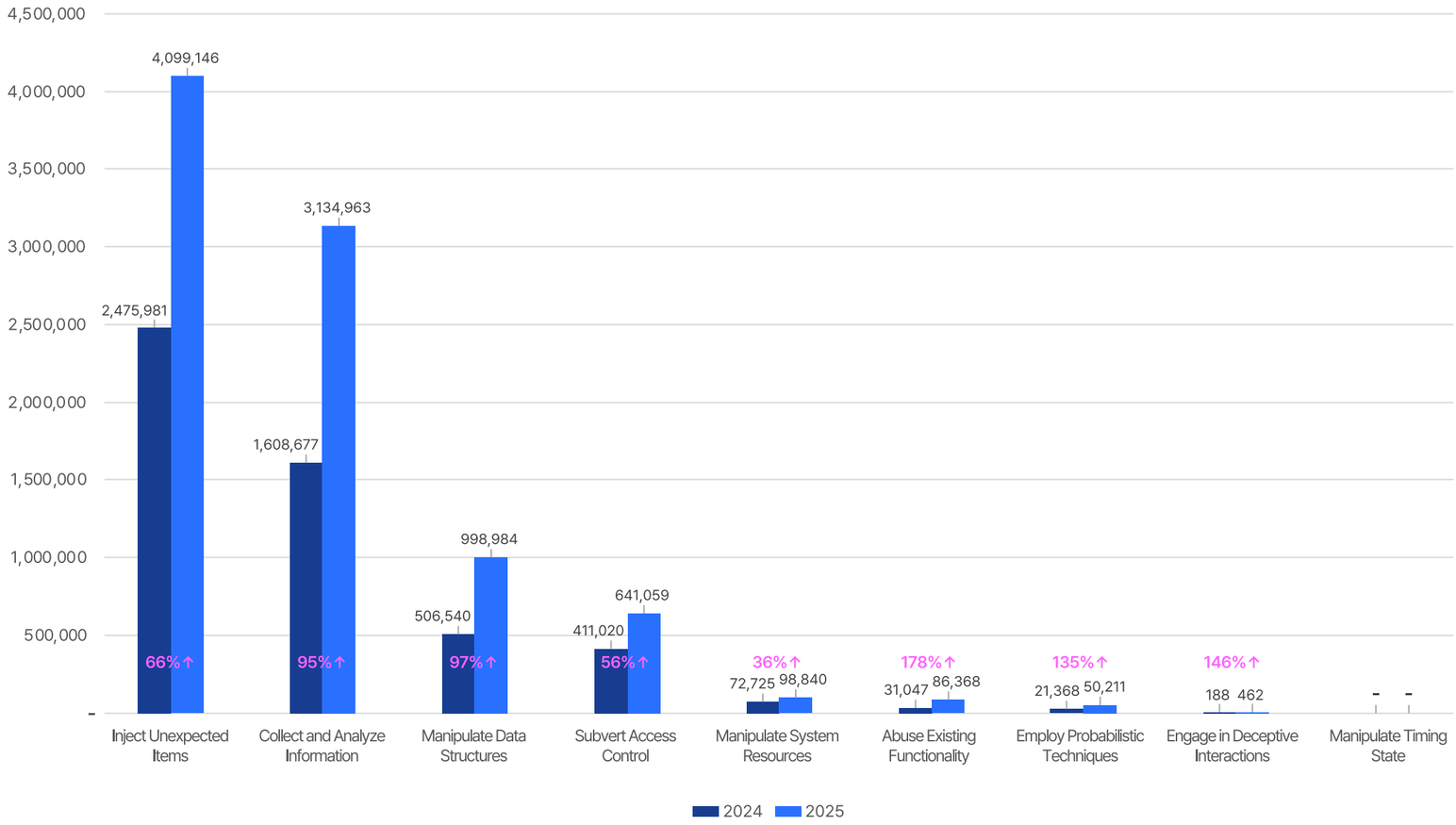
공격 유형 통계

안랩의 침해 대응 전문 조직 'CERT(Computer Emergency Response Team)'는 매월 사이버 위협 추이를 분석한 'CERT 월간 보고서'를 발행하고 있다. 해당 보고서를 기반으로 정리한 2025년 사이버 공격 유형 통계를 공개한다.

2025년, **전체 공격 탐지 건수는 전년 대비 78% 증가했다. 모든 유형이 전년 대비 두 자리 수 이상 늘어났으며,** 일부는 100% 넘게 증가하기도 했다. AI 기반 공격 고도화, 클라우드 환경 확대, 공급망 취약점 악용 등 다양한 요인이 복합적으로 작용한 결과로 분석된다.

가장 많이 발생한 유형의 공격은 **예상치 못한 데이터 인젝션(Inject Unexpected Items)**으로, 2024년에 이어 1위를 기록했다. 정보 수집 및 분석(Collect and Analyze Information), 데이터 구조 변경(Manipulate Data Structures), 접근 제어 조작(Subvert Access Control), 시스템 리소스 변경(Manipulate System Resources)이 뒤를 이었다.

2025년 공격 유형 순위



2025년 사이버 위협 동향

공격 유형 통계 – 유형 설명

1. Inject Unexpected Items

예상치 못한 데이터 인젝션(Inject Unexpected Items)는 **공격자가 시스템 데이터 입력 인터페이스를 통해 비정상 혹은 예외적인 데이터를 주입해 동작을 제어 혹은 방해하는 기법**이다. 입력 값 검증이 미흡한 경우, 입력 처리 로직이 허술한 경우 등에 발생한다. 시스템은 주입된 값에 따라 비정상 동작, 보안 정책 우회, 정보 유출 등의 문제를 겪을 수 있다.

2. Collect and Analyze Information

데이터 정보 수집 및 분석(Collect and Analyze Information)은 **공격자가 능동적 질의나 수동적 관찰을 통해 대상 시스템 정보를 확보하고 분석하는 공격 기법**이다. 공격자는 시스템 구성, 사용자 계정 등 세부 정보를 수집해 향후 공격 경로를 설계하거나 잠재적인 취약점을 식별한다. 이러한 과정은 초기 침투를 위한 준비 단계로 활용된다.

3. Manipulate Data Structures

공격자가 **시스템 내부 데이터 구조를 의도적으로 변경하여 정상적인 데이터 처리 흐름을 깨뜨리는 공격 방식**이다. 이를 통해, 시스템의 내부 데이터 흐름을 방해하거나 변조하여 비정상적인 결과를 유도한다. 이러한 조작은 예기치 않은 오류를 일으킬 뿐 아니라 데이터의 신뢰성까지 손상시킨다.

4. Subvert Access Control

접근 제어 조작(Subvert Access Control)은 **공격자가 접근 제어 메커니즘을 우회하거나 무력화해 허가되지 않은 권한을 획득하고 시스템에 부적절하게 접근하는 공격 방식**이다. 이를 통해, 관리자 권한이나 고급 사용자 권한을 확보하여 민감 데이터에 접근하거나 특정 기능을 조작할 수 있다.

5. Manipulate System Resources

피해자의 **CPU, 메모리 등 시스템 리소스를 과도하게 소모하도록 하여 성능을 저하시키거나 자원을 고갈시키는 방식**이다. 시스템은 정상적인 서비스를 제공하기 어려워지고, 사용자는 응답 속도가 느려지거나 시스템이 정지를 겪게 된다. 자원 고갈은 장기적으로 서비스 거부(DoS) 공격과 유사한 피해를 입히며, 시스템 가용성을 저해한다.

6. Abuse Existing Functionality

공격자가 **시스템이나 애플리케이션의 정상 기능을 활용해 피해를 유발하는 공격 기법**이다. 새로운 코드를 추가하지 않고, 기존 기능을 악용하는 것이 특징이다. 예를 들어, 고객 서비스의 파일 업로드 기능을 악성 파일 전달에 이용하거나, 검색 기능을 통해 내부 정보를 노출시키는 방식이 있다.

7. Employ Probabilistic Techniques

공격자가 **확률적 접근 방식을 통해 시스템 취약점을 탐색하거나 공격 성공 가능성을 점진적으로 높이는 기법**이다. 대표적으로, 브루트 포스(Brute Force)와 타이밍 공격이 있다. 암호 추측 등을 통해 시간이 지남에 따라 성공 확률을 높인다. 암호화 체계와 인증 절차가 취약한 시스템에 효과적이며, 사용자가 인지하지 못하는 사이에 침입한다.

8. Engage in Deceptive Interactions

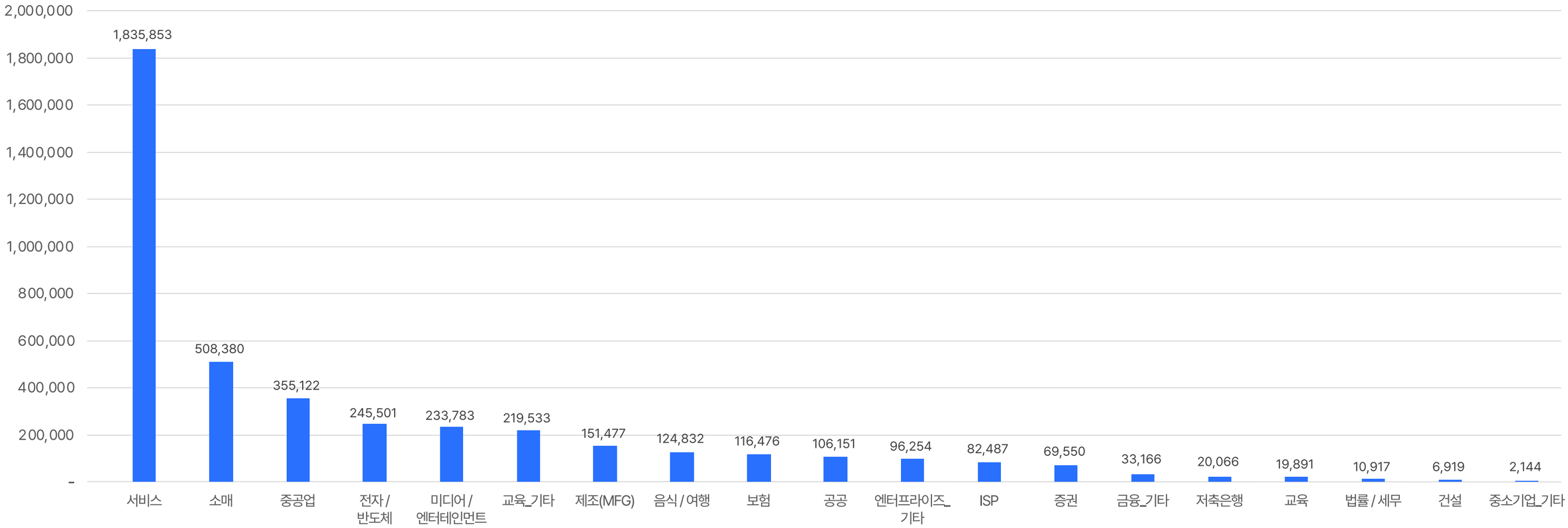
공격자가 **시스템이나 사용자와 상호 작용할 때 신원과 의도를 숨기고 잘못된 정보를 전달해 원하는 결과를 얻는 공격 기법**이다. 대표적으로, 피싱, 사회공학 기법, 가짜 웹사이트 및 이메일을 이용한 스캠이 있다. 이러한 방식은 사용자를 속여 신뢰를 얻은 뒤, 민감 정보 입력 혹은 악성 파일 다운로드를 유도한다.

2025년 사이버 위협 동향

공격 유형 통계 – 산업군 별 공격 횟수

2025년 하반기 산업군 별 공격 횟수를 보면 서비스업이 1,835,853 건으로 가장 많았다. 소매(508,380), 중공업(355,122), 전자/반도체(245,501)가 뒤를 이었다.

2025년 하반기 산업군 별 공격 횟수



2025년 사이버 위협 동향

공격 유형 통계 – 산업군 별 공격 유형

2025년 하반기 산업군 별 공격 유형 비율

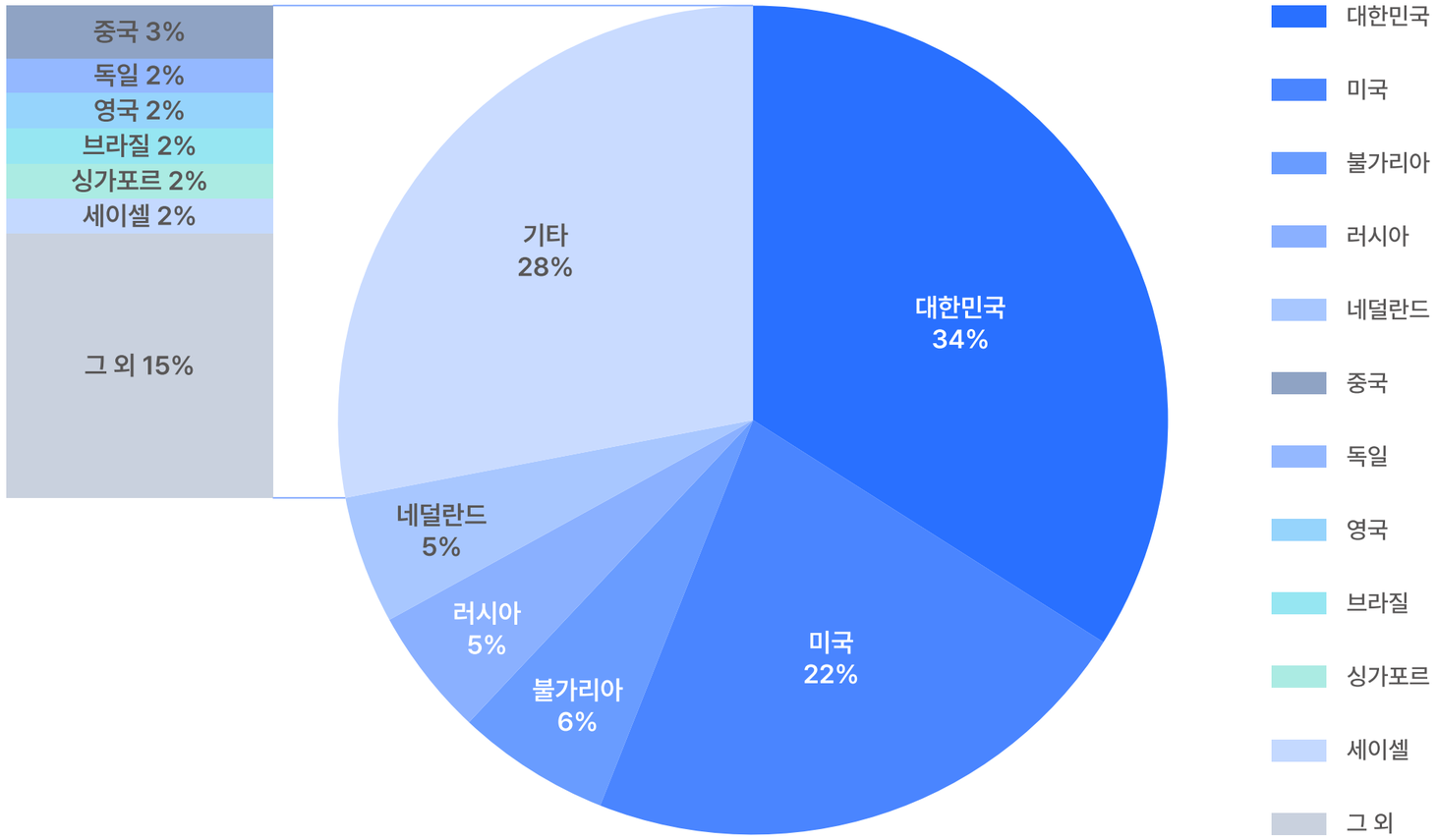
	Inject Unexpected Items	Collect and Analyze Information	Manipulate Data Structures	Subvert Access Control	Manipulate System Resource
서비스	**43%**	33%	12%	9%	1%
소매	37%	**50%**	7%	3%	1%
중공업	**51%**	34%	8%	3%	1%
전자/반도체	**48%**	14%	20%	12%	1%
미디어/엔터테인먼트	38%	**40%**	9%	10%	2%
교육_기타	28%	**62%**	6%	3%	1%
제조(MFG)	**48%**	37%	11%	2%	1%
음식/여행	41%	**48%**	6%	5%	0%
보험	30%	**62%**	4%	4%	0%
공공	40%	**45%**	7%	5%	1%
엔터프라이즈_기타	**50%**	41%	6%	2%	0%
ISP	38%	**53%**	6%	3%	0%
증권	**53%**	30%	9%	3%	4%
금융_기타	**44%**	39%	12%	3%	1%
저축은행	**41%**	36%	10%	8%	0%
교육	**49%**	42%	6%	3%	1%
법률/세무	**50%**	29%	13%	6%	0%
건설	35%	**51%**	8%	4%	1%
중소기업_기타	**80%**	1%	9%	3%	0.0%

2025년 사이버 위협 동향

대한민국 공격 국가 통계

안랩의 보안 장비별 탐지 로그를 출발지 IP 주소 기준으로 분석한 결과, **국내 IP 주소를 사용한 공격 시도 비율이 34%(+7%)로 가장 높게 나타났다.** 미국 22%(전년 대비, -2%), 불가리아 6%(-1%), 러시아 5%(+0%), 네덜란드 5%(+1%)가 뒤를 이었다. 중국은 2024년 6%에서 3%로 감소하며 6위를 기록했다. 국내외 다양한 위협 주체들이 한국을 주요 타깃으로 삼고 있음을 보여준다. 특히, **국내 IP를 활용한 공격은 내부자 위협 또는 IP 위장 가능성도 함께 고려해야 한다.**

2025년 대한민국 대상 공격 국가 비율



2026년 전망

→ 2026년 전망 Top 5

1. AI 기반 사이버 공격의 전방위 확산

2. 랜섬웨어 공격 확대 및 피해 심화

3. 오픈소스 생태계를 이용한 공급망 공격

4. 국가 핵심 인프라에 대한 위협 확대

5. 증가하는 리눅스 위협

2026년 전망

#1. AI 기반 사이버 공격의 전방위 확산

→ 안랩의 AI 보안 전략 자세히 알아보기

AI를 활용한 '맞춤형' 공격

2026년에는 AI가 실시간으로 피해자의 환경을 분석하고, 표적을 정확하게 타격할 수 있는 악성코드를 생성해 실행하는 적응형 공격이 확대될 것이다. 특히, AI는 탐지 회피를 위한 다양한 변형 코드를 생산해 낼 수 있어, 기존 보안 시스템을 우회할 수 있게 된다. 이로 인해, 정적 탐지 중심의 보안을 넘어 동적 분석과 행위 기반 탐지의 중요성이 더욱 부각될 전망이다.

또한, 딥페이크 기술 고도화로 실제 인물의 음성이나 얼굴을 정밀하게 모방한 실시간 피싱이 화상 회의나 전화 통화에 악용될 것으로 예측된다. 딥페이크 기술의 품질이 갈수록 향상되면서, 특정 인물의 목소리를 이용해 금융 정보 등 민감 데이터를 탈취하는 등의 딥페이크 공격은 피해자가 식별하기 어려운 수준까지 진화할 것으로 보인다.

AI를 활용한 스캠 자동화도 주목해야 한다. 가짜 투자 사이트, 챗봇, 쇼핑몰 등을 대량 생성해 피해자와 자연스럽게 상호작용하도록 할 전망이다. 이미 공격자들은 AI를 기반으로 육안으로 구분이 어려운 수준의 피싱 웹사이트와 이메일을 제작하고 있으며, 이러한 자동화 및 대량 생산 능력은 자연스럽게 공격 캠페인의 폭발적인 증가로 이어질 것이다.

이 밖에, AI는 공격자가 새로운 해킹 기법을 개발하는 데에도 큰 기여를 할 것이다. 취약점 탐지와 패턴 분석을 통해 알려지지 않은 보안 취약점을 찾아 제로데이(Zero-Day) 공격에 활용할 수도 있다. 결국, 공격자의 AI 활용은 해킹의 진입 장벽을 낮추면서, 공격 빈도와 정확도는 높여주게 된다.

AI를 노린 공격 확대

AI 모델 자체를 공격 대상으로 삼는 공격 기법도 더욱 발전할 것이다. 공격 기법은 크게 ▲프롬프트 인젝션 및 데이터 포이즈닝 ▲프롬프트 유출 ▲모델 역분석 등이 있다. 우선, 공격자는 챗봇, 자동 분석 시스템, 보안 AI 등에 악의적인 입력을 주입하거나 학습 데이터를 조작해 의도된 오작동이나 정보 노출을 유도한다. 이는 AI를 사용하는 시스템, AI 기반 보안 솔루션 등의 신뢰성과 무결성을 근본적으로 위협하는 요소로 작용하게 된다.

공격자는 프롬프트 유출을 통해 AI에 대한 프롬프트를 탈취할 수도 있다. 프롬프트가 깃허브(GitHub) 등 코드 공유 플랫폼을 통해 유출되면, 공격자가 이를 악용해 AI를 왜곡하는 것이다. 최근 AI 모델 사용이 늘어남에 따라 프롬프트 유출과 이를 방어할 데이터 보안에도 각별한 주의가 요구될 전망이다.

또한, 공격자는 AI 모델에 반복적인 쿼리를 수행해 모델의 작동 방식을 분석하고, 학습 데이터를 탈취하는 모델 역분석을 수행할 수 있다. 모델의 응답을 바탕으로 학습 데이터와 내부 구조를 파악하고, 민감 정보를 유출시키는 방식이다. 공격자는 보안 취약점이 있는 AI 모델에 대해 역분석을 수행해 공격을 확대해 나갈 것으로 보인다.

Key Point

- AI 기반 악성코드, 딥페이크, 스캠 자동화, 제로데이 취약점 발견 등 타깃 맞춤형 공격 증가
- AI 모델 사용이 증가함에 따라 프롬프트 인젝션, 프롬프트 유출, 모델 역분석 등 AI를 겨냥한 공격 기법도 고도화

2026년 전망

#2. 랜섬웨어 공격 확대 및 피해 심화

→ 안랩의 랜섬웨어 통합 보안 전략 자세히 알아보기

랜섬웨어 조직의 파편화 및 카르텔화 가속

2025년, 록빗(LockBit), 랜섬허브(RansomHub) 등 대형 랜섬웨어 그룹들의 세력이 약화되거나 활동이 중단되었다. 그렇지만, 랜섬웨어 생태계 자체가 약화된 것은 아니다. 대형 그룹 약화의 반작용으로 Akira, Qilin, Play, Gunra 등 수많은 소형·신생 그룹이 대거 등장했다. 앞서, 2025년 동향에서 살펴본 바와 같이 신생 그룹들은 활발하게 공격을 수행하고 있으며, 이렇게 재편된 랜섬웨어 생태계는 2026년에도 같은 모습을 띌 전망이다.

APT 그룹-랜섬웨어 조직 간 협력 및 RaaS 기반의 '랜섬웨어 카르텔화'는 2026년 더욱 심화될 것으로 보인다. 중앙 플랫폼에서 공격에 필요한 인프라와 도구를 제공하고, 계열사들이 공격을 수행한 뒤 '80 대 20'으로 수익을 배분하는 모델은 랜섬웨어 생태계에서 어느 정도 자리를 잡은 것으로 보인다. 또한, 2025년 일부 발견된 APT 그룹 – 랜섬웨어 조직 간 협력은 2026년 국가 간 지정학적 갈등이 심화되는 가운데, 더욱 활발하게 진행될 것으로 보인다.

방어자 입장에서는 공격자들이 해킹 진입 장벽이 낮아진 상황에서 더 다양하고 많은 공격을 감행할 수 있어, 보안의 난이도가 높아지게 된다. 특히, 랜섬웨어 생태계가 파편화되고 협력도 잦아져 공격 그룹을 특정하기가 더 어려워질 것으로 예상된다.

중소기업을 노린 공격 증가

2025년 랜섬웨어 동향의 주요 특징은 낮아진 진입 장벽과 공격의 다양화다. 금전적 이득이 최우선 목적인 공격자들 입장에서는 한 번의 공격으로 더 큰 수익을 낼 수 있는 대기업을 공략하는 것이 합리적이며, 2026년에도 대기업들은 랜섬웨어 그룹들의 주요 표적이 될 것이다.

다만, **다양한 공격을 더 쉽게 감행할 수 있는 현 상황에서 상대적으로 보안 태세가 취약한 중소기업 대상 공격이 더 가파르게 증가할 것으로 전망된다.** 특히, 공격자들은 랜섬웨어 신종과 변종을 만들어 공격을 지속할 수 있어, 체계적인 멀티 레이어 보안을 구축하기 어려운 중소기업 대상 공격은 성공률이 높아질 가능성이 크다.

실제, 2025년에도 공격자들이 대기업 대신 중견 기업을 주요 타깃으로 삼는 전략으로 전환하는 것이 포착된 바 있다. 규모가 작은 기업들일수록 정밀한 표적 공격, 내부자 매수, 사회공학 기법에 각별한 주의를 기울여야 한다. 또한, 유사한 공격이 언제든 다시 감행될 수 있음을 인지하고 위협을 사전에 식별해 예방할 수 있는 보안 체계를 갖춰야 한다.

Key Point

- 랜섬웨어 산업은 범죄자의 수익 모델로 자리 잡았고, 랜섬웨어 이름만 바뀔 뿐 공격은 지속 증가 예상
- 시스템 내 파일 암호화를 넘어 데이터베이스, 백업 솔루션, 가상화 환경 등에 대한 정밀한 랜섬웨어 공격 증가
- 랜섬웨어 공격 진입 장벽이 낮아진 만큼, 보안 태세가 취약한 중소기업 대상 공격이 늘어날 전망

2026년 전망

#3. 오픈소스 생태계를 이용한 공급망 공격

→ XDR과 ZTNA를 활용한 안랩의 공급망 보안 전략 자세히 알아보기

오픈소스 생태계 위협 확대

2025년, 오픈소스 패키지 레지스트리를 노린 공급망 공격이 급증했다. 악성 패키지가 대규모로 확산되었고, 개발자 및 CI/CD 환경 비밀번호와 토큰이 유출되는 사례가 다수 확인된 바 있다. 현대 소프트웨어 개발의 90% 이상이 오픈소스 컴포넌트에 의존함을 고려했을 때, 단일 패키지 침해는 수천 개 하위 프로젝트까지 연쇄 피해를 발생시킬 수 있다.

2026년에도 이러한 위협은 더욱 심화될 전망이다. 특히, **공격자가 설치 시점이나 CI 파이프라인에서 민감 정보를 수집해 연쇄 감염을 유도하는 공격이 더욱 정교화될 것**으로 예상된다. 타이포스쿼팅, 정상 패키지 유지 보수자 계정 탈취, 종속성 혼란 공격 등 다양한 수법이 복합적으로 활용될 가능성이 높다.

이러한 공급망 공격의 대상이 되는 기업 입장에서는 **오픈소스 사용 현황과 전체적인 데이터 플로우를 실시간으로 모니터링하여 오픈소스 파이프라인 전반에 걸쳐 가시성을 확보하는 것이 최우선 과제다.** 이를 통해, 취약점 발생 시 즉각적인 대응이 가능하고 피해를 최소화하면서 회복력을 갖출 수 있다.

소프트웨어에서 클라우드 및 하드웨어까지

2025년 공급망 공격은 소프트웨어를 넘어 클라우드 서비스, MSP, 보안 솔루션 제공업체까지 확대되는 모습을 보였다. 일례로, 공격 그룹 DragonForce와 Scattered Spider는 클라우드 MSP를 공격해 수십 개 고객사에 동시에 피해를 입히는 '연쇄 공급망 공격'을 실현한 바 있다.

또한, 공급망 공격에 소프트웨어를 넘어 하드웨어까지 활용되는 사례도 확인되었다. 2025년에는 안드로이드 OS 기반 스마트폰, 셋톱박스(set-top box) 등 일부 장비가 제조사 출고 전부터 악성코드가 포함된 상태로 유통되는 사례가 있었다. 이러한 장비들이 감염된 채 대규모로 유통되면 피해 규모는 가늠하기 어려울 정도로 커지게 된다.

2026년에도 공격자들은 피해 규모 확대를 위해 소프트웨어, 클라우드, 하드웨어 등 도메인을 가리지 않고 공격을 감행할 전망이다. 그리고, 공급망 공격은 이제 국경을 초월하는 사안이기 때문에, 2026년에는 범국가 간 협력 기반의 공급망 보안 프레임워크에 대한 필요성이 과거 대비 강조될 것으로 보인다.

Key Point

- 오픈소스는 현대 소프트웨어 개발의 핵심이지만, 그 개방성과 의존성 때문에 공격자에게 매력적인 표적
- 오픈소스를 안전하게 사용하기 위해 오픈소스 파이프라인 전반에 걸쳐 가시성과 통제력 확보 필요
- 2026년에는 소프트웨어, 클라우드, 하드웨어 등 도메인을 가리지 않고 공급망 공격을 감행할 전망

2026년 전망

#4. 국가 핵심 인프라에 대한 위협 확대

→ 안랩의 CPS 통합 보안 전략 자세히 알아보기

국가 기반 시설 타격 확대

2025년, 전체 랜섬웨어 공격의 절반이 제조, 의료, 에너지 등 핵심 인프라를 겨냥한 것으로 나타났다. 핵심 인프라가 집중 공격을 받는 이유는 운영 중단 우려로 인한 비용 지불 가능성, 고가치 데이터, 상대적으로 부족한 보안 투자 등 여러가지가 있다.

올해 산업군 별 피해를 보면, 서비스 산업이 디지털 전환 가속화로 가장 많은 피해를 입었다. 제조업은 스마트 팩토리 확대로 공격이 급증했다. 금기 시 되었던 의료 분야 공격도 계속 발생하고 있으며, 환자 생명과 직결된 의료기관은 고수익 표적이 되었다. 이러한 기반 시설 공격 추세는 2026년에도 계속될 전망이다.

또한, 내년에 공격이 증가할 것으로 전망되는 분야는 철도, 해상, 항공 운송 네트워크와 통신망 등이 있다. 해당 시설들의 디지털화가 진행되면서 항만과 선박 관리 시스템, 항공기 통제 시스템, 공항 보안 시스템 등이 공격 대상이 될 수 있다. 통신망은 정부, 기업, 개인의 모든 데이터를 연결하는 핵심 인프라로 공격 빈도 수가 높아지고 있으며, 2026년 공격 확대가 예상된다.

대부분 공격자들의 동기는 금전적 이익이지만, **2026년에는 일부 국가 배후 위협 그룹들이 지정학적 갈등을 이유로 공격을 감행할 것으로 보인다.** 국가 간 갈등이 계속되는 가운데, 사회 기반 시설에 대한 사이버 공격도 계속 정교화될 전망이다.

산업의 디지털화, 공격자의 표적이 될 것

국가 기반 시설 타격을 관통하는 키워드는 바로 '디지털화'다. 기존 아날로그 형태로 운영되었거나, 외부와 단절된 OT망 환경에서 운영되었던 산업 시스템들은 외부망 대비 안전하다는 인식이 있었다. 그러나 해당 환경의 디지털 전환이 가속화되면서, 외부 접점이 확대되고 공격 표면이 증가하고 있다. 공격자들은 이 확대된 공격 표면을 적극적으로 노리고 있다.

산업 시설의 디지털화로 인해 가장 두드러지는 변화는 기존 OT에서 OT와 IT를 아우르는 'CPS(Cyber-Physical System)'로의 개념 전환이다. **폐쇄된 OT 환경의 외부 접점이 늘어나면서 IT, IoT, 클라우드 연결까지 아우르는 보안이 필요해졌다.** 실제로도, 최근 스마트 제조 환경에는 IoT 포함 다양한 최신 디바이스들이 적용되는 것을 볼 수 있다.

CPS 환경을 향한 공격 수법 역시 고도화되고 있다. OT망이 IT 환경과 연결되는 특성을 노려 IT 환경을 먼저 침해한 후 OT망 내부로 침투하는 방법이 많이 쓰이고 있다. OT 환경을 노리고 제작된 악성코드와 랜섬웨어도 발견되고 있다. 이러한 CPS 환경을 노리는 공격은 2026년을 넘어 다가올 미래에도 계속 확대될 것으로 예상된다.

Key Point

- 기반 시설의 디지털화, 지정학적 갈등, 기술의 무기화가 CPS 환경의 국가 기반 시설 위협
- 국가 기반 시설 공격 발생 시 신속한 복구를 위해 백업 체계, 복구 프로세스, 모의 훈련 등 사이버 회복력 강화 필수

2026년 전망

#5. 증가하는 리눅스 위협

→ 안랩 리눅스 보안 전략 자세히 알아보기

늘어나는 취약점, 고도화되는 공격

안랩의 데이터에 따르면, 2025년 6월 한 달 동안에만 176개 리눅스 시스템을 대상으로 무려 1만 2천 건 이상의 공격이 감행되었다. 월 별로 차이가 있지만 매달 평균적으로 100개 이상의 시스템에서 수 천 건 많게는 1만 건 이상의 공격이 수행됐다고 볼 수 있다. 공격 종류도 ▲디도스 봇 ▲코인마이너 ▲백도어 ▲랜섬웨어 등으로 다양하다. 리눅스 취약점 역시 수 천개에 달하고, **리눅스 환경을 타깃한 신규 악성코드도 2025년 상반기에만 6만개 이상 발견됐다. 리눅스 환경을 향한 공격 빈도, 취약점 수, 악성코드 수는 2026년에도 증가세를 기록할 전망**이다.

2025년, 국내 통신사의 리눅스 서버가 해킹 당해 약 2,300만 명의 고객 개인정보가 유출되는 사건이 있었다. 공격에는 리눅스 기반 BPFDoor 백도어가 사용되었다. 공격자는 웹셸 및 원격 코드 실행(RCE) 취약점을 통해 내부 시스템에 침투한 뒤, HSS 서버에 BPFDoor를 설치하고 유심 정보를 탈취했다. **앞서, 2026년 국가 기반 시설 타격 확대를 전망했는데, 그 연장선에서 리눅스 서버에 대한 공격도 늘어날 것으로 보인다.**

리눅스 서버 공격이 늘어나는 이유는 간단하다. 수 많은 클라이언트 PC에 연결되어 있고 다양한 비즈니스 중요 데이터들이 저장되어 있기 때문이다. **특히, 클라우드 인프라 대부분이 리눅스 기반으로 운영되면서, 공격 표면이 급격히 확대되고 있다.** AWS, Microsoft Azure, Google Cloud 등 주요 클라우드 환경과 Docker, Kubernetes 같은 컨테이너 플랫폼이 모두 리눅스를 기반으로 한다. 리눅스 시스템 하나가 침해되면 수백 개의 가상머신과 컨테이너가 동시에 위협받을 수 있다.

아울러, **공격자들은 게스트 운영체제가 아닌 하이퍼바이저 계층을 직접 노리는 전략으로 전환하고 있다.** 2025년 6월, 아키라(Akira) 랜섬웨어는 VMware ESXi와 Hyper-V를 넘어 Nutanix AHV(Acropolis Hypervisor) 가상 머신 디스크 파일을 암호화하는 데 성공했다. 가상화 플랫폼 다변화가 공격 표면 확대로 이어지고 있다. **한 번의 침해로 수백 개 가상 머신을 몇 시간 내에 무력화시킬 수 있어 공격 효율이 극대화**된다. 랜섬웨어를 비롯해 리눅스 기반 시스템을 겨냥한 악성코드가 증가하면서, 비즈니스 중단 등 심각한 피해로 이어질 수 있다.

고도화된 리눅스 공격은 단편적인 보안 접근으로는 대응이 어렵다. 공격이 엔드포인트, 이메일 등 다양한 구간에서 시작되고, 신/변종 악성코드가 빈번하게 등장하기 때문이다. 따라서, **안랩 보안 아키텍처와 같이 여러 구간에 걸쳐 최적의 보안 기능을 수행하는 통합 보안 체계의 중요성이 높아질 것이다.**

Key Point

- 운영 및 성능 효율을 위해 서버 환경에서 리눅스 사용이 증가하고 있으나, 보안 관리는 미흡한 편
- 가상화 환경과 리눅스를 노린 공격이 증가할 전망 – 한 번의 공격으로 수 백개 가상 머신 침해 가능
- 여러 구간에 걸쳐 최적의 보안 기능을 수행하는 통합 보안 체계의 중요성이 높아질 것

AhnLab

© AhnLab, Inc. All rights reserved.

㈜ 안랩

경기도 성남시 분당구 판교역로 220 (우) 13493

대표전화: 031-722-8000 | 구매문의: 1588-3096 | 전용 상담전화: 1577-9431 | 팩스: 031-722-8901

홈페이지: www.ahnlab.com | 페이스북: www.facebook.com/AhnLabSP | 유튜브: www.youtube.com/OfficialAhnLab