2024. 12.

AhnLab

# 2024년 사이버 위협 동향 리뷰
# 2025년 전망

# 개요



## About

### About AhnLab

안랩은 첨단 기술을 바탕으로 최신 사이버 위협 인텔리전스와 위협 탐지 및 대응(TDR) 역량을 제공하는 국내 최고의 사이버 보안 기업입니다. 엔드포인트, 네트워크, 클라우드, 보안 운영, CPS(Cyber-Physical System) 등 다양한 사이버 보안 영역에 최적화된 솔루션과 플랫폼을 제공해 확장된 위협 가시성, 실용적인 위협 인텔리전스 및 최적의 위협 대응 역량을 보장합니다. 안랩의 미션은 고객의 비즈니스 혁신을 가속화하고 사이버 위협으로부터 안전하게 보호하는 것입니다. 이를 위해, 안랩의 위협 분석가와 개발 전문가들은 최고의 보안 노하우와 기술력을 제공해 한 차원 높은 수준의 보안 역량을 제공합니다.

### About ASEC

업계를 선도하는 사이버 위협 전문가들로 구성된 ASEC (AhnLab SEcurity Intelligence Center)은 빠르고 정확한 위협 분석 정보와 최적의 대응 방안을 제시하는 국내 최고의 위협 인텔리전스 조직입니다. ASEC은 악성코드, 취약점, 공격 그룹 등 위협에 관한 심층적인 분석을 기반으로 독보적인 인텔리전스를 적시에 제공하여 고객이 언제나 위협보다 한 발 앞설 수 있도록 합니다.

## Contents

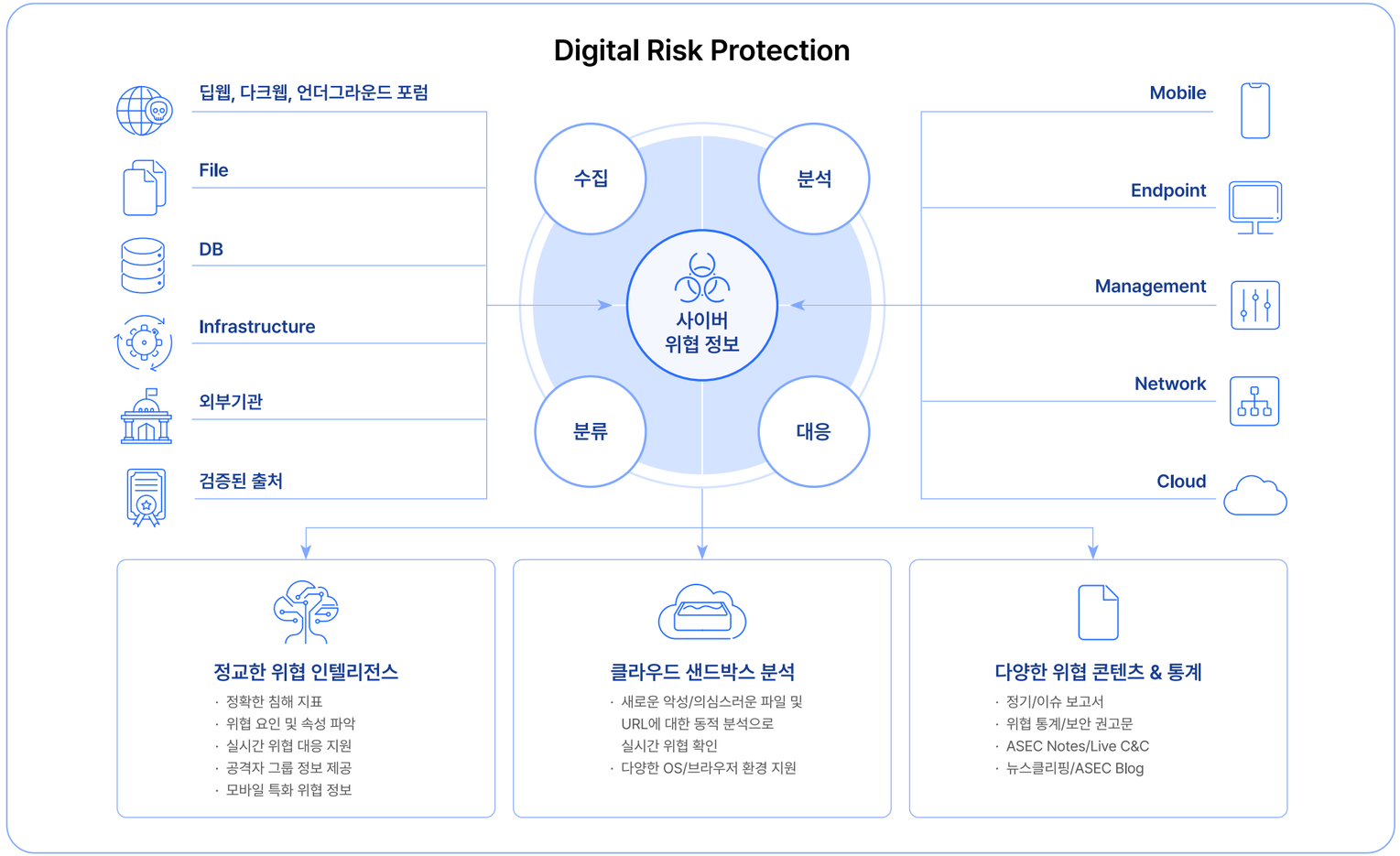
# 개요

## 서론

본 보고서는 안랩의 위협 인텔리전스 플랫폼 AhnLab TIP(AhnLab Threat Intelligence Platform)를 통해 제공되는 위협 정보를 바탕으로, 2023년 4분기부터 2024년 3분기까지 다양한 보안 이슈 및 트렌드를 살펴보고, 2025년 주요 사이버 보안 위협 동향을 전망한다.

AhnLab TIP는 여러 출처로부터 악성코드, 침해 사고, 위협 행위자, 취약점, 침해지표(IoC) 등에 관한 여러 위협 정보를 수집, 분석 및 분류하고 큐레이팅(curating)된 위협 인텔리전스를 제공해 고객이 사이버 보안 전략 수립과 의사결정에 활용할 수 있도록 한다.

AhnLab TIP에 관한 보다 자세한 사항은 AhnLab TIP 포털에서 확인할 수 있다.




[이미지] AhnLab TIP 개념도 및 기능 설명

# 개요

## 숫자로 보는 안랩의 위협 인텔리전스



최근 1년 간 AhnLab TIP를 통해 제공한 위협 정보 유형과 콘텐츠 수량은 다음과 같다.

### 1,157 위협 분석 게시글

Intelligence 게시판에서는 ASEC Notes, APT Group Report, CERT Report, Deep & Dark Web Report, Ransomware Report, Smishing Report, 악성코드 분석 보고서, 취약점 보고서, 포렌식 보고서, 금융 동향 보고서 등 다양한 형태의 위협 분석 정보를 제공하고 있다. 최근 1년간 게시된 콘텐츠 수는 1,157개에 달한다.

### 304 위협 그룹 분석

### 928 Malware Family 분석

안랩은 위협 그룹(Threat Actors)과 악성코드 패밀리(Malware Family)를 지속적으로 추적하고, 분석 정보를 AhnLab TIP를 통해 제공하고 있다. Threat Actors 게시판에서는 위협 그룹에 대한 상세 정보와 관련 TTPs, IoC, 보안 이슈, 최신 기사 등을 다각도로 파악할 수 있다. Malware Families 게시판에는 각 악성코드의 특징, 기법, 제작자 등 다양한 요소를 기반으로 분류 및 명명한 악성코드 군에 대한 정보를 제공한다.

### 802 보안 권고문

Security Advisories 게시판에서는 소프트웨어 취약점 정보와 대응 방안을 정리한 보안 권고문을 제공한다. 이를 통해, 사용자는 기업 혹은 기관에서 조치해야 할 제품 취약점 정보를 일목요연하게 파악해 대응할 수 있다. 최근 1년간 게시된 보안 권고문 수는 802개에 이른다.

### 11,495 뉴스 클리핑

AhnLab TIP의 News Clippings는 국내외 주요 언론사와 보안 기업이 발행한 보안 뉴스와 기술 문서를 제공한다. 각 뉴스에는 기업 보안 담당자가 이슈 별로 대응할 수 있도록 연관 IoC 정보를 함께 제공한다. 최근 1년간 제공된 뉴스는 총 11,495개다.

# 개요

## 숫자로 보는 안랩의 위협 인텔리전스

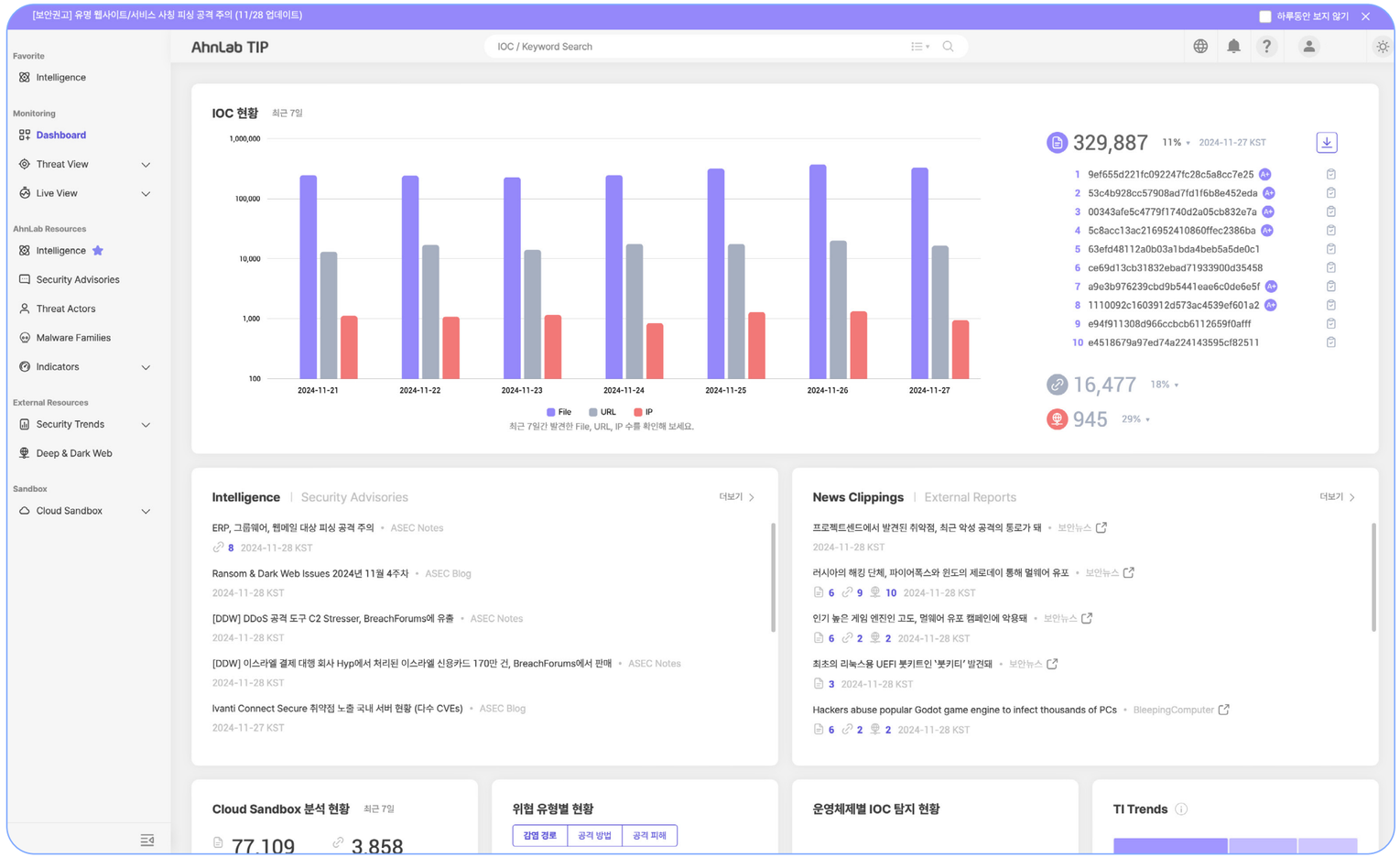


### 785 외부 보고서
### 62,375 주요 소셜미디어 콘텐츠

국내외 보안 기업과 전문가들이 발행한 보고서와 X(구 Twitter) 등에서 선별한 리포트 및 동향 정보를 제공한다. 해당 콘텐츠들 연관 IoC를 제공해 사용자가 빠르게 위협을 파악 및 대응할 수 있도록 한다.

### 10,000+ 일별 침해지표

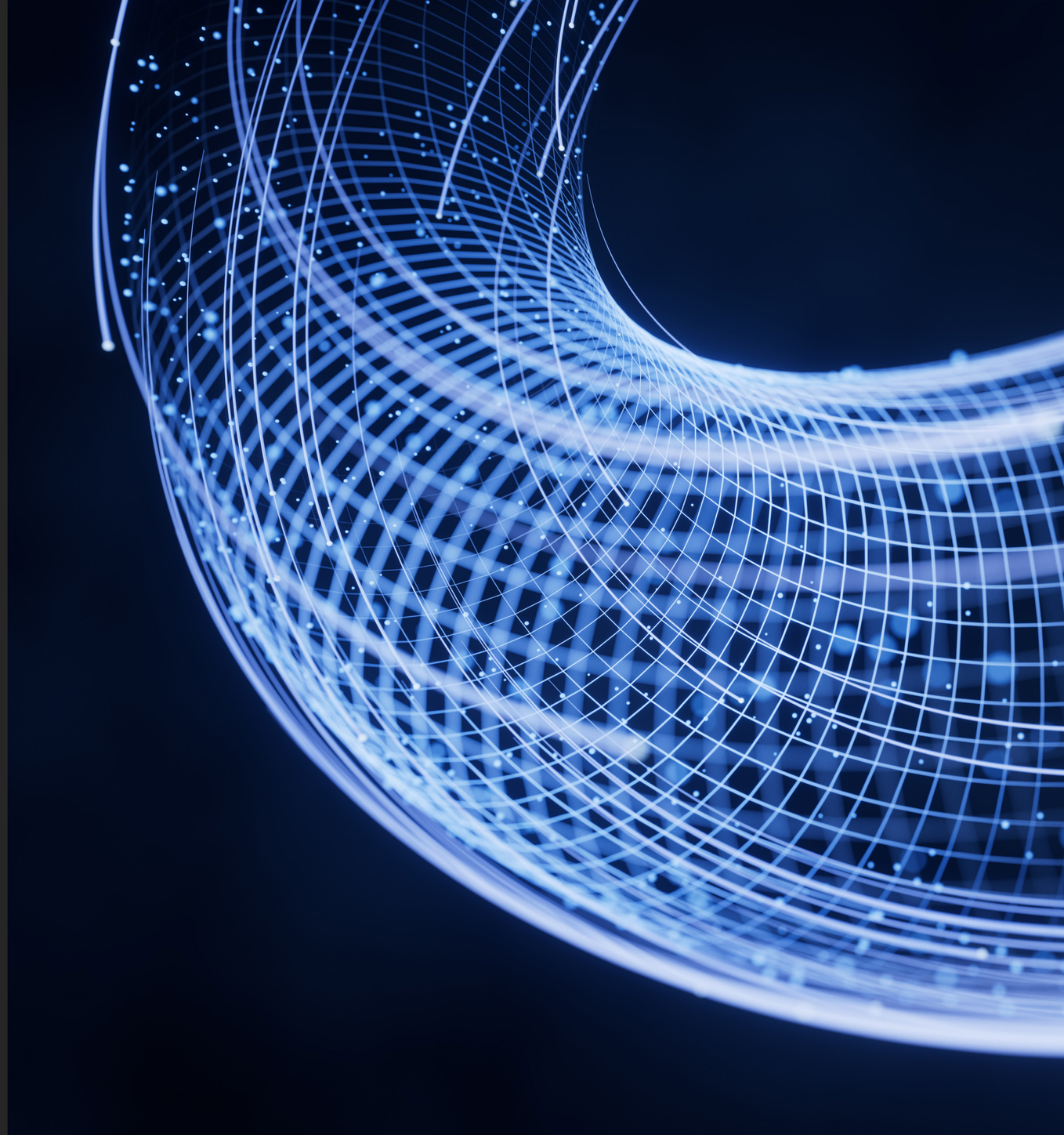
사용자가 신속한 위협 대응에 활용할 수 있도록 악성 파일, URL, IP, 도메인 등 매일 수천에서 수만 건에 달하는 IoC를 제공한다. 안랩은 국내 최대 악성코드 센서를 보유하고 있으며, 전체 IoC 중 OSINT(Open Source Intelligence)에서는 제공되지 않는 안랩만의 IoC 정보 비율이 약 30%에 이른다.




[이미지] AhnLab TIP 대시보드

# 2024년 주요 사이버 보안 이슈

- 주요 사건 사고
- 다크웹에서 파악된 공격자 트렌드
- APT 그룹 활동 요약
- 랜섬웨어 트렌드
- 실제 침해 사례에서 확인한 공격자들의 주요 전략
- 악성코드 관련 주요 이슈
- 모바일 위협 트렌드
- 공격 유형 통계



AhnLab

2024년 사이버 위협 동향 리뷰 & 2025년 전망

# 2024년 주요 사이버 보안 이슈



## 주요 사건 사고



최근 1년 간 발생한 사이버 보안 관련 주요 사건은 다음과 같다.

# 2024년 주요 사이버 보안 이슈



## 주요 사건 사고



### 1. 국제 사법기관 랜섬웨어 그룹 체포 작전

2023년 10월, 국제 사법기관들은 '크로노스 작전(Operation Cronos)'이라는 대규모 국제 협력 수사를 통해 영향력 있는 랜섬웨어 그룹 락빗(LockBit) 운영자들을 체포하는데 성공했다.

미국 연방수사국(FBI), 유럽 연합 법집행협력청(Europol), 국제형사경찰기구(Interpol), 그리고 여러 유럽 국가의 법 집행 기관들이 협력해 락빗의 핵심 인물들을 검거하고 조직의 서버와 인프라를 무력화했다. 이 작전의 성공은 국제적인 사이버 범죄 대응 협력의 중요성을 입증했고, 랜섬웨어 위협에 대한 법 집행 기관들의 적극적인 대응 의지를 보여 주었다.

### 2. XZ Utils 라이브러리 백도어 악성코드 발견

2024년 3월 29일, GNU/Linux에서 널리 사용되는 데이터 압축 라이브러리 'XZ Utils'에 백도어가 삽입된 사실이 밝혀졌다. 이 백도어는 XZ Utils 5.6.0 및 5.6.1 버전에서 발견되었으며, 지아 탄(Jia Tan)이라는 사용자가 프로젝트 관리자에게 신뢰를 얻은 후 깃허브(GitHub)의 투카니 프로젝트(Tukaani Project)에 악의적으로 추가한 것으로 밝혀졌다.

이 사건은 오픈소스를 이용한 공급망 공격의 위험성을 다시 한번 상기시켰다. 다행히 백도어가 초기에 발견되어 대규모 보안 사고로 이어지지는 않았지만, 개발자 간 신뢰 관계를 악용한 전형적인 공격 시도 사례로 주목 받았다.

### 3. 대한민국 대법원 해킹 사건

2024년 5월, 북한의 지원을 받는 것으로 추정되는 위협 그룹 라자루스(Lazarus)가 대한민국 대법원 컴퓨터 네트워크에 침투해 약 1TB의 데이터와 문서를 탈취했다. 이 사건은 대법원 시스템에 설치된 악성코드를 통해 약 2년에 걸쳐 진행됐다. 탈취된 데이터로는 개인정보, 주민등록번호, 재정 정보 등 민감 정보가 다수 포함되어 있어 국가 기밀과 국민의 개인정보 보호 측면에서 심각한 위협을 초래했다.

이번 사건으로 인해 국내 법무기관 정보 보안 시스템의 취약성을 드러났으며, 정부 기관 전반에 걸친 사이버 보안 강화 필요성을 재확인시켰다. 대법원은 해당 사건 이후 보안 시스템을 전면 재검토하고, 외부 전문가들과 협력하여 보안 체계를 강화하는 조치를 취했다.

### 4. 암호화폐 거래소 해킹 증가

2024년 암호화폐 가격 상승과 함께 거래소를 노린 공격이 증가하였다. 이러한 대규모 해킹 사건들은 암호화폐 거래소의 보안 취약성을 여실히 드러냈으며, 투자자들의 불안을 고조시켰다.

폴로닉스 거래소 해킹 사건:
폴로닉스(Poloniex) 거래소는 해킹으로 약 1억 3,000만 달러(한화 약 1,500억)의 손실을 입었다.

DMM 비트코인 해킹 사건:
일본 암호화폐 거래소인 DMM 비트코인은 해킹 공격으로 약 3억 달러(한화 약 4,154억 원)에 해당하는 4,500 BTC를 도난 당했다.

와지르엑스 해킹 사건:
인도 암호화폐 거래소 와지르엑스(WazirX)는 해킹으로 약 2억 3,500만 달러의 손실을 입었다.

# 2024년 주요 사이버 보안 이슈



## 주요 사건 사고



### 5. 크라우드스트라이크 BSOD 사건

2024년 7월 19일, 사이버 보안 기업 크라우드스트라이크(CrowdStrike)의 Falcon Sensor 업데이트 중 오류가 발생해 전 세계 윈도우(Windows) 시스템에서 블루스크린(BSOD) 현상이 일어났다. 약 8.5백만 대의 디바이스가 이 오류로 인해 부팅이 중단됐다.

은행, 항공사, 그리고 통신 회사들이 IT 시스템 중단으로 큰 타격을 받았으며, 일부 정부 기관은 긴급 회의를 소집해 해당 문제에 대응했다. 이번 사건은 소프트웨어의 업데이트 관리의 어려움과 단일 벤더 의존성이 미치는 위험성을 전세계 기업 및 기관들이 체감하는 계기가 됐다.

### 6. 레바논 무선 호출기 폭발 사건

2024년 9월 17일, 레바논과 시리아 전역에서 헤즈볼라 구성원들이 사용하던 무선 호출기 수천 대가 동시에 폭발했다. 호출기에 사전 설치된 소형 폭발 장치가 원격으로 작동해 폭발한 것이다. 이번 사건은 하드웨어와 소프트웨어의 경계를 넘나들며 현대판 '디지털 트로이 목마'로 불리고 있다.

본 사례는 직접적인 사이버 공격보다는 간접적인 공격으로 보는 것이 적절하나, 사이버 공간을 넘어 현실에 직접적으로 피해를 주는 사이버 전의 우려를 증가시키는 사례로 볼 수 있다.

### 7. 북한 해커 원격 근무자 위장 취업 사건

올해는 북한 해커들의 해외 기업 위장 취업 사례가 급증했다. 미국 법무부는 북한이 이러한 방식으로 미국 기업에 침투해 680만 달러 이상의 불법 수익을 창출했으며, 이 자금이 북한의 무기 개발에 사용되고 있다고 경고했다.

이들은 주로 중국과 러시아를 거점으로 활동하며, 가짜 신원과 이력서를 이용해 여러 기업에 동시에 지원했다. 취업 후에는 암호화폐 송금과 자금 세탁을 통해 자신들의 정체를 숨겼다. 본 사례는 북한 해커들이 기업들의 전 세계적인 채용 절차를 악용하고, 내부 시스템 침투 등 심각한 보안 위협을 초래할 수 있음을 시사했다.

### 8. 딥페이크 사기 사건

AI 기술이 빠르게 발전하면서 딥페이크 사기 사건이 늘어나고 있다. 해당 사건들은 딥페이크 기술의 위험성을 여실히 보여주었으며, 기업과 개인에게 화상 통화나 영상 메시지의 진위 여부를 더욱 신중히 확인해야 할 필요성을 각인시켰다. 이에 대응해 각국 정부와 기술 기업들은 딥페이크 탐지 기술 개발 관련 법률 및 제도 정비에 박차를 가하고 있다. 다음은 올해 발생했던 딥페이크 사기 사건들이다.

**금융회사 임원 사칭 사건:**

2023년 홍콩의 한 금융회사 직원이 딥페이크 기술로 재현된 가짜 CFO와 화상 회의를 통해 2억 홍콩달러(약 340억 원)를 사기 당한 사건이 일어났다. 공격자는 모든 회의 참석자의 얼굴과 목소리를 딥페이크로 조작해 피해자를 속였고, 이를 통해 거액의 돈을 송금 받을 수 있었다.

**납치 사기 사건:**

지난 10월 한국을 방문한 외국인의 딸을 납치 후 협박하는 내용의 영상이 부모에게 전송된 사건이 발생했다. 경찰 조사 결과, 해당 영상은 AI로 만들어진 가짜 영상이었으며, 납치 역시 실제로는 발생하지 않았다.

# 2024년 주요 사이버 보안 이슈



## 다크웹에서 파악된 공격자 트렌드

안랩은 다크웹에서 사이버 위협 관련 이슈를 모니터링 및 분석해 AhnLab TIP에서 콘텐츠로 제공하여 사용자가 다크웹 동향 및 당사 정보 유출 여부를 파악할 수 있도록 한다. 다음은 최근 1년간 다크웹 분석을 통해 도출한 주요 보안 인사이트를 정리한 것이다.

### 1. 국제 행사 연계 사이버 위협 증가

2024년 8월과 9월 사이 사이버 보안 사고가 급증했다. 이는 프랑스 파리 올림픽의 영향과 이에 대응하기 위한 집중적인 모니터링이 맞물린 결과로 분석되었다. 올림픽과 같은 대규모 국제 행사는 항상 사이버 공격의 주요 타깃이 되어왔다.

이번 파리 올림픽에서는 티켓 예매 시스템과 관련 인프라, 그리고 프랑스의 민간 및 정부기관에 대한 디도스(DDoS) 공격이 굉장히 많았다. 디도스 공격이 올림픽 운영에 막대한 영향을 주지는 않았지만 러시아-우크라이나 전쟁과 이스라엘-팔레스타인 분쟁에 따른 일부 핵티비스트(hacktivist)들의 선전 효과가 있었다.

파리 올림픽에 대한 사이버 공격 증가는 대규모 행사 시 사이버 보안의 중요성을 다시 한번 상기시켰다. 또한, 기업들의 연례 보안 점검과 모니터링 강화 기간과 맞물려 더 많은 보안 사고가 탐지된 것으로 보이는데, 이는 역설적으로 일상적인 보안 모니터링 체계 구축과 지속적인 보안 강화가 필요함을 시사한다.

### 2. 금융 산업을 향하는 사이버 범죄

다크웹 분석 결과, 금융 서비스 산업에 대한 공격 빈도가 높은 것으로 나타났다. 이는 해당 산업이 공격자들에게 여전히 매력적인 타깃 중 하나임을 보여준다. 실제로, 금융 기관들이 보유한 민감한 개인정보와 금융 데이터는 높은 가치를 지니고 있어 지속적인 공격 대상이 되고 있다.

제조업과 정부/공공기관이 그 뒤를 이었다. 디지털 전환 가속화로 인한 IT/OT 환경 확장과 이에 따른 공격 표면 증가가 주요 원인으로 분석된다. 특히 제조업의 경우, 스마트 팩토리와 IoT 기기 도입으로 새로운 취약점이 생겨나고 있다. 정부/공공기관은 중요 인프라와 민감한 정보를 보유하고 있어 지속적인 표적이 되고 있다. 결국, 주요 산업들이 사이버 보안을 핵심 과제로 다루어야 함을 시사한다.

# 2024년 주요 사이버 보안 이슈

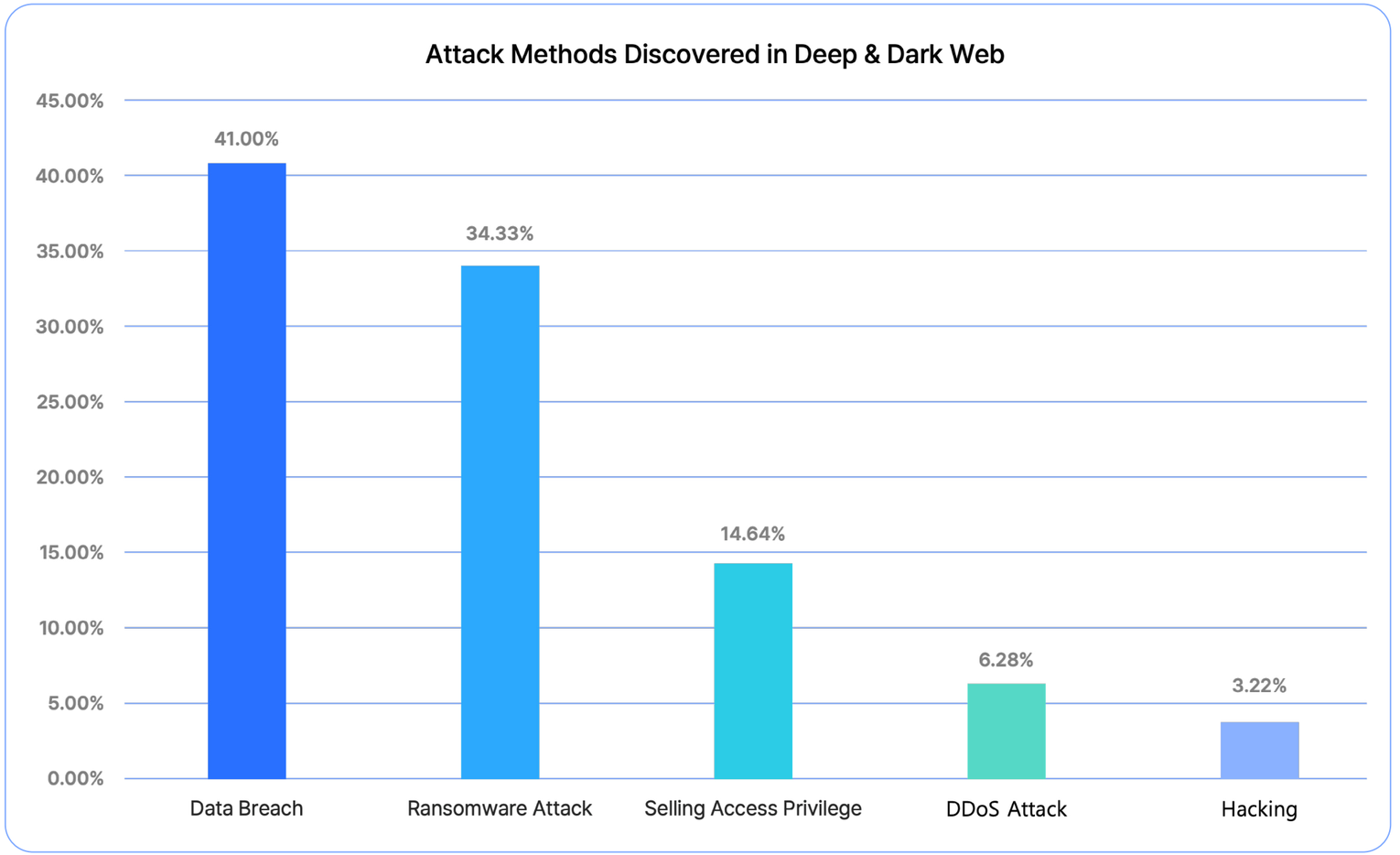
## 다크웹에서 파악된 공격자 트렌드



### 3. 대규모 데이터 유출 사고 증가

안랩이 다크웹 분석을 통해 보안 사고 유형을 도출한 결과,데이터 유출(Data Breach)이 41%로 가장 많았다. 대표적으로, 미국 통신사 AT&T는 고객의 통화 및 문자 기록이 유출되어 개인 프라이버시가 심각하게 침해됐다. 이 밖에, Advance Auto Parts, France Travail 등 글로벌 유수 기업들이 데이터 유출 사고를 겪었다. 지난 5월에는 클라우드 서비스 기업 드롭박스의 전자서명 서비스인 드롭박스 사인(Dropbox Sign)의 보안 취약점이 노출되고 고객들의 정보가 유출되는 사건이 있었다.

이와 같은 대규모 데이터 유출 사건들은 현재 기업들의 데이터 관리 체계에 미흡함이 있음을 암시한다. 이제 기업들이 데이터 암호화, 접근 제어, 이상행위 탐지 등 다층적 데이터 보호 전략을 수립하고 제로 트러스트 기반 보안 체계를 구축해야 한다.




[이미지] 딥웹 & 다크웹에서 확인된 공격 유형 분석 그래프

# 2024년 주요 사이버 보안 이슈

## 다크웹에서 파악된 공격자 트렌드



### 4. 접근 권한 거래 위협 증가

안랩 분석 결과에 따르면, 다크웹 관련 보안 사고 유형 중접근 권한 판매(Selling Access Privilege)가 약 15%를 차지하며 새로운 위협으로 부상하고 있다. 이는 사이버 범죄 방식이 진화하고 있음을 보여주는 중요한 지표다. 특히, 주요 기업과 정부 기관의 VPN 접근 권한 거래가 증가하고 있는데, 이는 보안 관점에서 굉장히 우려스러운 부분이다.

주요 예시로는 국제적인 해커 인텔 브로커(Intel Broker)가 시스코(Cisco)의 중요 데이터와 접근 권한을 판매하려 한 사례가 있다. GitHub/GitLab 프로젝트, 소스코드, 하드코딩된 자격 증명 등 비즈니스 민감 정보들이 유출된 것으로 알려졌고, 특히 하드코딩된 자격 증명 유출은 공격자들이 시스템에 지속적으로 접근할 수 있는 수단을 제공했다.

이처럼 기업 및 기관들이 침해 당할 경우, 고객사들도 영향을 받기 때문에 공급망 이슈와도 연관된다. 따라서, 조직들은 최소 권한 원칙(Principle of Least Privilege)을 기반으로 실시간 권한 사용 모니터링과 강력한 접근 권한 관리 체계를 갖춰야 한다.

### 5. 아시아 지역 표적화 증가

지난 1년 간 사이버 공격들을 살펴보면, 아시아 국가들 중에서 특히 한국, 일본, 인도네시아가 주요 타깃이 되었다. 이는 경제적 성장과 디지털 인프라 발전에 따른 결과로 볼 수 있다. 해당 국가 기업들이 글로벌 시장에서 차지하는 비중이 커지면서 사이버 공격자들의 관심도 함께 증가했다.

특히, 한국과 일본은 첨단 기술 산업이 발달해 있어 기술 유출을 노린 공격이 많았다. 인도네시아는 디지털 경제가 빠르게 성장하면서 새로운 타깃으로 부상했다. 아시아 지역 전체를 아우르는 범 국가 간 위협 인텔리전스 공유 체계 강화 및 글로벌 수준에 부합하는 사이버 보안 체계 구축이 시급함을 시사한다.

### 6. 사이버 공간에서 확산되는 지정학적 갈등

친러시아 및 친팔레스타인 핵티비스트 그룹의 활동이 활발해지면서 사이버 공간에서도 지정학적 갈등이 심화되고 있다. 핵티비스트 그룹들은 주로 디도스 공격, 웹사이트 변조, 정보 유출 등을 통해 정치적 메시지를 전달하려는 목적으로 움직였다. 특히, 러시아-우크라이나 전쟁과 이스라엘-팔레스타인 분쟁의 영향으로 핵티비스트 활동이 더욱 활발해졌다.

핵티비스트 활동은 국가 지원 APT 그룹의 은폐 수단으로 활용될 수 있어, 사이버 위협 환경을 한 층 더 복잡하게 만든다. 기업과 정부 기관들은 이러한 지정학적 이슈에 따른 사이버 위협에 더욱 주의를 기울여야 한다. 더 나아가, 지정학적 리스크에 기반한 위협 인텔리전스를 수집하고, 이를 보안 운영에 통합해야 한다.

# 2024년 주요 사이버 보안 이슈

## 다크웹에서 파악된 공격자 트렌드



### 7. 의료·헬스케어 분야 표적화

의료/헬스케어 분야에서 디지털화가 빠르게 진행되면서 해당 산업을 표적으로 한 공격도 증가하고 있다. 특히, 높은 가치를 지닌 환자들의 데이터를 노린 공격이 활발하게 감행되고 있다. 해당 공격은 북미와 유럽에서 집중적으로 나타나고 있으며, 랜섬웨어와 데이터 유출이 주를 이뤘다.

의료 기관들이 보유한 민감한 개인정보와 의료 기록은 범죄자들에게 매력적인 공격 대상이다. 하지만, 보안 태세는 상대적으로 미흡한 경우가 많아 사이버 보안 체계 강화가 시급하다. 특히, 의료기기의 IoT화, 원격 의료 확대 등으로 인해 공격 표면이 넓어지고 있는 만큼, 종합적인 보안 전략 수립이 필요한 시점이다.

### 8. 공급망 보안의 중요성 부각

상호 연결된 현대 비즈니스 환경에서는 단일 기업을 직접적으로 타격하는 것뿐만 아니라, 연관된 기업 및 사용자들까지 영향을 주는 공급망 공격이 주요 화두로 떠오르고 있다. 랜섬웨어 침해 사고를 살펴보면, 대형 기업 및 기관들과 긴밀한 협력 관계를 구축하고 있는 파트너사들을 공략하는 경우가 많아지고 있다. 파트너사들은 상대적으로 보안이 다소 취약하며, 침해 시 공급망 전반에 걸쳐 심각한 영향을 미친다. 또한, 소프트웨어 공급망 공격이 증가하고 있으며, 솔라윈즈(SolarWinds) 해킹 사건 이후 더욱 주목 받고 있다.

공급망 공격은 한 번의 침투로 여러 기업에 영향을 미칠 수 있어 위험도가 높다. 기업들은 당사 보안 뿐만 아니라 협력사의 보안 상태도 면밀히 점검하고 관리해야 한다. 또한, 써드 파티 위험 관리(Third-party Risk Management)의 중요성을 인지하고 기업의 전반적인 위험 관리 전략의 핵심 요소로 받아들여야 한다. 즉, 단일 기업의 보안을 넘어 전체 생태계 차원의 보안을 갖춰 나가야 한다.

# 2024년 주요 사이버 보안 이슈

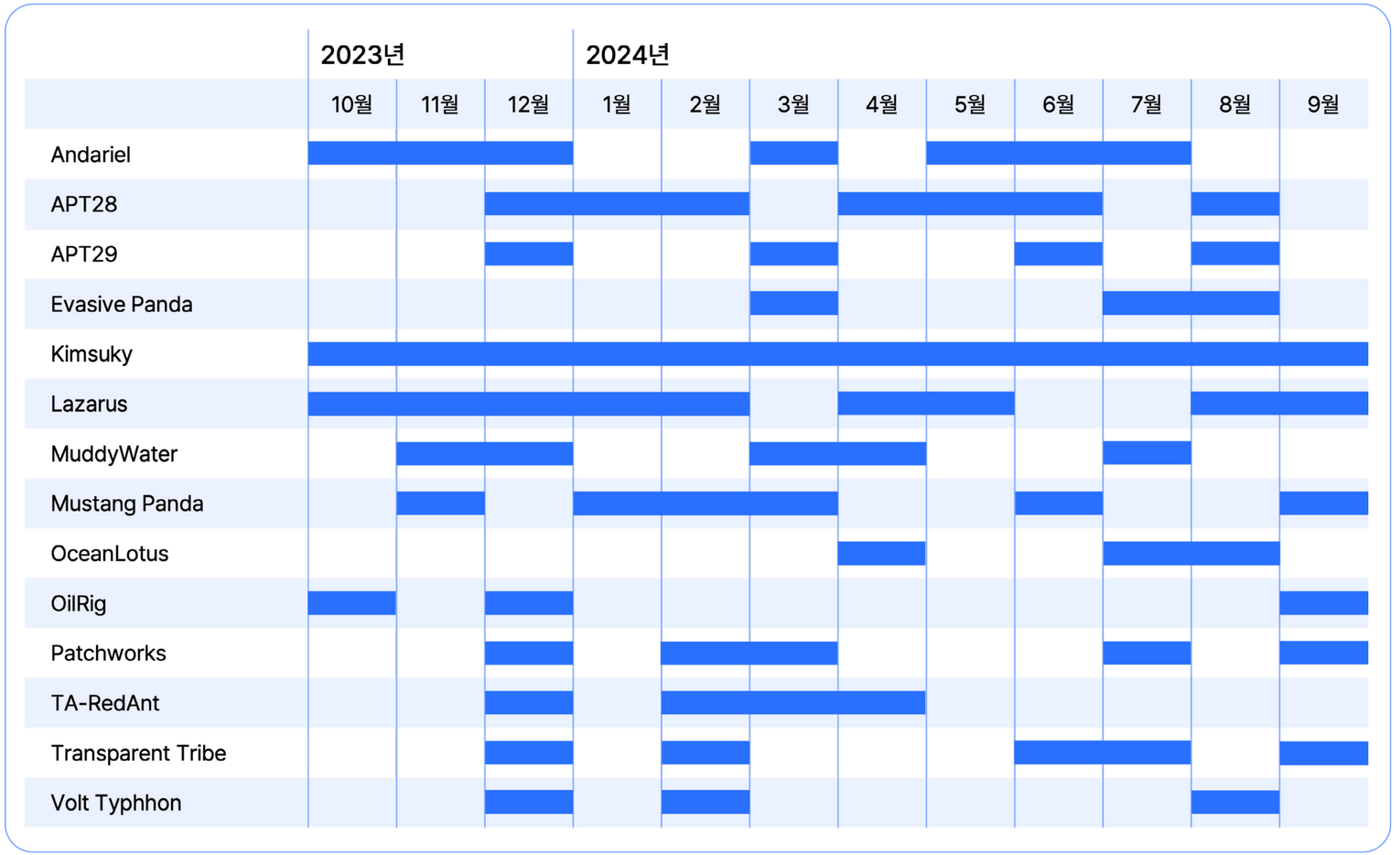


## APT 그룹 활동 요약

2023년 10월부터 2024년 9월까지 보안 업체와 관계 기관에서 공개한 APT 그룹 정보 중 3회 이상 언급된 그룹은 Andariel, APT28, APT29, Kimsuky, Lazarus, MuddyWater, Mustang Panda, Patchwork, TA-RedAnt, Transparent Tribe, Volt Typhoon이다.

이 중 가장 많이 언급된 그룹은 김수키(Kimsuky)로 매월 정보가 공개되었다. 다음으로 라자루스(Lazarus) 그룹이 9회, 안다리엘(Andariel) 그룹 7회 언급되었다. 주로 북한 APT 그룹의 활동이 활발했다. 다음으로, Transparent Tribe와 APT28가 6회, Mustang Panda와 MuddyWater가 5회 정보가 공개되었다. 파키스탄, 중국, 이란 APT 그룹의 활동도 많았음을 알 수 있다.

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




[이미지] 주요 APT 그룹 활동 빈도

# 2024년 주요 사이버 보안 이슈



## APT 그룹 활동 요약

### Andariel

안다리엘(Andariel) 그룹은 한국 방위 산업, 사이버 보안 기업, 연구소, 반도체 기업 등을 대상으로 공격을 수행해 오고 있다. 특히, 랜섬웨어 공격을 통해 금전적 수익을 벌어들이는 것으로 나타났다. 또한, Log4j 취약점(CVE-2021-44228)을 악용해 남미와 유럽 제조업체들을 공격하기도 했다. 이 밖에도, 미국 IT 기업, 유럽 에너지 기업, 아시아 제약 회사 등을 공격하며 전 세계적으로 활동하고 있다. 주요 공격 사례를 보면, 우선 한국에서 국산 중앙 집중형 관리 솔루션의 제로데이 취약점이나 ERP 솔루션의 업데이트 서버 취약점을 악용해 시스템을 감염시킨 바 있다. 미국에서는 주로 의료 기관을 대상으로 랜섬웨어 공격을 수행해 첩보 활동을 위한 자금을 마련했다. 미국에서의 공격은 Apache ActiveMQ(CVE-2023-46604), TeamCity(CVE-2023-42793), Citrix NetScaler(CVE-2023-3519) 등의 취약점을 활용했다. 미국 정부는 안다리엘 그룹과 연관된 인물을 기소하기도 했다.

### APT28

APT28 그룹은 유럽과 북미 교육, 정부, 제조, 항공 우주 산업을 대상으로 Microsoft Outlook 권한 상승 취약점(CVE-2023-23397)과 WinRAR의 원격 코드 실행 취약점(CVE-2023-38831)을 이용한 피싱 공격을 수행했다. TNEF 파일을 사용해 CSV, Excel, Word 파일로 위장한 첨부파일로 공격을 시도했다. 또한, 이스라엘-하마스 갈등을 이용한 사이버 스파이 활동을 벌이며, 다양한 악성코드를 배포했다. 주요 악성코드는 Headlace, MASEPIE, GooseEgg 등이 있고, 자격 증명 탈취와 네트워크 탐색을 위한 도구들을 활용했다. 미국 정부는 2024년 1월 법원이 승인한 다잉 엠버 작전(Operation Dying Ember)으로 러시아 GRU에서 운영한다고 의심받는 APT28 그룹의 봇넷을 차단했다. 외교관을 대상으로 자동차 판매 광고를 위장한 피싱 공격을 수행해 HeadLace 악성코드를 유포하는 공격도 발견됐다.

### Kimsuky

김수키(Kimsuky) 그룹은 주로 피싱과 사회공학 기법을 활용한 공격을 수행했다. 특히, 한국 정부 및 외교 기관 대상 침투 활동이 두드러졌다. 최근 활동을 보면, 한국 뿐만 아니라 일본, 미국 등으로 활동 반경을 넓히고 있다. 공격 기법 측면에서는 기업 소프트웨어 업데이트 프로그램을 악용하는 새로운 전술을 도입했다.

**Andariel**
APT45, Clasiopa, DarkSeoul, Jumpy Pisces, Onyx Sleet, PLUTO...

안다리엘(Andariel) 그룹은 북한의 지원을 받고 있다고 추정되는 라자루스(Lazarus) 그룹의 하위 그룹 혹은 협력 그룹으로 2008년 부터 활동이 확인되었다. 이 위협 그룹은 2012년 오퍼레이션 원미션(Operation 1 ...

- 주요 공격 분야: 방위산업, 교육, 국방, 의료, 건설, 국가기관, 에너지...
- 최초 보고일: 2008-08-05 KST
- 최근 보고일: 2024-11-11 KST

Files 814건 IPs 28건 URLs 74건

**APT28**
APT-C-20, Blue Delta, Fancy Bear, Fighting Ursa, Forest Blizzar...

APT28는 Fancy Bear, Softcy 등으로도 알려졌으며 러시아의 GRU (General Staff Main Intelligence Directorage) 85th Main Special Service Center(GTsSS) 군부대 26165와 인간된 위협 그룹으로 추정된...

- 주요 공격 분야: 방위산업, 정부기관, 외교, 에너지
- 최초 보고일: 2004-01-01 KST
- 최근 보고일: 2024-08-02 KST

Files 10건 URLs 3건

**Kimsuky**
APT-C-55, APT-Q-2, Baby Coin, Black Banshe, Black Banshee,...

Kimsuky (김수키)는 북한의 지원을 받고 있다고 생각되는 위협그룹으로 2013년부터 활동하고 있다. 초기에는 한국의 북한 관련 연구기관 등에 대한 공격을 진행했으며 2014년 한국의 에너지 기관에 대한 공격을 진행...

- 주요 공격 분야: 방위산업, 개인, 언론, 외교, 국가기관, 학술
- 최초 보고일: 2013-09-01 KST
- 최근 보고일: 2024-11-11 KST

Files 1,015건 IPs 47건 Domains 441건 URLs 360건

# 2024년 주요 사이버 보안 이슈

## APT 그룹 활동 요약



### Lazarus

라자루스(Lazarus) 그룹은 여러 하위 그룹이 다양한 국가와산업에 걸쳐 공격을 수행하고 있다. 한국에서는 국산 소프트웨어의 제로데이 취약점을 이용했고, 내부 전파 과정에서 자산 관리 솔루션 취약점을 악용했다. 하위 그룹인 BlueNoroff 그룹은 암호화폐 거래소, 투자회사, 은행 등을 공격하고 있다. 이들은 LinkedIn, Upwork, Braintrust 등의 작업 플랫폼에서 가짜 신원을 만들어 이메일, 소셜미디어 (LinkedIn), 메신저(WhatsApp, Telegram) 등을 통해 목표 사용자에게 연락해 신뢰를 형성하고 구인 제안이나 협업 요청을 가장한 이메일을 보낸다. 이들이 사용하는 악성코드 중 일부는 사용자나 악성코드를 추적할 수 없도록 루트킷 기법을 사용했다.

### MuddyWater

머디워터(MuddyWater) 그룹은 이스라엘 공무원 위원회의 공식 메모를 미끼로 스피어 피싱 메일을 발송하고, MuddyC2Go, SimpleHelp, Venom Proxy, AnyDesk, 맞춤형 키로거 등 다양한 도구를 활용해 이집트, 수단, 탄자니아 통신 조직을 공격했다. 기존 사용하던 Atera 원격 모니터링 & 관리 도구 대신 BugSleep(MuddyRot)을 사용한 것이 특징이다. 또한, BugSleep 백도어를 배포해 여러 국가의 항공사, IT 회사, 통신, 제약, 자동차 제조업체 등을 공격하기도 했다. 사우디아라비아와 이스라엘 조직들을 타깃으로 피싱 이메일을 배포한 사례도 있는데, 사우디아라비아에서는 RMM 도구를, 이스라엘에서는 BugSleep 백도어를 최종 페이로드로 사용했다.

### Mustang Panda

무스탕 판다(Mustang Panda) 그룹은 필리핀 정부를 포함한 남태평양 여러 기관을 대상으로 크게 세 가지 캠페인을 진행했다. 먼저, Solid PDF Creator와 SmadavProtect와 같은 정상 소프트웨어를 사용해 악성 DLL 파일을 로드하고, 정상 마이크로소프트 트래픽으로 가장해 명령 및 제어(C2) 연결을 시도했다. 또한, LNK 파일을 사용해 베트남의 국가 세금 및 교육 섹터를 타깃으로 악성 HTA 파일을 실행하는 등 다양한 공격 기법을 사용했다. 주요 악성코드로는 PubLoad와 Doplugs가 있으며, USB 감염과 정보 수집에 특화된 KillSomeOne 모듈을 사용했다.

**Lazarus**
Diamond Sleet, Guardians of Peace, HIDDEN COBRA, Labyrinth...

Lazarus (라자루스) 그룹은 Guardians of Peace, Hidden Cobra, Nickel Academy, Whois Team, Zinc 등으로도 알려졌다. 북한의 지원을 받고 있다고 추정되며 2009년 부터 활동하고 있다. 초기에는 한국에서 ...

- 주요 공격 분야: 방위산업, 금융, 암호화폐, 첨단
- 최초 보고일: 2009-06-06 KST
- 최근 보고일: 2024-10-04 KST

Files 941건 IPs 78건 Domains 6건 URLs 81건

**MuddyWater**
ATK 51, MERCURY, Mango Sandstorm, MangoSandstorm, Sand...

MuddyWater 그룹은 2017년부터 활동하고 있는 위협그룹으로 미국 FBI와 영국 기관에 따르면 이란 정보기관 (MOIS)이 배후에 있다고 한다. 주로 중동 지역에서 활동하지만 조지아, 파키스탄, 튀르키예, 미국 등에서...

- 주요 공격 분야: 교육, 방위, 언론, 국가기관, 에너지, 통신, 첨단
- 최초 보고일: 2017-01-01 KST
- 최근 보고일: 2024-04-22 KST

**Mustang Panda**
Bronze President, Earth Preta, HoneyMyte, RedDelta, Stately Ta...

중국에 기반을 둔 그룹으로 추정되고 있으며 2017년 처음 발견되었지만 적어도 2014년 이후로 작전을 수행하고 있을 것으로 추정되는 그룹이다. 미국, 독일의 정부기관, 비영리 단체, 종교 및 기타 비정부 조직을 표적으...

- 주요 공격 분야: 비정부기구, 활동가
- 최초 보고일: 2018-01-01 KST
- 최근 보고일: 2024-07-19 KST

Files 79건 IPs 13건 Domains 1건 URLs 2건

# 2024년 주요 사이버 보안 이슈



## APT 그룹 활동 요약

### Transparent Tribe

트랜스페어런트 트라이브(Transparent Tribe) 그룹은 인도 조직들을 대상으로 매크로를 포함한 문서를 통해 CrimsonRAT 악성코드를 배포했다. 이들은 스피어 피싱, 악성 ISO, ZIP 아카이브, 악성 링크 등을 사용해 자격 증명을 탈취했다. 또한, Golang으로 컴파일된 새로운 스파잉 도구를 도입하고, Telegram, Discord, Google Drive와 같은 웹 서비스를 통해 다양한 악성 도구를 배포했다. 이 밖에, SideCopy 그룹과의 유사점도 발견되었으며 인프라 재사용 패턴도 확인됐다.

### APT29

APT29 그룹은 TeamCity 취약점(CVE-2023-42793)을 이용해 생명공학 및 의료 제조산업을 공격했다. 이들은 Python으로 작성된 맞춤형 익스플로잇 스크립트를 사용해 GraphicalProton 악성코드를 배포했다. 또한, WineLoader 악성코드를 활용해 독일 정치 조직을 공격했고, 2023년 11월부터 2024년 7월까지는 몽골 정부 웹사이트를 통해 워터링 홀 공격을 감행했다. 몽골에서의 공격은 iOS 취약점(CVE-2023-41993)과 안드로이드 취약점(CVE-2024-5274, CVE-2024-4671)을 이용했다.

### Patchwork

패치워크(Patchwork) 그룹은 파키스탄 연방 국세청을 미끼로 피싱 공격을 수행했다. 공격 기법을 보면, 먼저 PowerShell을 호출하는 LNK 파일을 사용해 악성 파일을 다운로드하고, 수집된 정보를 Base64로 인코딩한 후 RC4로 암호화해 통신했다. 또한, Nexe 백도어 변종을 사용해 보안 경고를 우회하고 Salsa20 암호화 알고리즘을 통해 데이터를 암호화했다. 또한, 이들은 VajraSpy 악성코드를 포함한 안드로이드 앱을 통해 로맨스 스캠 캠페인을 벌였고, 파키스탄과 인도 사용자를 대상으로 스파이 활동을 진행했다.

**Transparent Tribe**

APT-C-56, APT36, C-Major, COPPER FIELDSTONE, Green Havild...

Transparent Tribe 그룹은 파키스탄의 위협그룹으로 추정되며 2013년부터 아프가니스탄, 인도, 카자흐스탄, 사우디아라비아 등의 외교 및 군사 자원에 대한 공격을 진행하고 있다. 2022년 이후에는 인도 교육 분야에...

- 주요 공격 분야: 교육, 국방, 정부기관, 항공우주
- 최초 보고일: 2013-01-01 KST
- 최근 보고일: 2024-07-23 KST

Files 336건 IPs 32건 Domains 30건 URLs 28건

**APT29**

APT-C-25, ATK 7, BlueBravo, Cloaked Ursa, CloudLook, Cozy B...

APT29는 러시아의 SVR(Foreign Intelligence Service)에 기인한 위협 그룹이다. 최소 2008년부터 활동을 시작한 것으로 알려졌으며 유럽 및 NATO 소속되어 있는 국기기관, 연구기관, 정책연구소를 주요 공격대상으...

- 주요 공격 분야: 국가기관, 연구기관, 정책연구소
- 최초 보고일: 2008-01-01 KST
- 최근 보고일: 2024-08-29 KST

Files 4건 URLs 3건

**Patchwork**

APT-C-09, APT-Q-36, ATK11, Chinastrats, Dropping Elephant, ...

Patchwork 그룹은 2015년 12월에 처음발견된 위협그룹으로 APT-C-09, APT-Q-36, ATK11, Chinastrats, Dropping Elephant, Hangover, Orange Athos, Quilted Tiger, Sarit, White Elephant, ZINC EM...

- 주요 공격 분야: 교육, 정부기관, 외교, 국가기관, 방송, 비정부기구, ...
- 최초 보고일: 2015-12-01 KST
- 최근 보고일: 2024-07-17 KST

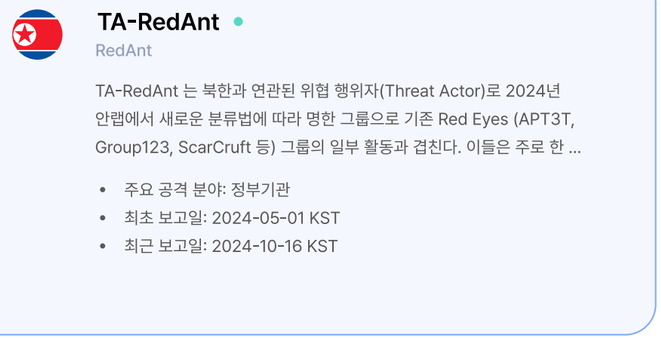
# 2024년 주요 사이버 보안 이슈

## APT 그룹 활동 요약



### TA-RedAnt

TA-RedAnt 그룹은 정부 및 군사 기관을 대상으로 워터링 홀 공격과 피싱 캠페인을 주로 감행했다. 특히 정찰 활동 강화를 목적으로 새로운 악성코드인 Dolphin을 사용해 파일 탈취, 키로깅, 스크린샷 캡처 등을 수행했다.



# 2024년 주요 사이버 보안 이슈

## 랜섬웨어 트렌드



### 개요 및 동향

2024년 한 해 간, 랜섬웨어 공격은 급격한 변화와 진화를 보였다. 랜섬웨어로 인한 위협이 지속적으로 고조되는 가운데, 주목할 만한 점은 법 집행기관의 대응으로 기존 랜섬웨어 생태계가 빠르게 재편되었다는 것이다.

### 랜섬웨어 대응 체계 강화

법 집행기관의 랜섬웨어 대응 강화는 사이버 범죄와의 전쟁에서 중요한 진전이었다. 락빗(LockBit) 소탕을 위한 크로노스 작전(Operation Cronos)과 라그나 로커(Ragnar Locker) 및 ALPHV(BlackCat)의 폐쇄는 주목할만한 국제적 협력의 성과다. 특히, 락빗(LockBit)의 입지가 줄어들면서 랜섬웨어 생태계에도 큰 변화가 생겼다.

다만, 폐쇄 후 다시 부활한 트리고나(Trigona) 랜섬웨어 갱단 사례는 법적 제재에 대한 위협 그룹들의 적응력과 회복력을 보여주며, 그 중심에는 동적인 특성을 가진 '서비스형 랜섬웨어(Ransomware-as-a-Service, RaaS) 모델이 있다. 따라서, 법 집행기관들 역시 보안과 단속에 있어 대응 전략을 지속적으로 고도화 시켜야 하는 과제를 안고 있다.

### 주요 공격 트렌드 및 전술

2024년, 랜섬웨어 공격 기법은 더욱 정교해지고 체계화되었다. 이중 및 삼중 갈취 전술이 랜섬웨어 공격의 표준으로 자리잡았고, 취약점 악용 기술은 제로데이 공격을 포함한 고도화된 형태로 발전했다. 특히, 서비스형 랜섬웨어(RaaS)모델이 보편화되면서 랜섬웨어 캠페인의 진입 장벽이 낮아졌고, 이는 공격 건수의 증가로 이어졌다. 주목할 만한 점은 AI 기반 자동화 도구 도입이 가속화되면서 공격의 효율성과 정확성이 크게 향상되었다는 것이다.

공격 대상 산업군에도 뚜렷한 변화가 감지되었다. 의료 분야에 대한 공격이 급증했는데, 중요 인프라의 특성상 큰 비용(ransom)을 지불할 가능성이 높기 때문으로 분석된다. 제조업과 IT 서비스 업체를 겨냥한 공격도 증가세를 보였는데, 특히 클라우드 인프라를 표적으로 한 공격이 새로운 위협 벡터로 부상했다. 디지털 전환 가속화에 따른 클라우드 의존도가 높아졌기 때문으로 보인다.

# 2024년 주요 사이버 보안 이슈

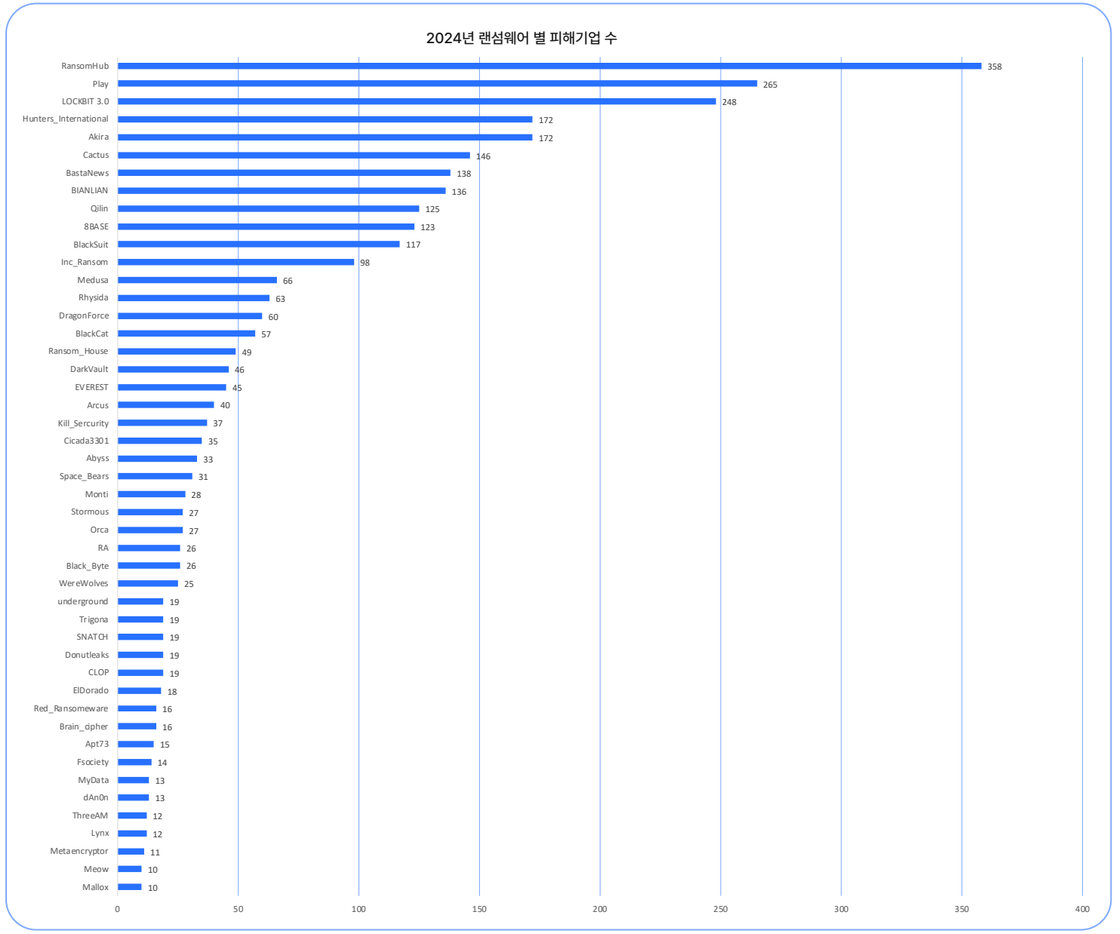
## 랜섬웨어 트렌드



### 대응 및 전망

2024년, 랜섬웨어는 그 어느 때보다 복잡하고 역동적인 변화를 보여주었다. 기존 강자의 몰락과 새로운 위협 행위자의 등장, 국가 지원 세력과의 결합 등 다양한 변화가 관찰되었다. 효과적인 랜섬웨어 대응을 위해서는 다층적(multi-layered) 방어 체계 구축이 필수적이다. 우선 엔드포인트 보안을 강화해 초기 침투를 차단하고, 네트워크 세그멘테이션을 통해 피해 확산을 방지해야 한다. 또한, 최신 위협 인텔리전스를 기반으로 지속적인 모니터링 체계를 구축해 위협을 조기에 탐지하고, 사고 발생 시 신속한 대응을 위한 포렌식 기반 침해 분석 역량을 확보해야 한다.

랜섬웨어는 앞으로도 고도화를 거듭할 것으로 예상된다. AI 기술이 적용된 새로운 형태의 랜섬웨어가 등장하고, 자가 전파 능력을 갖춘 크립토웜 기능이 탑재된 변종도 출현할 것으로 전망된다. 특히, 대규모 언어 모델(LLM)을 활용한 협상 전술이 더욱 정교화될 것으로 보이며, 암호화 없이 데이터 유출만을 노리는 전용 공격도 증가할 것이다. 이러한 변화는 기업들의 보안 전략에 새로운 도전과제를 제시할 것이다.




[이미지] 주요 APT 그룹 활동 빈도

# 2024년 주요 사이버 보안 이슈

## 랜섬웨어 트렌드



### 주요 랜섬웨어 그룹 활동 분석

안랩이 분석한 전체 침해 사고 중 랜섬웨어 공격이 34%를 차지했다는 사실은 랜섬웨어가 여전히 주요 위협으로 자리잡고 있음을 보여준다. 랜섬웨어 그룹들은 강력한 법적 제재에 맞서 진화를 거듭하고 있다.

공격 그룹 중에는 랜섬허브(RansomHub)를 주목할만하다. 랜섬허브는 2024년 2월 등장한 신생 그룹임에도 불구하고 빠르게 성장해 락빗(LockBit)을 제치고 가장 활발히 활동하는 랜섬웨어 그룹으로 부상했다. 이들은 숙련된 랜섬웨어 운영자들을 영입하고, 수익 분배율 상향 등 공격자 친화적 조건을 제시하며 급속히 세력을 확장했다.

또한, Cicada3301, Eldorado, Embargo 등 새로운 랜섬웨어 그룹들이 등장했다. 이를 통해, 랜섬웨어 생태계가 계속해서 진화하고 있음을 알 수 있다. 반대로 보면, 방어자 입장의 기업 및 기관들이 선제적이고 능동적인 랜섬웨어 대응 체계를 구축해야 함을 시사한다.

다음은 주요 랜섬웨어 그룹들의 활동 동향이다.

#### LockBit: 몰락과 부활 시도

락빗(LockBit)은 2024년 2월 국제 사법기관의 공조로 진행된 '크로노스 작전' 이후 심각한 타격을 입었다. 5월에는 전체 랜섬웨어 공격 건수의 37%에 달하는 176건의 공격을 감행했다고 주장했다. 다만, 이는 건재함을 알리기 위한 조치로 보이며, 온전히 신뢰하기는 힘든 수치로 평가된다. 계열 조직들이 이탈하면서 시장 지배력이 현저히 약해졌고, 이는 랜섬웨어 생태계가 재편되는 계기가 되었다.

#### RansomHub: 급부상하는 랜섬웨어 그룹

2024년 랜섬웨어 생태계에서 가장 주목할 만한 포인트가 바로 랜섬허브(RansomHub)의 급성장이다. 이들은 2024년 2월 등장 이후, 3분기까지 전체 공격의 14.2%를 감행하며 주요 공격 그룹으로 자리매김했다. 2024년에 210개가 넘는 조직에 피해를 입혔으며, 90%라는 파격적인 계열사 수익 배분 모델을 도입해 공격자들의 관심을 끌었다. 또한, 미국 Rite Aid, Planned Parenthood 등 대기업 공격에 성공하며 위험성을 입증했다.

**LockBit**

LockBit(락빗, 록빗)은 2019년 9월에 처음 등장한 세계에서 가장 악명 높고 활발한 Ransomware=as=a=Service(RaaS) 조직 중 하나이다. 초기에는 파일을 호화하고 확장자를 ".abcd"로 바꿨기 때문에 ABCD ...

- 주요 공격 분야: 다양한 산업 및 조직
- 최초 보고일: 2019-09-01 KST
- 최근 보고일: 2024-10-02 KST

Files 54건 URLs 5건

**RansomHub**

RansomHub라고 알려진 랜섬웨어 갱단은 2024년 2월부터 활동을 시작하였다. 이들은 자신들이 운영하는 DLS (Dedicated Leak Sites)에 비교적 자세히 자신들을 소개하고 있다. 이들은 전 세계 해커들로 구성된 팀...

- 주요 공격 분야: 소프트웨어 개발, 에너지, 첨단산업
- 최초 보고일: 2024-02-10 KST
- 최근 보고일: 2024-11-06 KST

Files 11건

# 2024년 주요 사이버 보안 이슈



## 랜섬웨어 트렌드



### Play: 국가 지원 세력과 결합

플레이(Play) 랜섬웨어는 북한 해킹 그룹 안다리엘(Andariel)과 협력해 랜섬웨어 그룹과 국가 지원 해킹 조직 간 새로운 위협 모델을 제시했다. 연간 전체 랜섬웨어 공격 사례의 7.5%(96건)를 차지했으며, ESXi 환경을 특정 표적으로 하는 전문화된 접근 방식을 선보였다.

### BlackCat: 극단적인 변화

블랙캣(BlackCat)은 2024년 가장 극단적인 변화를 보여준 그룹이다. 블랙캣은 미국 의료기업 '체인지 헬스케어(Change Healthcare)를 공격해 2,200만 달러의 랜섬을 수금하며 미국 의료 분야 역대 최악의 사이버 사고를 일으켰다. 이후, 랜섬을 지불 받고 시스템을 복구해주지 않는 엑시트 스캠(Exit Scam)을 벌인 후 활동을 중단했다.

### Akira: 클라우드 특화 전술

아키라(Akira)는 클라우드 서비스를 표적으로 한 전문적인 접근법으로 주목받았다. Tietoevry 공격 포함, 250개 이상의 조직을 공격하며 4,200만 달러의 랜섬을 요구했다. 윈도우(Windows)와 리눅스(Linux) 시스템을 모두 아우르는 기술적 역량을 과시했다.

**Play**
PlayCrypt

Play 랜섬웨어 갱단은 2022년 8월 아르헨티나 코르도바 사법부를 공격하면서 처음 세상에 알려졌다. 일부 보안업체와 연구원은 그보다 조금 빠른 2022년 6월과 7월에 컴퓨터 관련 커유니티에 Play 확장자로 자신의 파일...

- 주요 공격 분야: 클라우드, 정부기관, 법률, 첨단산업
- 최초 보고일: 2022-08-13 KST
- 최근 보고일: 2024-11-04 KST

Files 1,015건 IPs 47건 Domains 441건 URLs 360건

**ALPHV**
BlackCat, Noberus, 블랙캣

ALPHV 는 BlackCat 으로도 알려졌으며 2021년 11월 처음 활동을 시작하였다. BlackCat 으로 알려진 계기는 랜섬웨어 그룹이 운영하는 데이터 유출 사이트에 검은 고양이 이미지가 있어 BlackCat 으로 더 잘 알려져 ...

- 주요 공격 분야: 정보통신기술, 의료기관
- 최초 보고일: 2021-11-01 KST
- 최근 보고일: 2024-03-13 KST

Files 52건

**Akira**
Akira Gang, Storm-1567

Akira 는 2023년 3월부터 활동하고 있는 섬웨이 검으로 주로 미국과 캐나다의 기업과 기관을 공격하고 있다. Akira 랜섬웨어를 사용하며 이 조직의 DLS (Dedicated Leak Site)는 1980년 대 녹색 화면 콘솔을 인상...

- 최초 보고일: 2023-03-01 KST
- 최근 보고일: 2023-10-11 KST

Files 4건

# 2024년 주요 사이버 보안 이슈

## 랜섬웨어 트렌드



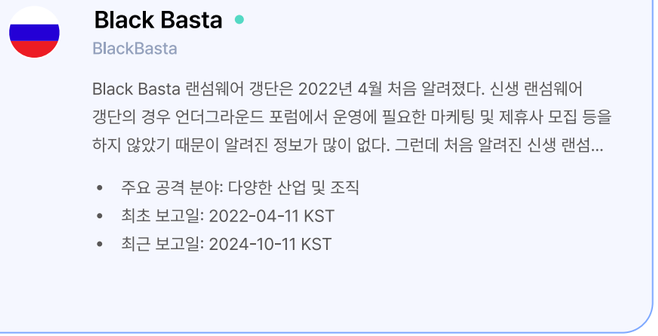
### BlackBasta: 의료 분야 특화

BlackBasta는 의료 분야를 중심으로 500개 이상의 조직을 공격했다. 2024년 초부터 4개월 간 102건의 공격을 수행하며, 지속적인 위협 행위자의 입지를 굳혔다. FBI와 CISA의 공동 대응이 필요할 정도로 심각한 위협으로 인식되었다.

### 새로운 위협 행위자들

이 밖에도, 2024년 랜섬웨어 생태계에는 새로운 위협 행위자들의 전문화된 공격 양상이 두드러졌다. 8BASE는 자동차 산업을 주요 표적으로 삼아 포드 딜러십 네트워크와 폭스바겐을 대상으로 한 고도화된 공격을 감행했다. Hunters International은 금융권 대상 공격에서 강세를 보였다. 특히, 중국공상은행을 대상으로 한 대규모 공격에서 6.6TB 이상의 데이터를 탈취하며 공격 역량을 과시했다.

한편, Cactus는 Qlik Sense 데이터 시각화 소프트웨어의 취약점을 전문적으로 공략하는 특화된 접근 방식을 보여줬다. 취약점 공개 후 24시간 이내에 조직적인 공격을 개시하는 신속성도 주목할만 했다. BIANLIAN은 악랄한 방식으로 피해 조직을 위협하기 위해 기존 암호화를 넘어, 순수 데이터 탈취를 주요 목표로 삼았다. 특히 인명과 직결된 의료 산업과 제조업의 민감한 데이터를 노린 공격으로 막대한 피해를 안겼다. 피해 기업 임원들을 협박하기 위해 그들의 개인정보와 사진을 무차별적으로 유출하는 등 심각한 프라이버시 침해도 수반됐다. 이러한 공격은 임원들 뿐만 아니라 가족들의 안전까지 위협하는 중대한 범죄 행위로 이어졌다.



# 2024년 주요 사이버 보안 이슈

## 랜섬웨어 트렌드

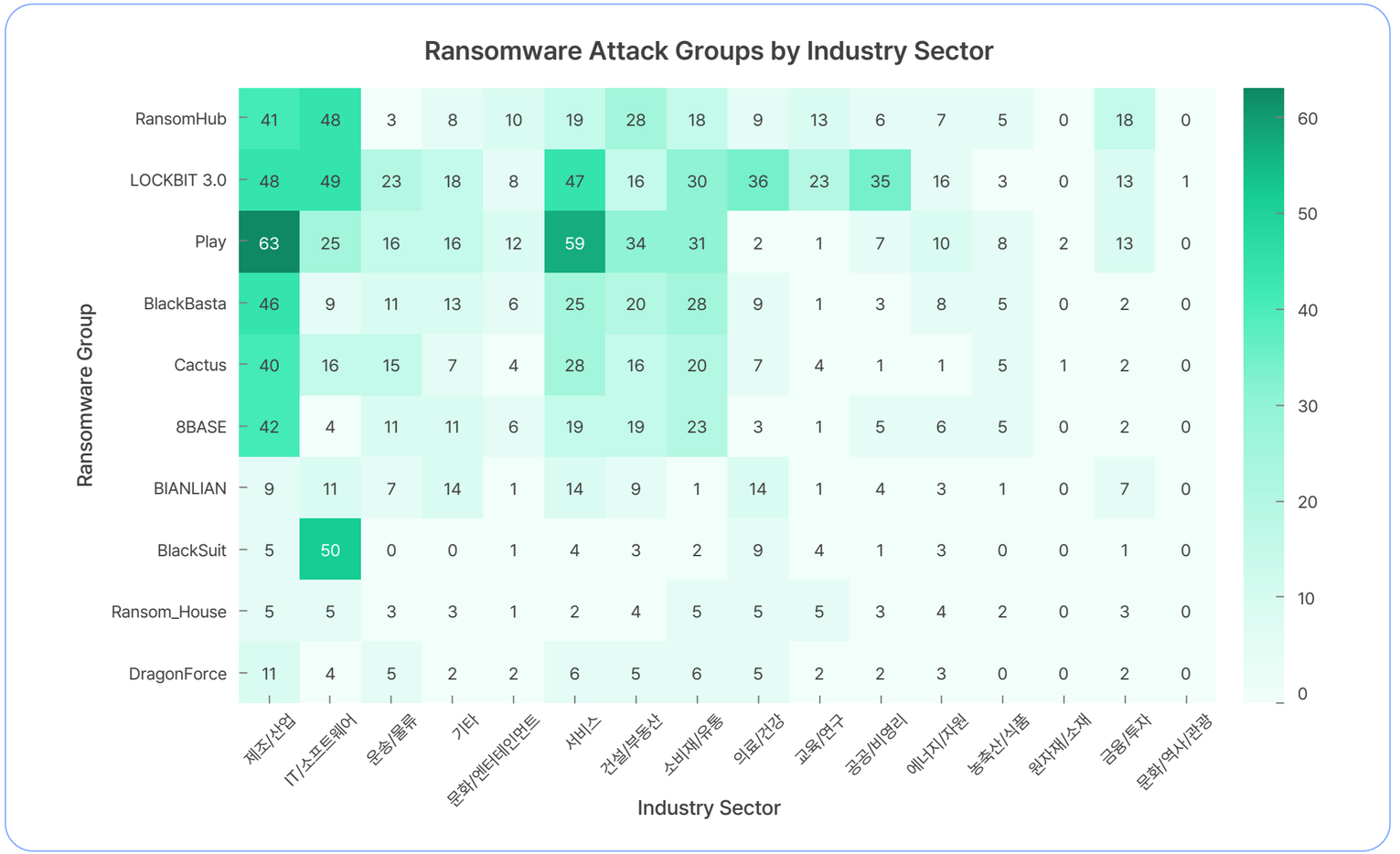


### 랜섬웨어 주요 피해 산업군

2024년 랜섬웨어 공격 그룹별 피해 산업군 데이터를 분석한 결과, 각 그룹들이 특정 산업군을 집중적인 표적으로 삼는 것을 확인할 수 있었다. 제조/산업, IT/소프트웨어/통신, 건설/부동산, 소비재/유통 산업군이 특히 많은 공격을 받았다. 이는 각 산업의 고유한 특성과 밀접한 관련이 있다.

제조/산업군은 생산 라인 중단으로 인한 막대한 경제적 손실 위험이 높고 지적 재산권 등 핵심 기술 데이터에 대한 보호가 필요하다. IT/소프트웨어/통신 산업은 서비스 중단의 파급력과 민감한 고객 데이터 보유로 인해 빈번하게 공격 대상이 되고 있다. 소비재/유통 산업 역시 대규모 고객 정보와 결제 데이터를 보유하고 있어 개인정보 유출에 따른 피해가 크다. 건설/부동산은 프로젝트 일정 지연에 따른 비용 증가와 계약 관련 중요 문서 접근 불가 시 피해가 크기 때문에 신속한 복구가 이뤄져야 하는 특성을 갖고 있다.

이들 산업군은 시스템 의존도가 높아 공격 성공 시 즉각적인 업무 중단으로 이어지며, 높은 복구 비용을 지불할 가능성이 크기 때문에 지속적인 공격 대상이 되고 있다. 반면, 농축산/식품, 문화/역사/관광 등의 산업군은 전통적인 생산 방식을 유지하고 있거나, 디지털 시스템 의존도가 낮기 때문에 상대적으로 공격 빈도 수가 적다.




[이미지] 산업군 별 주요 랜섬웨어 피해 빈도

# 2024년 주요 사이버 보안 이슈

## 랜섬웨어 트렌드



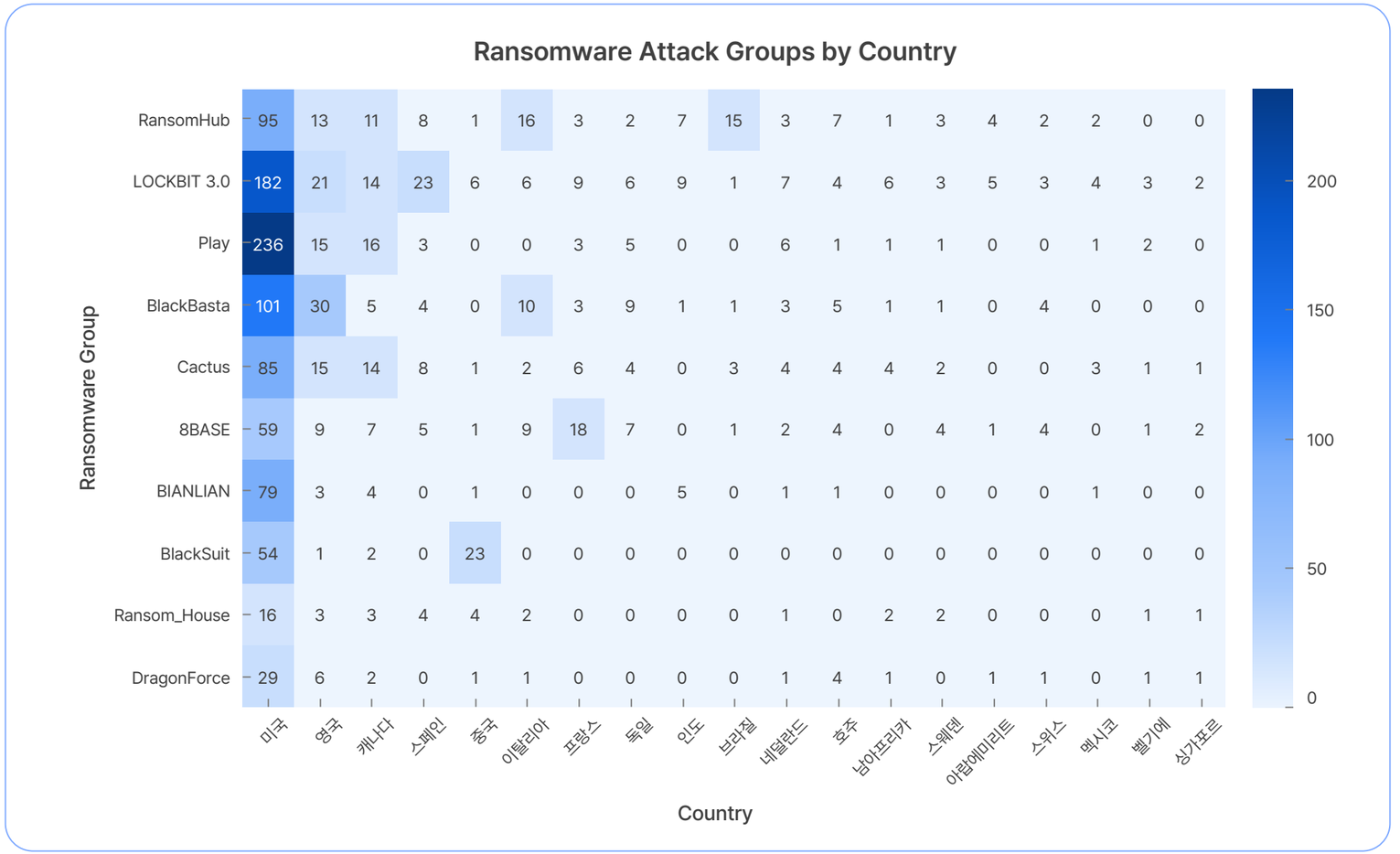
### 랜섬웨어 주요 피해 국가

2024년 랜섬웨어 피해 통계에 따르면, 미국이 가장 많은 랜섬웨어 공격을 받고 있고, Lockbit 3.0, Play 등 대규모 공격 그룹들이 미국의 기업 및 기관들을 주요 표적으로 삼았다.

미국의 공격 빈도가 높은 것은 다양한 요인이 복합적으로 작용하는데, 일단 세계 최대 경제 대국으로 제조, IT, 의료, 금융 등 다양한 산업이 발달해 있어 공격자들이 금전적 이득을 얻기 적합하다. 또한, 미국 기업들은 디지털 전환과 클라우드 도입 등 디지털 인프라 의존도가 높아 사이버 위협에 노출되기 특성을 가지고 있다. 특히, 많은 고객 데이터와 민감 정보가 디지털 공간에 저장되어 있어 이를 탈취해 랜섬을 요구하는 협박의 표적이 되기 쉽다.

미국 정부는 이러한 사이버 범죄에 대해 강력히 대응하고 있지만, 공격자들은 법적 관할권의 한계를 이용해 해외에서 공격을 수행하는 방식으로 제재를 피하고 있다. 또한 일부 랜섬웨어 그룹은 정치적·이념적 이유로 미국을 표적으로 삼는 경우도 있다.

이 밖에 캐나다, 영국, 스페인 등이 주요 피해국으로 나타났다. 유럽에서는 스페인, 프랑스, 독일 등이 Play, Cactus, LockBit 3.0 같은 공격 그룹들의 타깃이 되고 있다. 아시아와 남미에서는 인도와 브라질, 중동에서는 아랍에미리트가 랜섬웨어 공격에 일부 노출된 것으로 확인됐다.




[이미지] 국가 별 주요 랜섬웨어 피해 빈도

# 2024년 주요 사이버 보안 이슈

## 실제 침해 사례에서 확인한 공격자들의 주요 전략



안랩은 침해사고 분석(포렌식)을 통해 얻은 인사이트를 AhnLab TIP를 통해 제공하고 있다. 지난 1년 동안에는 총 22건의 포고서를 게시한 바 있다. 다음은 각 침해 사례를 포렌식하며 확인한 공격자들의 주요 전략 7개를 정리한 것이다.

### 1. 중앙 집중형 관리 솔루션 제로데이 취약점 악용

먼저, 중앙 집중형 관리 솔루션의 제로데이 취약점을 이용한 공격 사례가 다수 확인되었다. 공격자는 외부에 노출된 솔루션 취약점을 악용해 관리자 권한을 획득한 후, 솔루션의 기능을 이용해 악성코드를 전파했다. 이러한 솔루션들은 연결된 에이전트(agent) 시스템에 원격 제어, 원격 명령 실행, 프로그램 설치 및 실행 등 다양한 기능을 제공한다. 또한 에이전트는 시스템 제어를 위해 높은 권한으로 동작하기 때문에 이를 장악할 경우 별도의 권한 상승 없이도 시스템을 완전히 제어할 수 있게 된다. 공격자들은 이러한 특성을 이해하고 취약한 관리 솔루션에 접근한 뒤, 악성코드를 다운로드하는 원격 명령을 실행하거나 필수 소프트웨어 목록에 악성코드를 등록해 강제 설치하도록 유도했다

### 2. 공동 인증 솔루션 취약점 지속 악용

2024년 2월 26일, 드림시큐리티社 Non-ActiveX 공동인증서 프로그램 MagicLine4NX 프로그램의 버퍼 오버플로우 원격 코드 실행(RCE) 취약점(CVE-2023-45797)이 공개됐다. 이 취약점은 북한의 라자루스(Lazarus) 그룹이 활용한 것으로 알려졌다. 취약점 공개 후 보안 패치가 배포되고 업데이트가 강력히 권고되었음에도 불구하고, 여전히 취약한 버전의 MagicLine4NX를 사용하는 조직들이 있었다. 이로 인해, 침해 사고가 계속해서 발생했다.

### 3. 외부 노출 데이터베이스 서버 공격

외부에 노출된 MS-SQL 및 MySQL 서버들이 지속적으로 공격자들의 표적이 되었다. 공격자들은 이러한 서버들을 대상으로 무차별 대입 공격(Brute Forcing)과 사전 공격(Dictionary Attack)을 시도했다. 로그인에 성공한 공격자들은 xp_cmdshell, SQLShell 등의 기능을 이용해 악성코드를 감염시켰다. 해당 공격 방식은 랜섬웨어 그룹부터 APT 그룹까지 다양한 공격 집단에서 활용한 것으로 확인됐다.

### 4. MFA를 우회하는 피싱 공격의 진화

피싱 공격 기법이 지속적으로 진화하면서, 다중 인증(MFA)을 우회하는 AiTM(Adversary in The Middle) 피싱 공격이 새롭게 등장했다. 계정 정보를 노린 전통적인 피싱 공격은 정상 사이트를 사칭해 사용자의 로그인 계정 정보를 탈취한다. 탈취된 계정 정보의 악용을 예방하기 위해 추가 인증(MFA,Multi-Factor Authentication) 적용이 권고된다. 실제 사례를 보면, 공격자들은 Indirect Proxy 환경에 인프라를 구축하고 피해자가 피싱 사이트에 입력한 계정 정보 탈취했다. 그리고, 실시간으로 공격자 인프라에서 로그인을 시도해 MFA 요청을 발생시키는 방법으로 MFA를 우회한 사례가 확인됐다. 해당 기법은 피해자가 정상적인 로그인 과정으로 착각하기 쉬우며, 공격자는 정상 로그인 세션을 획득할 수 있게 된다.

### 5. 클라우드 전환에 따른 새로운 보안 과제

지난 수 년간, 비용, 관리, 보안 등 다양한 측면을 고려해 온프레미스에서 클라우드로의 마이그레이션이 진행되고 있다. 하지만, 보안 관점에서 보면 단순히 클라우드 환경으로 이전한다고 해서 안전이 보장되는 것은 아니다. 일부 침해 사례를 보면, 온프레미스 환경의 취약한 설정이 그대로 클라우드 환경으로 이전되거나, 클라우드의 보안 서비스를 제대로 활용하지 않아 오히려 더 많은 공격에 노출되는 경우가 있었다. 클라우드 서비스 제공자(CSP)와 보안 기업들은 다양한 클라우드 보안 서비스 및 솔루션들을 제공하고 있다. 클라우드 특성에 맞는 보안 정책을 수립하고, 보안 솔루션과 서비스를 적절히 사용해야만 강력한 보안 체계를 구축할 수 있다.

### 6. 업무 종사자를 사칭한 스피어 피싱

스피어 피싱 공격이 더욱 정교해지면서, 피해자와 업무 상 연관성이있는 실제 인물을 사칭하는 사례가 늘어난 것으로 파악됐다. 공격자들은 실존 인물로 위장해 수차례 메일을 주고받으며 피해자와 신뢰 관계를 구축했다. 이후, 견적서 등의 문서로 위장한 악성코드를 첨부해 전달했고 피해자는 의심 없이 첨부파일을 다운로드 받아 실행했다. 첨부 파일은 백도어 악성코드로 공격자는 백도어를 이용해 유효한 인증서 서명을 탈취했으며, 탈취된 인증서는 추후 공격자가 자체 제작한 악성코드를 서명하는데 악용됐다.

### 7. OT 환경을 겨냥한 랜섬웨어 공격 증가

OT 환경을 대상으로 한 랜섬웨어 공격 사례도 늘어나는 것으로 나타났다. 특히 제조업, 기반 시설 등에서 피해 사례가 두드러졌다. 일반적으로 OT 환경은 설비와 장비 유형을 고려해 네트워크 세그멘테이션(network segmentation)을 통해 네트워크를 구분하고, 외부와 단절된 폐쇄망 환경으로 운영한다. OT 환경의 시스템들은 외부에 노출되는 경우가 극히 드물기 때문에 보안 관리가 상대적으로 취약한 경우가 있다. 일부 침해 사례를 보면, OT 환경이 외부 인터넷과 연결되면서 보안이 취약한 시스템들이 랜섬웨어로 인한 피해를 입었다. 피해 환경에는 동일 제조사 장비들이 많았으며, 제조사에서 제공하는 초기 패스워드를 그대로 사용하면서 더 큰 피해로 이어졌다.

# 2024년 주요 사이버 보안 이슈

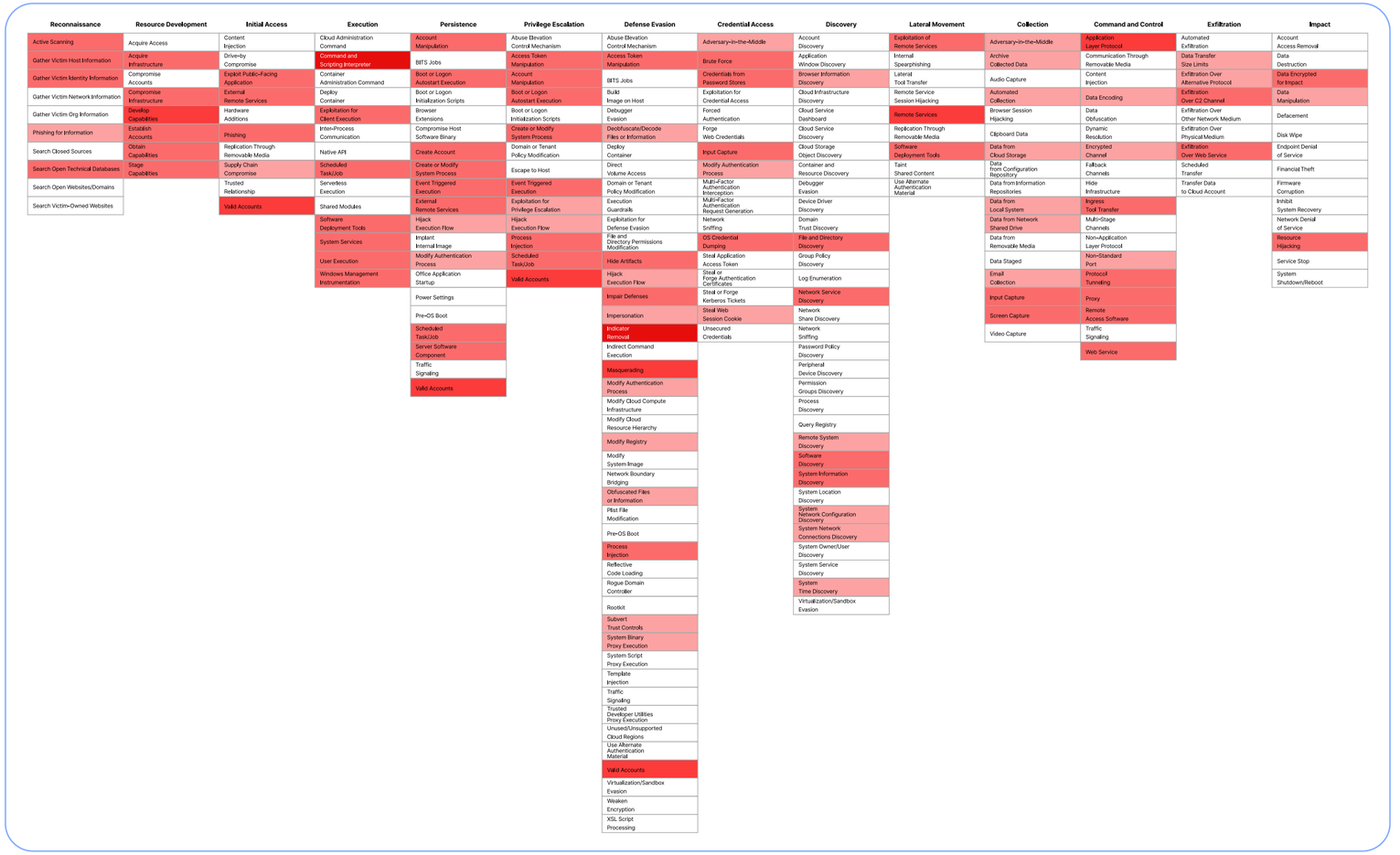


## 실제 침해 사례에서 확인한 공격자들의 주요 전략



### 공격자들의 주요 TTPs

2024년 공격자들이 주로 활용한 공격 전술, 기법 및 절차(Tactics, Techniques and Procedures, TTPs)는 다음과 같다. 주목할만한 점은 초기 침투 단계에서 유효한 계정을 활용한 접근이 빈번하게 이뤄졌다는 것이다. 또한, 대다수의 사례에서 추적을 피하기 위한 '안티 포렌식(anti-forensics) 기법이 적용된 흔적도 발견되었다.




[이미지] MITRE ATT&CK Framework 기준 2024년 공격자들이 사용한 주요 기법

# 2024년 주요 사이버 보안 이슈

## 악성코드 관련 주요 이슈



최근 1년 간 AhnLab TIP를 통해 제공한 위협 정보 유형과 콘텐츠 수량은 다음과 같다.

### 1. 실제 공격에 사용된 인터넷 익스플로러 제로데이 취약점

최근, 제로데이(0-day) 취약점을 통한 침해 사례가 증가하는 가운데, 불특정 다수를 대상으로 한 악성코드 유포에도 제로데이 취약점이 악용되는 것으로 나타났다. 안랩 ASEC(AhnLab SEcurity intelligence Center)과 국가사이버안보센터(NCSC, National Cyber Security Center) 합동분석협의체는 공동 분석을 통해 마이크로소프트 인터넷 익스플로러(Microsoft Internet Explorer, 이하 IE) 브라우저에서 새로운 제로데이 취약점을 발견하고, 해당 취약점을 이용한 공격을 상세 분석한 합동 분석 보고서(Operation Code on Toast by TA-RedAnt)를 공개했다.

해당 취약점은 IE의 자바스크립트 엔진(jscript9.dll)을 최적화하는 과정 중 데이터 타입을 잘못 해석해 'Type Confusion'이 발생하면서 발현될 수 있다.
분석 결과, 공격자는 토스트 광고 프로그램의 웹사이트를 해킹하고, 광고 페이지가 로드될 때 해당 취약점을 이용해 광고 프로그램이 설치된 PC에 악성코드 감염을 시도했다.

### 2. 유효한 인증서를 악용한 국내 게임사 대상 공급망 공격

최근 공격자들이 공급망 공격을 활발하게 시도하고 있다. 이유는 크게 두 가지가 있는데, 먼저 공격 성공 시 소프트웨어가 설치된 신뢰할 수 있는 경로를 사용해 악성코드를 은폐할 수 있다. 그리고, 침해한 소프트웨어를 사용하는 모든 조직 및 개인이 영향권에 있어 피해를 극대화시킬 수 있다. 일례로 2024년 4월과 5월, Larva-24008 공격 그룹은 국내 게임 보안 기업 '웰비아(Wellbia)'를 공격해 게임 보안 프로그램(XIGNCODE) 모듈(WatchDog)에 악성코드를 삽입했다. 그리고, 웰비아의 유효한 인증서로 서명해 악성코드를 유포했다.

그 결과, 해당 업체의 보안 모듈을 사용하는 게임들은 악성코드가 포함된 채로 배포됐다. 2024년 9월까지도 국내 게임사 공식 사이트를 통해 게임을 설치하는 과정에서 악성코드가 함께 설치된 것으로 확인됐다. 게임을 설치한 시스템에는 최종적으로 원격 제어 악성코드가 설치되어 제어 권한이 탈취됐다.

### 3. MS 오피스 크랙을 위장해 유포된 악성코드

윈도우, MS 오피스 등 정상 프로그램의 인증 도구나 크랙으로 위장해 악성코드를 유포한 사례도 다수 확인되었다. 이 기법은 웹하드, 토렌트 등 사용자들이 소프트웨어를 불법적으로 확보하고자 할 때 이용하는 경로를 주로 활요하며, 일반 사용자들이 많이 사용하는 프로그램으로 위장한다. 주로 설치되는 악성코드는 원격 제어 기능을 갖춘 Orcus RAT나 코인마이너(CoinMiner)인 XMRig 등이 있다. 여기에 더해 공격자는 감염 시스템에 작업 스케줄러를 등록해 악성코드를 업데이트하고 있다. 파일 진단을 우회하기 위해 한 주에도 수 차례 이상 새로운 악성코드를 유포하고 있으며 이는 최근까지도 지속되고 있다. 사용자들은 자료 공유 사이트에서 다운로드한 실행 파일 사용에 각별한 주의를 기울여야 한다. 또한, 유틸리티, 게임 등의 프로그램은 반드시 공식 홈페이지에서 다운로드해야 한다.

### 4. 정부기관 인물 사칭 피싱 메일 유포 (MSC 악성코드)

APT 공격 그룹은 악성코드 유포에 스피어 피싱 기법을 많이 사용한다. 공격자는 정찰을 통해 공격 대상자 정보를 수집하고 이를 기반으로 정상 사용자로 위장한 피싱 이메일을 제작한다. 이 때문에, 해당 메일을 수신한 사용자는 신뢰할 수 있는 이메일로 판단할 가능성이 높다. 안랩이 발행한 APT 공격 그룹 동향 보고서를 보면, 올해 하반기부터 스피어 피싱 기법을 이용한 악성코드 유포에 MSC 확장자를 가진 악성코드를 사용하는 유의미한 변화가 확인됐다. MSC(snap-ins/Management Saved Console) 확장자는 Microsoft Management Console(MMC)에서 사용하는 파일로 다양한 명령을 등록 및 실행하는데 활용할 수 있다.

이 기법은 김수키(Kimsuky) 그룹이 많이 사용하는 것으로 파악됐다. 공격자는 대상 업체 산업군과 관련된 인물을 사칭해 이메일을 발송했으며, 최초 발송 메일 첨부파일에는 악성코드를 포함시키지 않는 치밀함을 보였다. 사용자는 첨부된 정상 파일을 열람해 회신하고, 공격자는 재회신한 메일에 MSC 확장자의 악성코드를 다운로드 하도록 하는 URL이 포함된 메일을 보내 악성코드 감염을 유도했다.

### 5. 중국 세금 관련 프로그램을 통해 유포되는 백도어

국가의 기업 및 기관의 홈페이지는 많은 사용자들이 신뢰를 바탕으로 접속한다. 올해는 공격자들이 이러한 특성을 고려해 공격을 감행한 사례가 발견됐다. 2024년 4월, 중국 국가세무총국 홈페이지에서 배포 중인 세금 관련 프로그램을 통해 백도어로 의심되는 악성 파일이 유포되는 것을 확인했다.

대표적으로 악성 파일이 유포되는 주소는 hxxps://inv-veri.chinatax.gov[.]cn/xgxz.html이며, 동일한 파일이 다수의 중국 기업과 기관 홈페이지에서 배포된 것으로 확인됐다. 프로그램명은 "增值税发票开票软件（税务UKey版）"이고, 번역하면 "VAT 계산서 발행 소프트웨어(세금 UKey 버전)"라는 의미다. 자사 ASD(AhnLab Smart Defense) 인프라 로그 확인 결과, 해당 프로그램에 포함된 특정 실행 파일이 악성 실행 파일을 생성 후 실행하는 것으로 확인되었다. 결과적으로 시스템에 명령 실행이 가능한 백도어가 시스템에 상주하게 된다. 분석 당시 공격자 서버(C2)에서 악성 명령에 응답한 정황이 발견되지는 않았다. 하지만, 언제든 악성코드 실행, 정보 유출 등의 악성 명령을 내릴 수 있는 상태였다.

### 6. 보안 프로그램 설치 과정에서 감염되는 TrollAgent

홈페이지 접속 시 보안 프로그램 설치를 요구하는 이유는 주로 사용자와 웹사이트 간 데이터 전송을 보호하고, 악성코드나 해킹 시도로부터 시스템을 안전하게 지키기 위해서다. 2024년 2월 국내 건설 관련 협회 홈페이지에서 보안 프로그램 설치 시도 시, 악성코드가 다운로드 되는 정황을 확인했다. 홈페이지는 여러 서비스 사용을 위해 로그인이 필요하며, 다양한 보안 프로그램들을 설치해야 로그인을 진행할 수 있었다. 이 공격은 김수키(Kimsuky) 그룹의 소행으로 추정된다. 로그인을 위해 설치해야 하는 프로그램들 중 악성코드가 포함 설치 프로그램이 있었고, 사용자가 이를 다운로드해 설치할 경우 악성코드가 보안 프로그램과 함께 설치되는 형식이었다.

이러한 과정을 통해 설치되는 악성코드는 외부에서 공격자의 명령을 받아 악의적인 행위를 수행할 수 있도록 하는 백도어(Backdoor) 악성코드와 감염 시스템 정보를 수집하는 정보 탈취(Infostealer) 악성코드가 있다. 결론적으로 사용자는 공식 홈페이지에서 보안 프로그램을 설치하는 것 만으로도 개인 정보 탈취 등의 위험에 노출될 수 있는 것이다.

# 2024년 주요 사이버 보안 이슈

## 모바일 위협 트렌드



2024년 모바일 위협의 특징은 공격 기법 고도화와 피해 범위 확대로 요약할 수 있다. 금전적 이득을 노린 암호화폐 관련 스미싱과 금융 정보 탈취 목적의 악성 앱 유포가 급증했으며, 스테가노그래피(Steganography) 기술과 정교한 사회공학적 기법을 활용한 지능형 공격도 늘어났다. 메신저 서비스를 겨냥한 타깃형 공격이 증가하고, 북한 연계 위협 그룹의 스파이 활동도 발견되었다. 이는 모바일 위협이 개인을 넘어 국가 안보까지 위협하는 수준으로 발전했음을 시사한다.

### 1. 암호화폐 관련 스미싱 및 스캠 급증

2024년에는 암호화폐 관련 스미싱과 스캠이 크게 증가했다. 공격자는 이더리움 소각 등 암호화폐 관련 가짜 알림을 통해 피해자를 속였고, 소각 취소를 위한 수수료 명목으로 금전을 송금하도록 유도했다.  로맨스 스캠 방식의 접근도 확인되었는데, 소셜미디어를 통해 피해자에게 접근한 후 친분을 쌓고 가짜 암호화폐 거래소에 투자하도록 유도했다. 이 과정에서 가상 계정을 통해 먼저 소액의 수익을 보게 하여 피해자를 안심시킨 후 실제 투자를 유도해 큰 금전적 손실을 초래했다.

### 2. 금융 정보 탈취 목적의 악성 앱 증가

금융 정보 탈취를 목적으로 한 안드로이드 플랫폼을 기반 악성 앱 유포가 두드러졌다. SMSstealer와 같은 악성 앱은 문자메시지를 가로채 2단계 인증 절차를 우회하고, 피해자 계정에 접근해 금융 자산 탈취를 시도했다. 은행 및 백신 앱을 사칭한 카이시(Kaishi) 악성 앱은 원격 제어 기능을 통해 피해자의 금융 및 개인정보를 탈취하는데 사용됐고, 피해자의 통화 기록을 제어 및 감시하는 기능도 수행했다. 공격자는 주로 스미싱을 통해 악성 앱 설치를 유도하고, 피해자의 금융 정보와 개인 데이터를 공격자 서버로 전송하는 방식으로 심각한 피해를 입혔다.

### 3. 스테가노그래피 기법을 활용한 악성코드 은닉

스테가노그래피는 데이터를 다른 데이터에 삽입해 데이터를 은폐하는 기법이다. 2024년에는 스테가노그래피 기법을 사용해 탐지를 회피하는 악성 앱이 등장했다. 이 악성 앱은 이미지 파일에 악성 데이터를 숨긴 후, 앱 실행 시 이미지 연산을 통해 악성코드를 활성화하였다. 악성코드가 은닉되어 있고, 일부 코드가 무한 루프 상태로 설정되어 보안 탐지가 어려운 구조다. 일반 이미지 파일처럼 보이도록 만들어 피해자가 악성코드임을 인지하지 못하도록 한 점에서 올해 모바일 위협의 새로운 방식으로 주목받았다.

### 4. 텔레그램 계정을 노린 스미싱 증가

텔레그램 사용자 수가 늘어나면서, 이를 겨냥한 스미싱 공격도 급증했다. 공격자는 '정책 위반'이나 '보안 문제'와 같은 경고 메시지를 보내 텔레그램과 유사하게 제작된 피싱 사이트로 피해자가 접근하게 했다. 피싱 사이트에서 로그인 정보를 입력하면 공격자에게 전송되었다. 결국 피해자의 금융 및 개인정보가 공격자 서버로 전송되어 심각한 피해가 발생했다. 더 나아가, 공격자는 탈취한 피해자 계정에 접근해 대화 내용과 개인정보를 유출하고, 피해자의 지인들에게 유사한 스미싱 메시지를 발송해 추가적인 공격을 감행했다.

### 5. 북한 연계 공격 그룹의 악성 앱 활용

북한 연계 공격 그룹이 한국에서 민감 정보 수집과 스파이 활동을 목적으로 악성 앱을 배포한 것으로 나타났다. 해당 공격 그룹은 먼저 쿠팡(Coupang) 앱을 위장한 악성 앱을 제작해 피해자가 정상 앱으로 인식하게 만들었다. 악성 앱은 정상 앱과 거의 유사한 인터페이스를 제공해 사용자가 쉽게 인지하지 못하도록 설계되었다. 그리고, 포그라운드 서비스 권한을 요청해 백그라운드에서 개인정보와 금융 데이터를 수집 및 탈취했다.

# 2024년 주요 사이버 보안 이슈



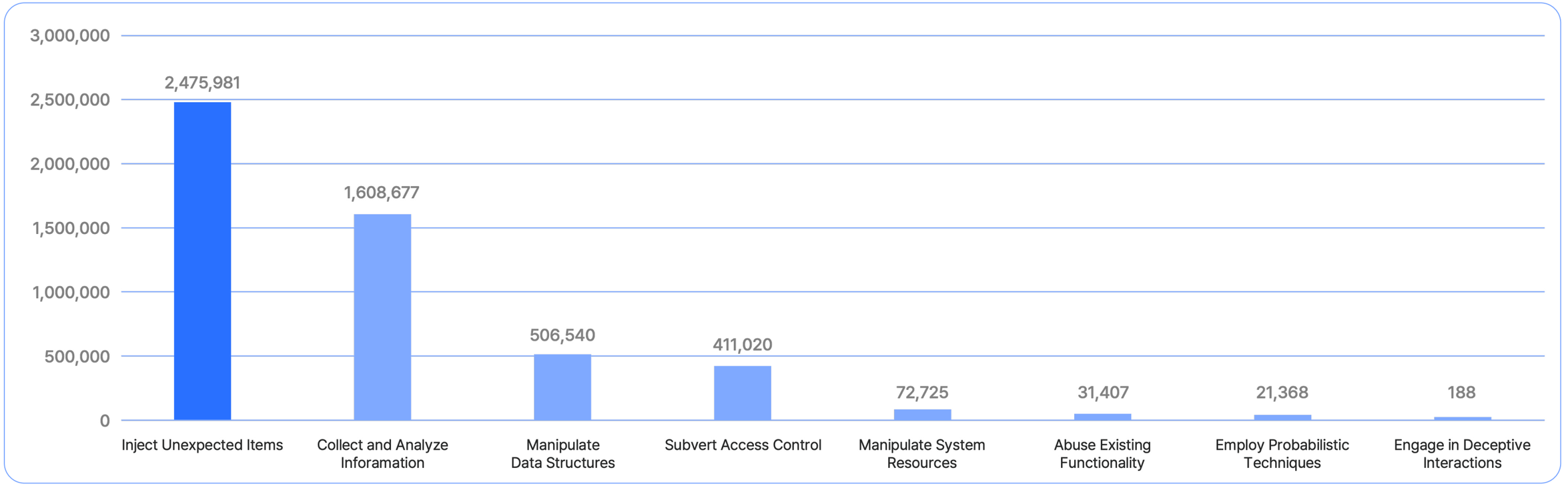
## 공격 유형 통계



### 2024 공격 유형 순위

안랩은 침해 대응 전문 조직인 CERT(Computer Emergency Response Team)을 운영하고 있으며, 매월 사이버 위협 추이를 분석한 'CERT 월간 보고서'를 발행하고 있다. 이를 통해, 2024년 사이버 공격 유형에 관한 통계를 확인할 수 있었다.

올해 가장 많이 발생한 유형의 공격은 예상치 못한 데이터 인젝션(Inject Unexpected Items)으로 나타났다. 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) 등이 뒤를 이었다




[이미지] 2024년 사이버 공격 유형 및 감행 빈도

# 2024년 주요 사이버 보안 이슈

## 공격 유형 통계



### 1. Inject Unexpected Items

예상치 못한 데이터 인젝션(Inject Unexpected Items)는 공격자가 시스템의 데이터 입력 인터페이스를 통해 예상치 못한 데이터를 주입해 시스템 동작을 제어 혹은 방해하는 방식이다. 이를 통해 애플리케이션이 정상적인 흐름에서 벗어나 예상치 못한 동작을 수행하게 한다. 주입된 값에 따라 애플리케이션이 비정상적으로 작동하거나 심각한 오류가 발생해 공격자가 의도한 목적을 달성할 수 있게 된다. 해당 공격은 주로 입력 값 검증이 미흡하거나 사용자 입력 처리가 허술한 시스템에서 발생하며, 시스템 안전성과 신뢰성이 크게 훼손될 수 있다.

### 2. Collect and Analyze Information

데이터 정보 수집 및 분석(Collect and Analyze Information)은 공격자가 능동적 질의나 수동적 관찰을 통해 대상 시스템의 정보를 수집하고 탈취하는 공격 패턴이다. 공격자는 시스템 구성 정보, 사용자 정보, 네트워크 구조 등의 정보를 수집해 향후 공격 경로를 설계하거나 잠재적인 취약점을 찾아낸다. 정보 수집 과정은 향후 더 정밀한 공격의 발판이 되고, 초기 침투의 중요한 준비 단계로 사용된다. 특히, 수집된 정보는 피싱 공격이나 소셜 엔지니어링 등 추가적인 공격 계획에 핵심적인 역할을 한다.

### 3. Manipulate Data Structures

공격자가 데이터 구조를 조작하여 시스템이 정상적인 데이터 처리 흐름에서 벗어나도록 한다. 이를 통해 시스템의 내부 데이터 흐름을 방해하거나 변조하여 비정상적인 결과를 유도한다. 데이터의 무결성 또는 일관성을 깨뜨려 시스템 안정성에 영향을 주며, 예기치 않은 오류를 일으킬 뿐 아니라 데이터의 신뢰성을 손상시키는 경우가 많다. 이러한 조작은 데이터베이스, 메모리 구조 등에 영향을 주어 프로그램이 악의적인 목적으로 오작동하게 하며, 데이터 유출이나 조작된 결과를 초래할 수 있다.

### 4. Subvert Access Control

접근 제어 조작(Subvert Access Control)은 공격자가 접근 제어 메커니즘을 우회해 허가되지 않은 권한을 얻고 시스템에 부적절하게 접근하는 것을 의미한다. 공격자는 관리자 권한이나 고급 사용자 권한을 부당하게 획득해 민감 데이터나 특정 기능을 조작할 수 있게 된다. 접근 제어가 무력화되면서, 중요 정보가 노출되고 시스템의 전반적인 무결성이 위협 받게 된다. 더 나아가, 보안 아키텍처의 근간을 흔들어 사용자 인증 절차를 훼손하고, 중요 자산에 무단으로 접근해 조직 전체 보안에 심각한 위험을 초래한다.

# 2024년 주요 사이버 보안 이슈

## 공격 유형 통계



### 5. Manipulate System Resources

공격자가 시스템 리소스(예: CPU, 메모리 등)를 과도하게 소모하게 하여 성능을 저하시키거나 자원을 고갈시키는 방식이다. 시스템은 정상적인 서비스를 제공하기 어려워지며, 사용자는 응답 속도가 느려지거나 시스템이 정지 상태에 빠지는 상황을 경험하게 된다. 자원을 고갈시키는 방식으로 장기적인 관점에서 서비스 거부(DoS)와 유사한 공격 효과가 있다.

### 6. Abuse Existing Functionality

공격자가 시스템이나 애플리케이션의 기존 기능을 악용해 의도하지 않은 방식으로 작동하게 만드는 기법이다. 새로운 코드를 추가하지 않고, 정상적인 기능을 악용해 피해를 유발시킨다. 예를 들어, 고객 서비스의 파일 업로드 기능을 악성 파일 전달에 이용하거나, 검색 기능을 악의적으로 사용해 내부 정보를 노출시키는 방식이 있다. 기존 기능의 예상치 못한 활용으로 보안 허점을 파고들며, 시스템이 원래 제공하지 않는 기능을 의도적으로 수행하게 만든다.

### 7. Employ Probabilistic Techniques

공격자가 확률 기반 기법을 사용해 시스템의 취약점을 찾거나 성공 확률을 높이기 위한 기법을 의미한다. 일반적으로 브루트 포스(Brute Force) 공격이나 타이밍 공격이 이에 해당된다. 통계적으로 보면, 반복적인 접근 시도를 통해 목표한 시스템에 침투하거나 암호를 추측해내는 경우가 많다. 시간이 지남에 따라 점진적으로 성공 확률을 높여 공격 목표를 달성하는 형태다. 특히, 암호화 체계가 약한 시스템에 효과적이며, 사용자가 알지 못하는 사이에 점진적인 침입을 받게 된다.

### 8. Engage in Deceptive Interactions

공격자가 대상 시스템이나 사용자와 상호작용할 때, 실제 신원이나 의도를 숨기고 잘못된 정보를 전달해 원하는 결과를 얻는 방식이다. 피싱, 사회공학, 가짜 웹사이트 혹은 이메일을 이용한 스캠을 통해 자주 나타난다. 간단히 하면, 사용자를 속여 민감 정보를 입력하게 하거나 악성 파일을 다운로드하게 만드는 방식이다. 사용자의 신뢰를 악용해 시스템에 침투하며, 피해자가 의심 없이 조작된 정보를 제공하도록 유도하는 점이 특징이다.

# 2024년 주요 사이버 보안 이슈

## 공격 유형 통계



### 2024 산업군 별 공격 유형 통계

2024년에는 거의 모든 산업군에 걸쳐 예상치 못한 데이터 인젝션(Inject Unexpected Items) 공격의 비율이 높았다. 해당 기법은 보험 업종에서 가장 높은 비율(69.8%)로 탐지됐다. 건설, 법률/세무, 통신사 업종은 정보 수집 및 분석(Collect and Analyze Information) 공격의 비율이 가장 높았고, 건설 업종(76.8%)에서 가장 높은 비율로 탐지됐다.

두 공격 유형 제외하면, 운송 업종에서 시스템 리소스 변경(Manipulate System Resources)이 16.2%로 타 산업군에 비해 두드러졌다. 게임 개발 및 전자/반도체 업종은 데이터 구조 변경(Manipulate Data Structures) 공격 비율이 각각 18.1%와 20.5%로 다른 업종에 비해 높았다.

이처럼 산업군 별 공격 유형 특성과 비율을 참고 및 분석하면, 각 산업 특성에 맞는 보안 대책과 가이드라인을 마련하는데 도움이 된다.

산업군 별 공격 유형 비율 TOP 5

| | Inject Unexpected Items | Collect and Analyze Inforamtion | Manipulate Data Structures | Subvert Access Control | Manipulate System Resource |
|---|---|---|---|---|---|
| 개임개발 | 55.5% | 11.2% | 18.1% | 13.9% | 1.0% |
| 공공 | 42.3% | 40.0% | 12.0% | 4.2% | 1.0% |
| 교육 | 37.6% | 43.2% | 5.8% | 5.1% | 6.8% |
| 금융 | 47.4% | 29.6% | 11.7% | 4.1% | 2.8% |
| 닷컴(IT) | 47.9% | 29.4% | 11.3% | 9.2% | 0.4% |
| 방송 | 41.2% | 30.3% | 9.9% | 16.4% | 1.4% |
| 유통 | 46.1% | 43.3% | 6.5% | 3.3% | 0.2% |
| 제조 | 53.7% | 30.9% | 8.4% | 6.4% | 0.4% |
| 의료 | 48.1% | 35.2% | 8.3% | 7.3% | 0.9% |
| 보험 | 69.8% | 10.8% | 9.7% | 8.0% | 0.1% |
| 중공업 | 60.8% | 26.0% | 7.4% | 5.1% | 0.2% |
| 전자/반도체 | 57.5% | 12.9% | 20.5% | 7.4% | 1.2% |
| 여행/숙박/외식업 | 46.9% | 36.0% | 8.9% | 2.9% | 5.1% |
| 건설 | 20.1% | 76.8% | 2.2% | 0.9% | 0.0% |
| 운송 | 47.3% | 16.1% | 17.0% | 3.0% | 16.2% |
| 법률/세무 | 35.0% | 49.5% | 5.5% | 2.6% | 0.4% |
| 통신사 | 44.0% | 47.6% | 4.6% | 3.8% | 0.0% |
| 지역케이블 | 0.0% | 0.0% | 0.0% | 0.0% | 0.0% |
| ISP 기타 | 0.0% | 0.0% | 0.0% | 0.0% | 0.0% |
| 기타 | 38.9% | 50.5% | 5.5% | 3.5% | 1.2% |

[이미지] 산업군 별 공격 유형 비율 TOP 5

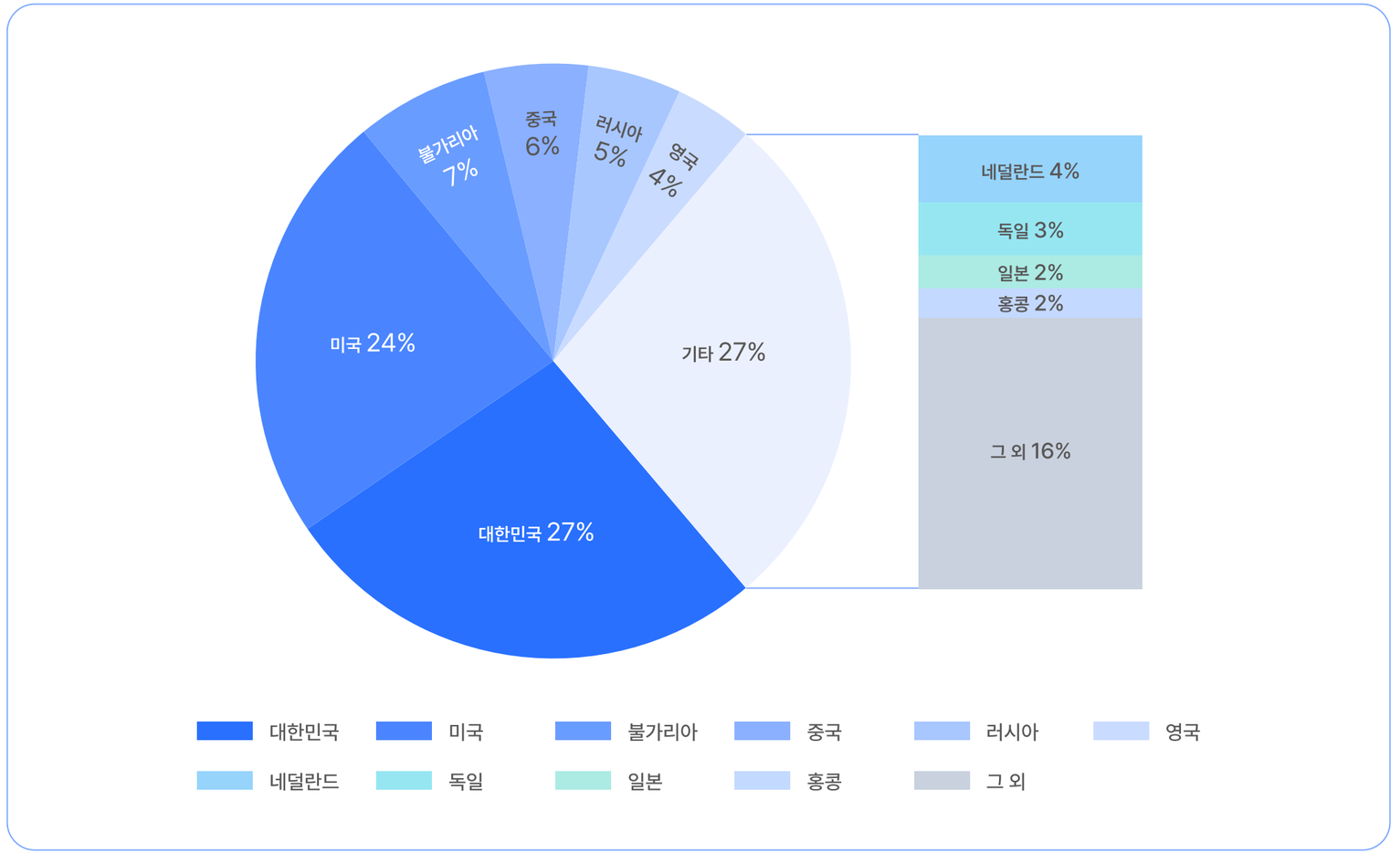
# 2024년 주요 사이버 보안 이슈

## 공격 유형 통계



### 공격 국가 TOP 5

안랩의 보안 장비별 탐지 로그의 출발지 IP 주소를 기준으로 분석을 진행한 결과, 국내 IP 주소를 사용한 공격 시도 비율이 27%로 가장 높았다. 그 뒤를 이은 공격 시도 출발지는 미국 24%, 불가리아 7%, 중국 6%, 러시아 5%로 집계됐다




[이미지] 공격 시도 국가 비율

# 2025년 사이버 보안 전망

- 2025년 전망 Top 5

# 2025년 사이버 보안 전망



## 2025년 전망 Top 5

2025년 사이버 보안 환경은 AI 기술 발전, 클라우드 및 IoT 확산 등으로 인해 더욱 복잡하고 도전적인 양상을 띨 것으로 전망된다. 조직들은 예방 중심의 보안 접근법을 강화하고, AI 기반 도구를 적극 활용해 진화하는 위협에 대응해야 한다.

### 1. AI 기반 공격 증가

AI는 2025년 공격자들이 사이버 공격을 전개하는데 있어 핵심적인 역할을 담당할 것으로 예상된다. 생성형 AI 기술이 공개된 이후, AI는 전 산업에 걸쳐 다양한 형태로 적용되고 있다. 공격자들도 사회공학 기법, 취약점 탐색, 악성코드 개발 등에 AI를 적극적으로 사용하고 있다. AI로 인해 공격의 진입 장벽은 낮아지고, 자동화 및 대규모화가 진행될 것으로 예상된다. 또한, AI를 활용해 만든 새로운 형태의 공격도 등장할 것이다.

- AI 기반 사회공학 기법 활용 증가 (타깃의 언어, 상황, 심리 등을 고려하고, 딥페이크 등을 활용한 정교한 피싱 및 비즈니스 이메일 침해)
- 소프트웨어의 소스코드, 바이너리, 설정 취약점 탐색에 활용
- 실시간 데이터 기반 학습을 통해 탐지를 회피하는 적응형 멀웨어 개발
- 소규모 해커 그룹도 대규모 사이버 공격 가능

### 2. 공급망 공격 증가

디지털 전환과 초연결이 가속화되면서 소프트웨어와 IT 시스템에 대한 기업과 기관들의 의존도도 점점 높아지고 있다. 타사 소프트웨어, 오픈소스 활용이 증가하고, 소프트웨어 공급망이 복잡하게 얽히면서, 공급망 관리는 단일 기업이 관리할 수 있는 수준을 넘어섰다. 공격자 입장에서는 공급망 공격은 성공 시 큰 효과를 얻을 수 있기 때문에 앞으로도 소프트웨어 공급망 공격은 지속적으로 증가할 전망이다.

### 3. 클라우드 및 IoT 확산에 따른 공격 표면 확대

기업과 기관들의 클라우드 도입이 가속화되면서 클라우드 취약점을 노린 공격도 증가할 것으로 예상된다. 특히, 멀티 클라우드 환경의 복잡성을 악용한 공격이 늘어날 전망이다.  또한, 2025년까지 IoT 기기 수가 320억 개를 넘어설 것으로 예상되는 가운데, 클라우드와 연결된 디바이스까지 더해져 공격 표면이 크게 확대될 것으로 보인다. 이는 공격자들에게 더 많은 공격 기회를 제공할 것이며, IoT 기기 취약점이 악용되는 사례도 늘어날 것으로 보인다.

### 4. 적대 세력 간 사이버전 및 핵티비스트 활동 증가

러시아-우크라이나 전쟁과 중동 지역 분쟁 등 국가 간 갈등국면은 2025년에도 계속될 전망이다. 이에 따라, 적대 세력 간 사이버 공격도 더 빈번하게 전개될 것으로 보인다. 교묘한 공격 기법을 활용해 주요 기반 시설이나 정부 시스템을 노리는 등 더욱 파괴적인 형태를 띨 가능성이 높다. 이와 함께 정치적, 사회적 이슈에 대한 해킹 활동을 펼치는 핵티비스트(hacktivist)들의 활동도 더 활발해질 것으로 예상된다. 특히, AI와 딥페이크 기술의 발전으로 더욱 영향력 있는 공격 캠페인이 가능해질 것이다.

### 5. 랜섬웨어 공격 고도화

랜섬웨어에 의한 피해는 특정 국가 및 특정 산업군에 국한되지 않으며, 피해 규모도 점점 증가하고 있다. 이에 각 국가 법집행 기관의 대응도 점점 강화되는 추세다. 하지만, 랜섬웨어는 공격의 마침표를 찍을 수 있는 공격자의 확실한 무기이므로, 2025년에도 여전히 주요 위협 중 하나로 자리할 전망이다. 랜섬웨어 시장 자체도 점점 포화 상태에 이르고 있기 때문에, 시장에서 경쟁력을 갖추고 생존을 위해 노력하는 공격자들의 기법과 기술 수준도 고도화를 거듭할 것으로 보인다. 그 결과, 무차별적 공격이 아닌 특정 기업이나 기관을 노린 표적 공격이 증가할 것으로 예상된다.

AhnLab



㈜ 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