2026 에디션

악성 봇 보고서

에이전틱 시대의 악성봇

#2026악성봇보고서

cpl.thalesgroup.com

THALES
CYBERSECURITY

#2026악성봇보고서

보고서 소개

AI 기반 자동화는 이제 태동기를 지나, 인터넷 트래픽 속에 깊숙이 자리 잡고 있습니다.

2026 탈레스 악성 봇 보고서는 AI 기반 자동화가 애플리케이션 및 API 접근 방식을 어떻게 변화시키고 있는지 분석합니다.
현재 봇은 전 세계 웹 트래픽의 대부분을 차지하고 있습니다. 에이전틱 AI가 새로운 유형의 자동화 트래픽을 만들어 냄에 따라, 기업들은 의도를 파악·구분·통제하기가 더욱 어려워진 복잡한 환경에 대응해야 합니다.

본 보고서는 2025년 전체 봇 활동 데이터를 분석하며, 전 세계 산업 전반의 봇 공격을 탐지·대응하는 탈레스 위협 연구팀(Thales Threat Research)과 보안 분석가 서비스(SAS) 팀의 인사이트를 종합했습니다.

THALES
CYBERSECURITY

#2026악성봇보고서

주요 수치

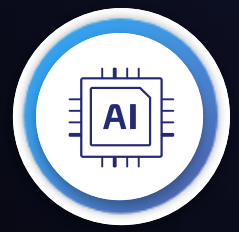
17.2조
2025년 탈레스가 차단한 봇 요청 수

21%
비지니스 로직을 표적으로 한 봇 공격 비율

12.5x
AI 기반 봇 공격의 전년 대비 증가율

40%
악성 봇이 차지하는 인터넷 트래픽 비율

20%
탈레스가 차단한 봇 요청 비율



봇이 차지하는 전체 인터넷 트래픽 비율

THALES
CYBERSECURITY

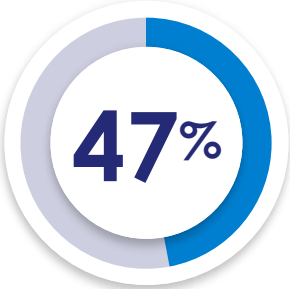
#2026악성봇보고서

중요한 수치

42%
단순 봇 공격

41%
Chrome으로 위장해 정상 트래픽처럼 보이는 봇 공격

24%
금융 서비스 사이트를 겨냥한 봇 공격



봇이 차지하는 인터넷 트래픽 비율

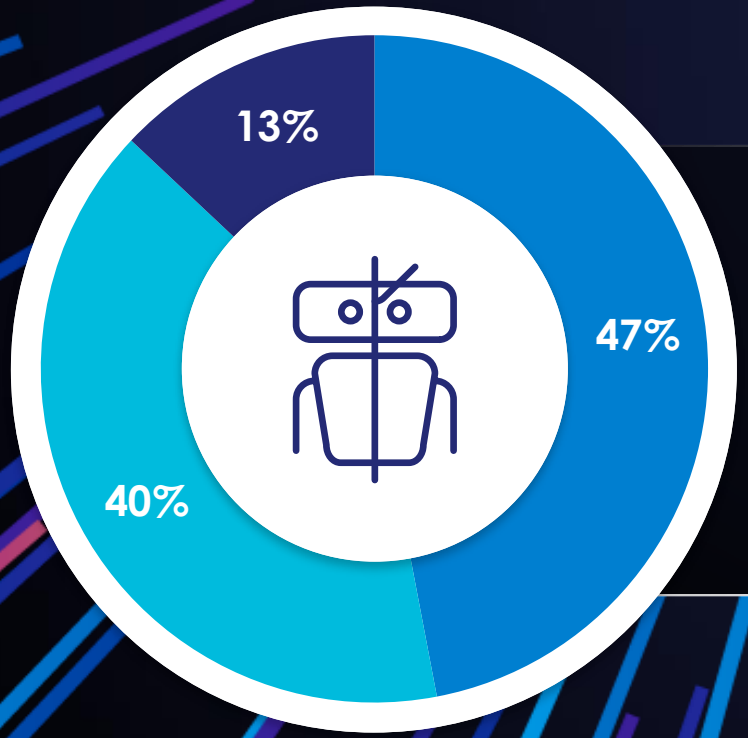
27%
API를 표적으로 한 공격

46%
금융 서비스를 겨냥한 계정 탈취(ATO)공격

THALES
CYBERSECURITY

#2026악성봇보고서

악성 봇 vs 정상 봇 vs 인간 트래픽



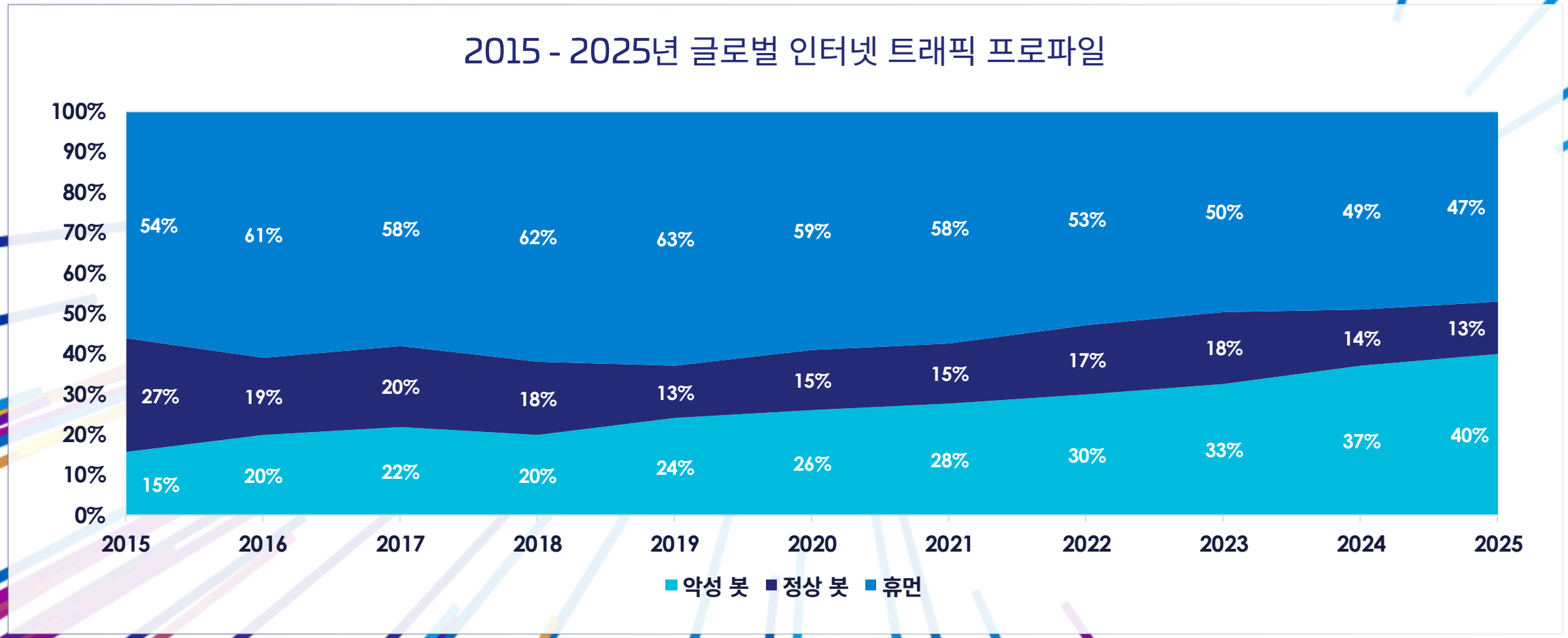
2025년 봇 트래픽 vs 정상 봇 트래픽 vs 휴먼 트래픽

휴먼 악성 봇 정상 봇

봇 트래픽이 2년 연속 휴먼 트래픽을 앞질렀습니다.

THALES
CYBERSECURITY

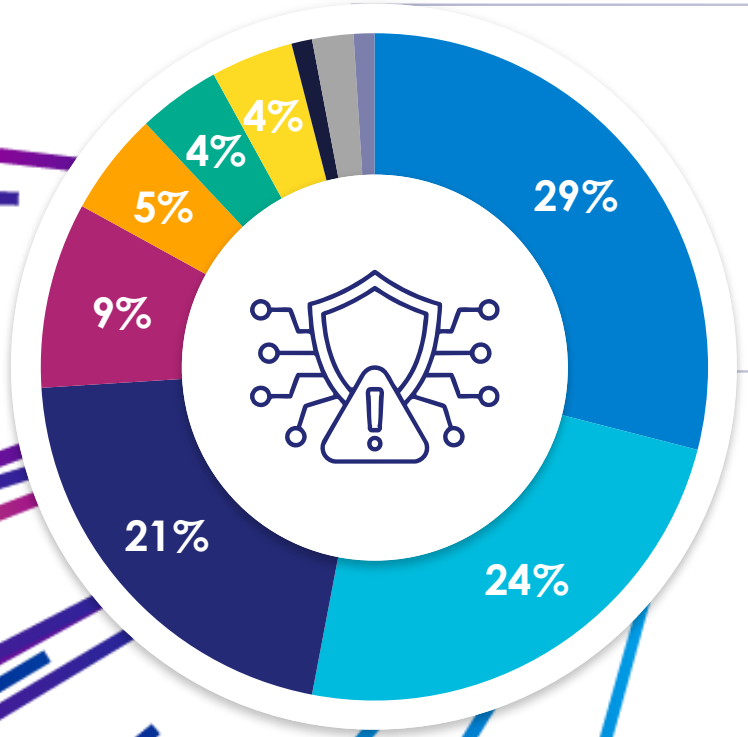
년도별 봇 트래픽 추이



THALES
CYBERSECURITY

#2026악성봇보고서

가장 일반적인 공격 유형



2015 - 2025년 글로벌 인터넷 트래픽 프로파일

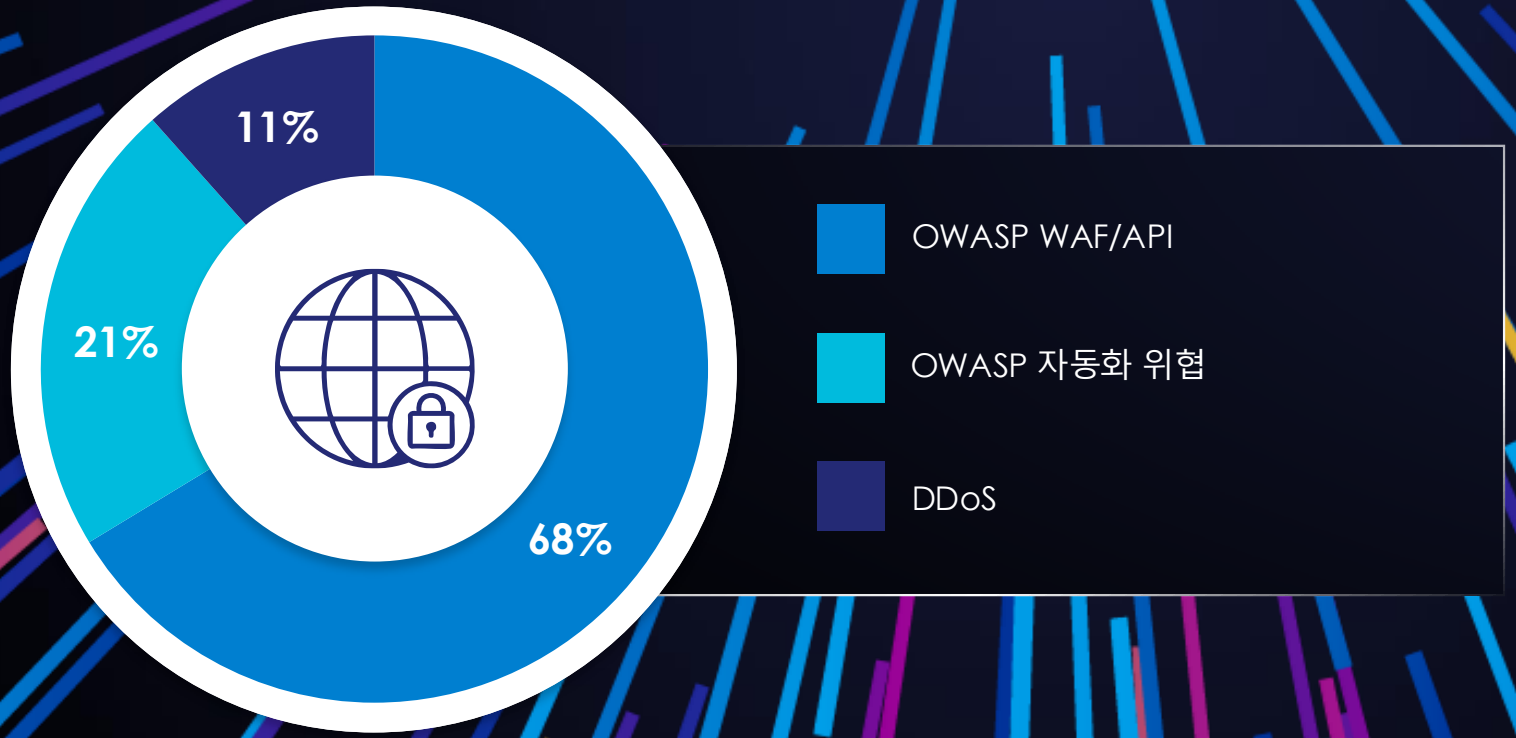
- 일반 자동화
- 경로 탐색
- XSS
- 기타 2%
- API 위반
- 데이터 유출
- SQI 1%
- 비지니스 로직 악용
- RCE/RFI
- 프로토콜 조작 1%

- 일반 자동화(무차별 대입 및 위약점 스캐닝) 29%
- API 위반24%
- 비지니스 로직 악용21%

THALES
CYBERSECURITY

#2026악성봇보고서

OWASP 공격 카테고리



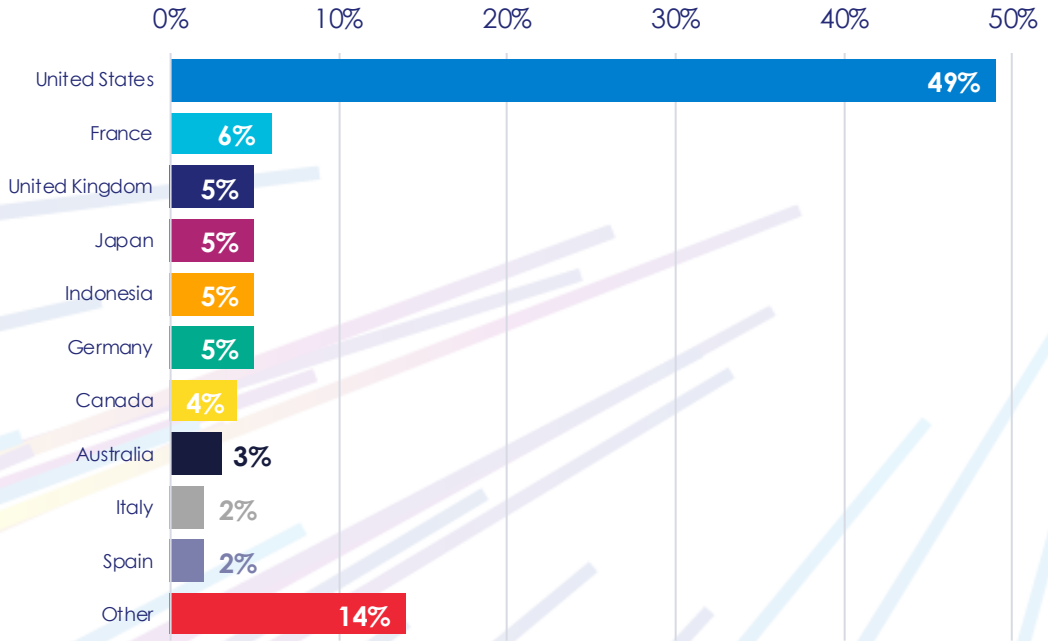
- 탐지·대응된 전체 공격의 21%가 OWASP 정의 자동화 위협
- OWASP 21대 자동화 위협은 자동화를 활용해 웹 애플리케이션 취약점을 대규모로 악용

THALES
CYBERSECURITY

#2026악성봇보고서

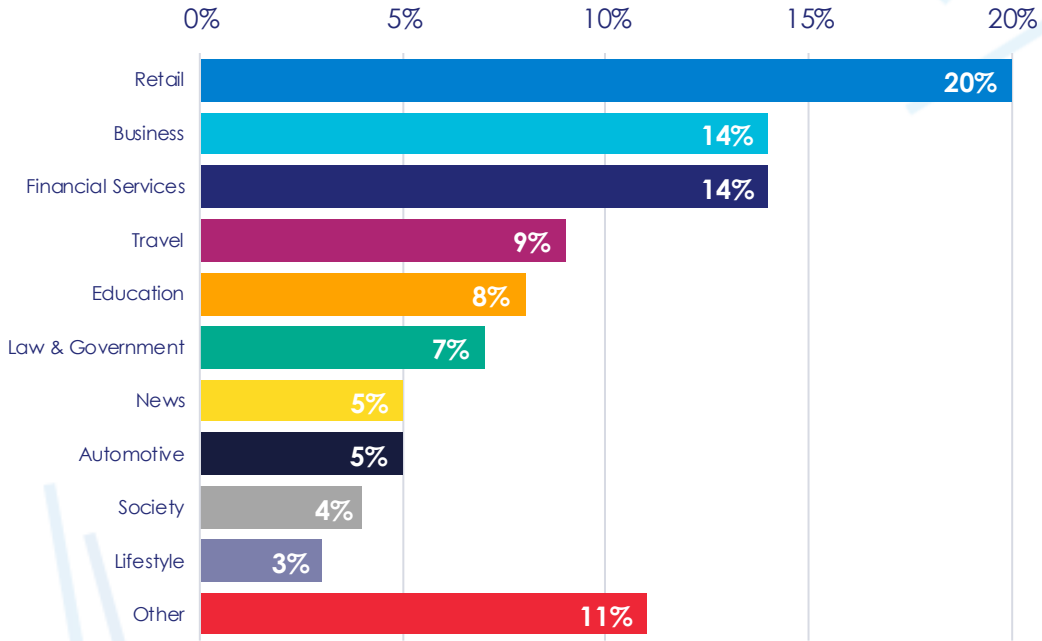
에이전틱 AI와 악성 봇 – 인프라 위협

AI 봇에 가장 많은 표적이 된 상위 10개국



AI 봇의 공격을 가장 많이 받은 국가는 미국입니다.₩

AI 봇에 가장 많은 표적이된 상위 10개 산업



AI 봇 공격을 가장 많이 받은 산업은 리테일입니다.

THALES
CYBERSECURITY

#2026악성봇보고서

탐지가능한 AI 트래픽은 빙산의 일각

2024
2 Million
일일 평균 차단 공격

증가
12.5x

2025
25 Million
일일 평균 차단 공격

탐지 가능한 AI 트래픽 (수면 위)

탐지 불가능한 AI 트래픽 (수면 아래)

THALES
CYBERSECURITY

#2026악성봇보고서

AI 크롤러 봇 트래픽 출처 (7일간)

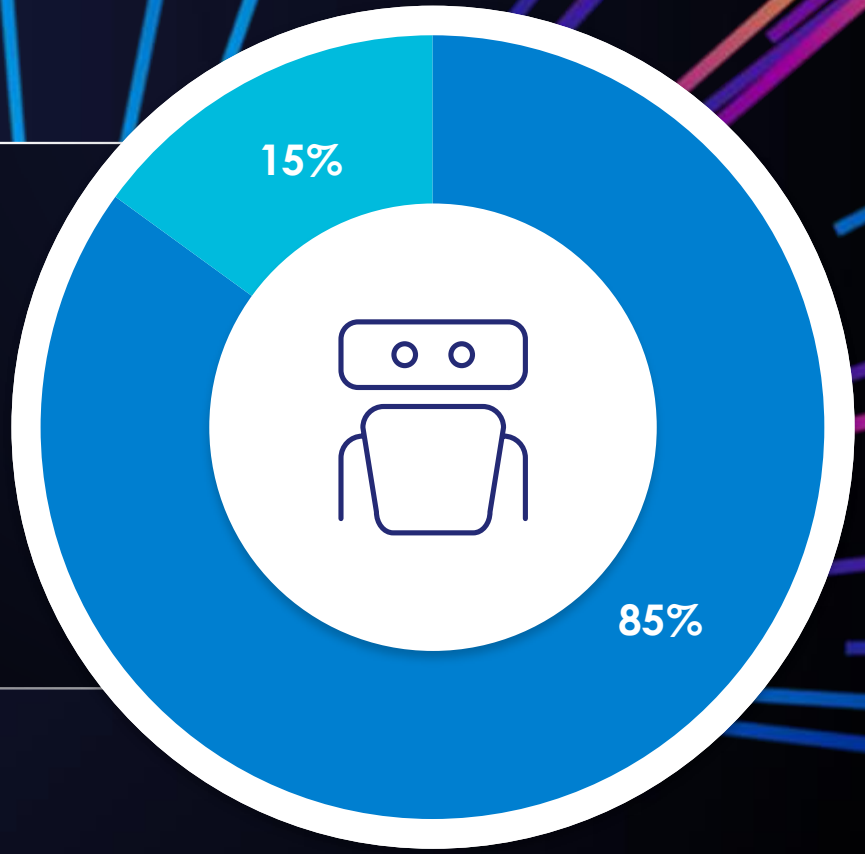
약
9%
의 AI 크롤₩러 세션이 악성 봇 탐지 규칙 발동

10% 이상
의 AI 수행봇은 악성 봇 탐지 규칙 발동

2025

AI 크롤러 봇
AI 크롤러 봇은 모델 학습용 데이터 수집

AI 패처 봇
AI 페처봇은 사용자 프롬프트에 따라 작업 수행



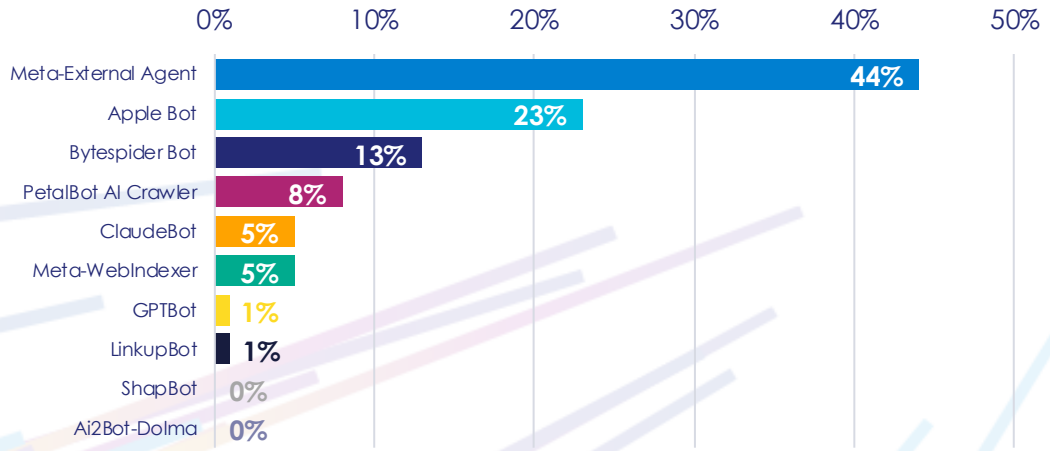
크롤러의 약 12%, 페처의 7% 가 고객이 정의한 규칙에 의해 차단

THALES
CYBERSECURITY

#2026악성봇보고서

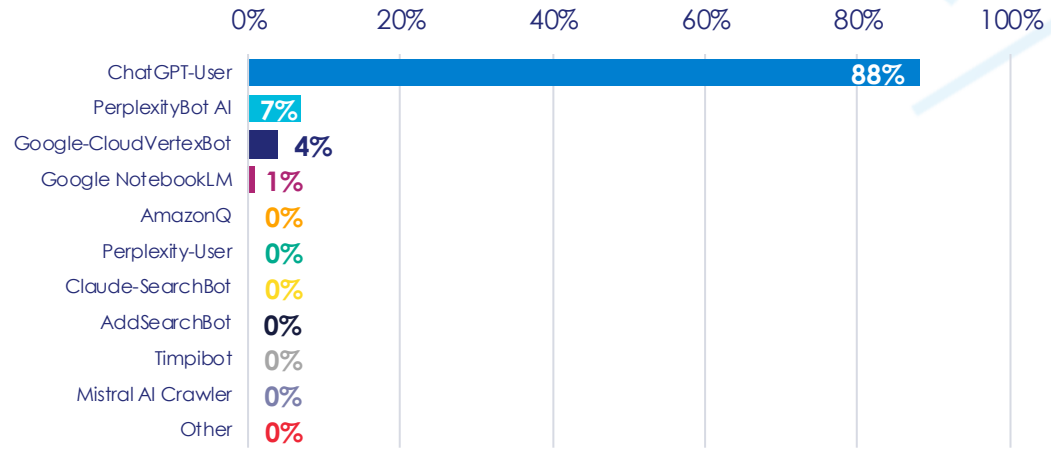
AI 크롤러 및 패처 봇 트래픽

AI 크롤러 봇 트래픽 출처 (7일간)



- 7일간 AI 크롤러 봇 트래픽 출처별 분석
- 소수의 지배적 사업자가 활동을 주도함

AI 패처 봇 트래픽 출처 (7일간)

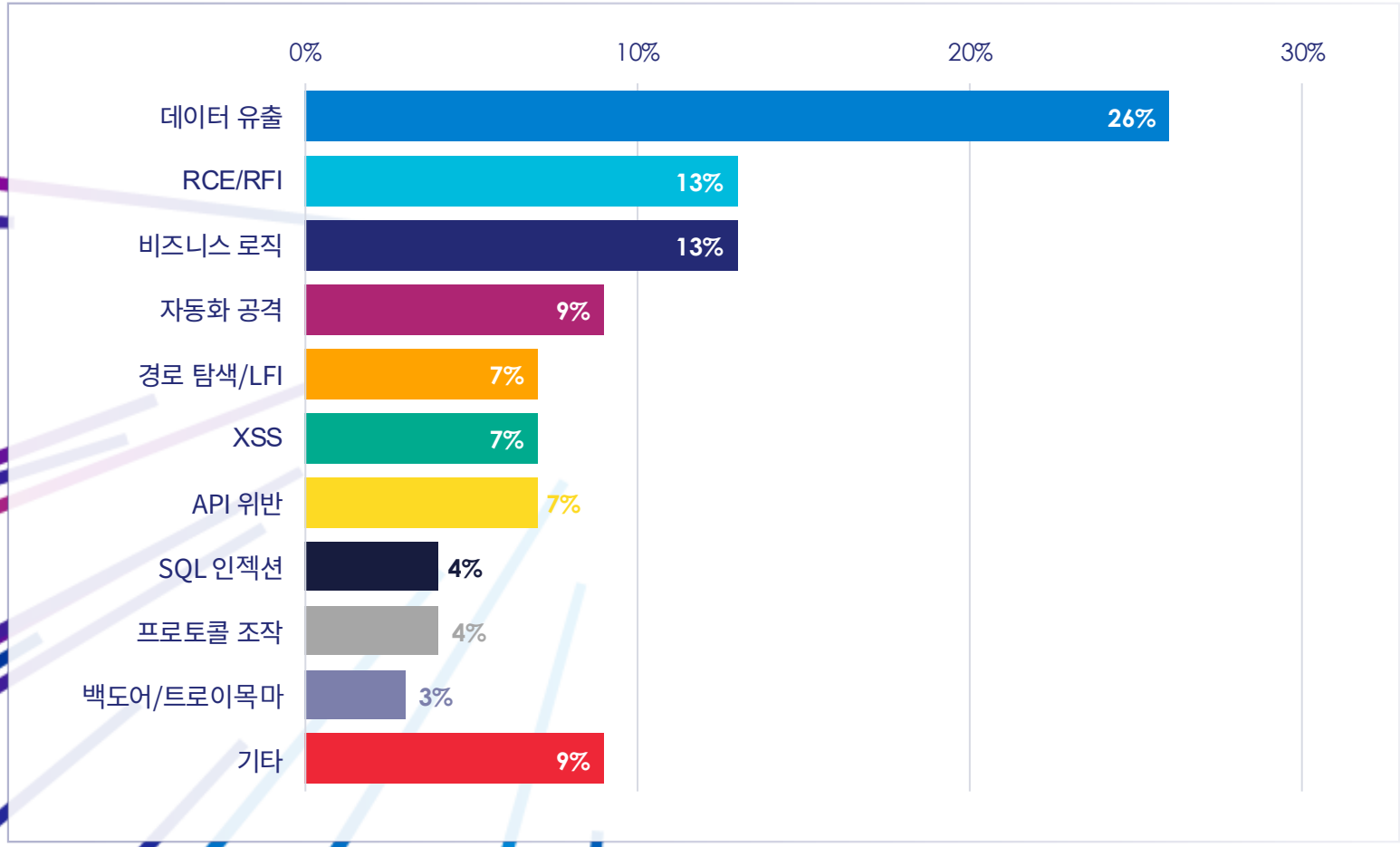


- 7일간 AI 페처 봇 트래픽 출처별 분석
- 단일 지배적 사업자가 개부분의 활동을 차지함

THALES
CYBERSECURITY

#2026악성봇보고서

악성 봇과 API 공격 표면

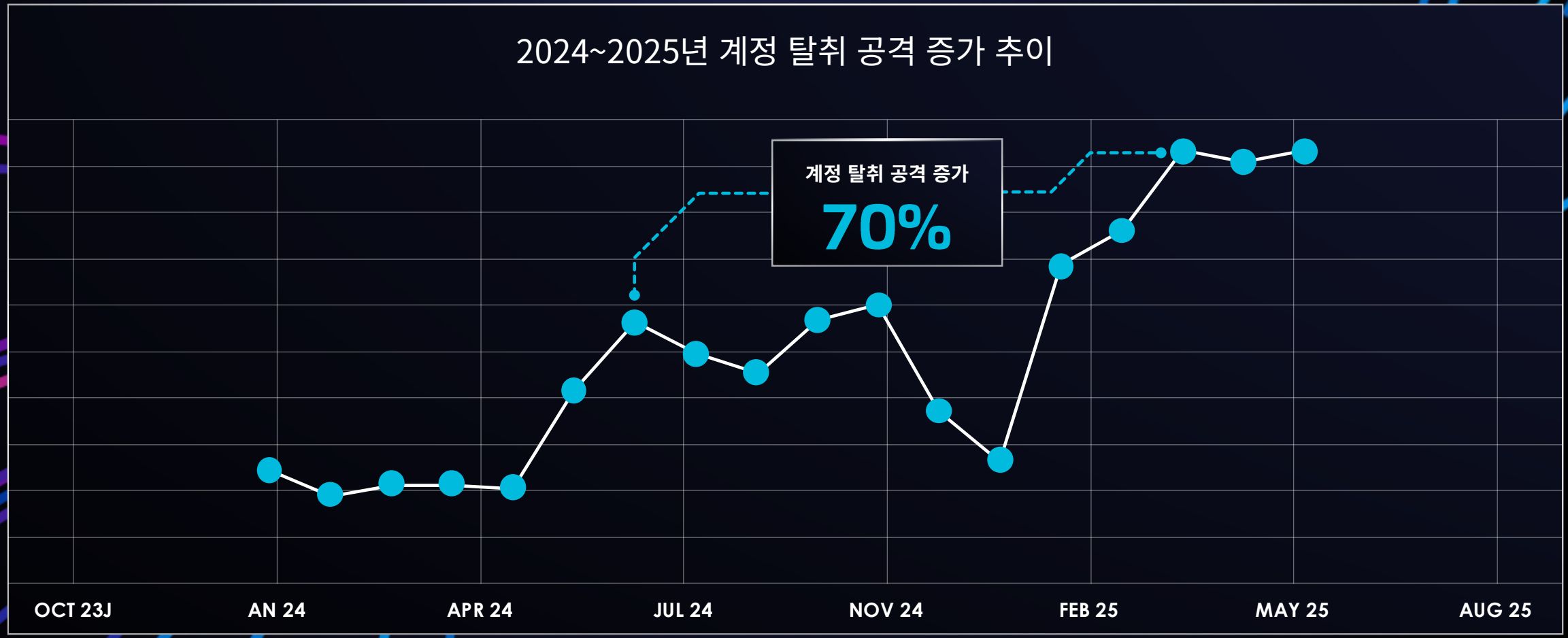


API가 보호되지 않으면
비즈니스 로직이
노출됩니다.

THALES
CYBERSECURITY

#2026악성봇보고서

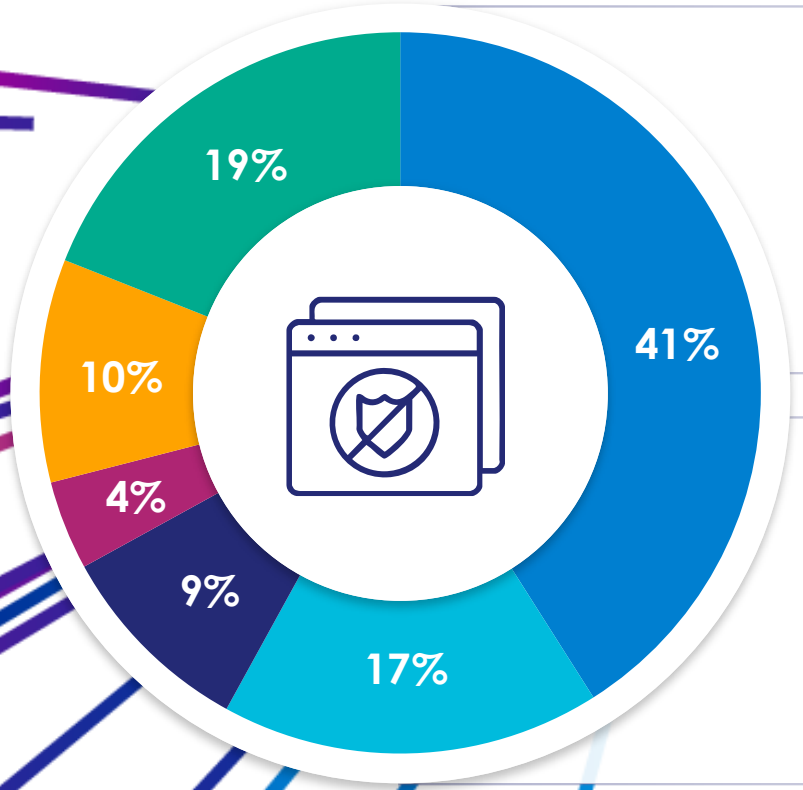
계정 탈취: 자동화 사기로 가는 최단 경로



THALES
CYBERSECURITY

#2026악성봇보고서

브라우저로 위장하는 봇



2025년 봇의 브라우저 위장 현황

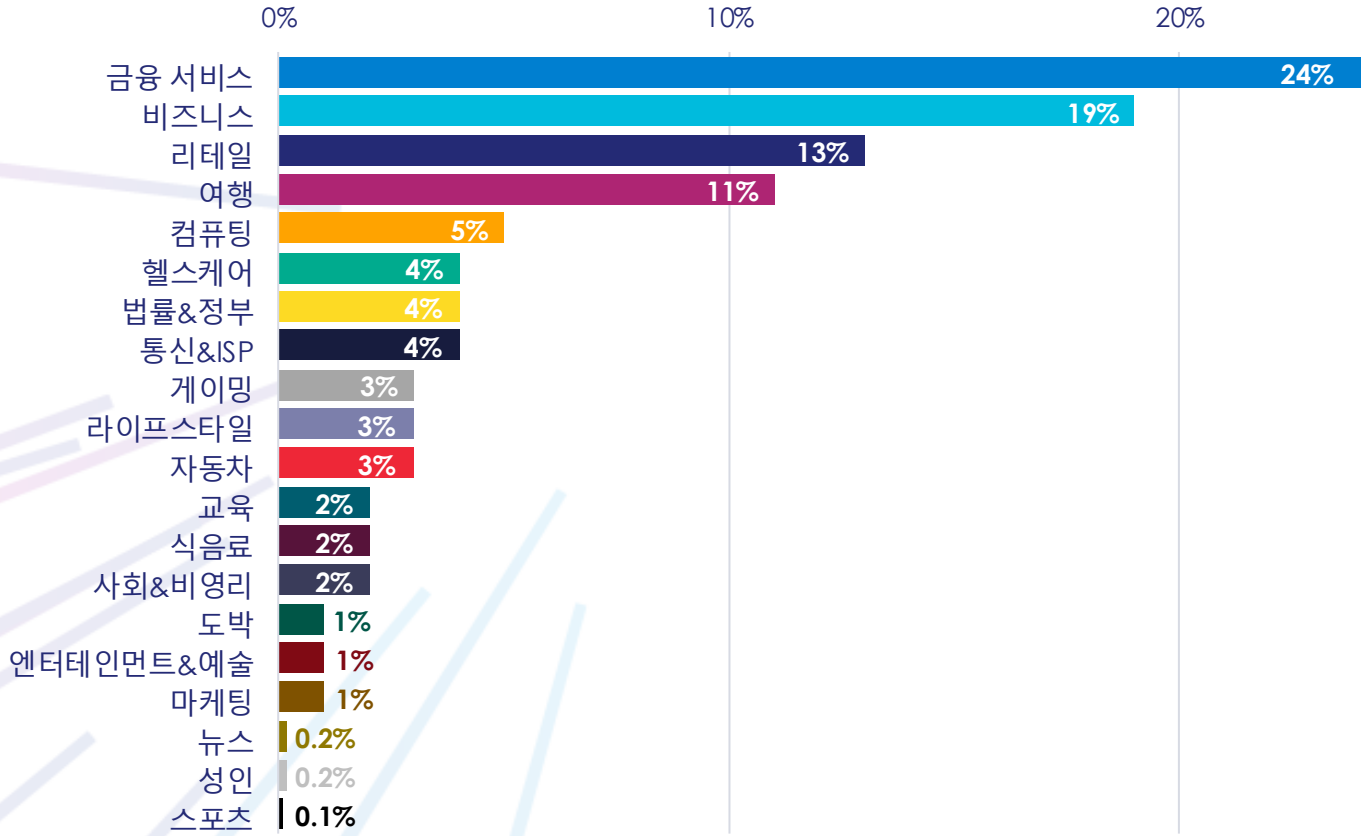
- CHROME
- MOBILE CHROME
- ANDROID BROWSER
- FIREFOX
- MOBILE SAFARI
- OTHER

봇이 휴먼 트래픽과 구별되지 않으면 기존 탐지 방식은 무력화됩니다.

THALES
CYBERSECURITY

#2026악성봇보고서

산업별 악성 봇 현황



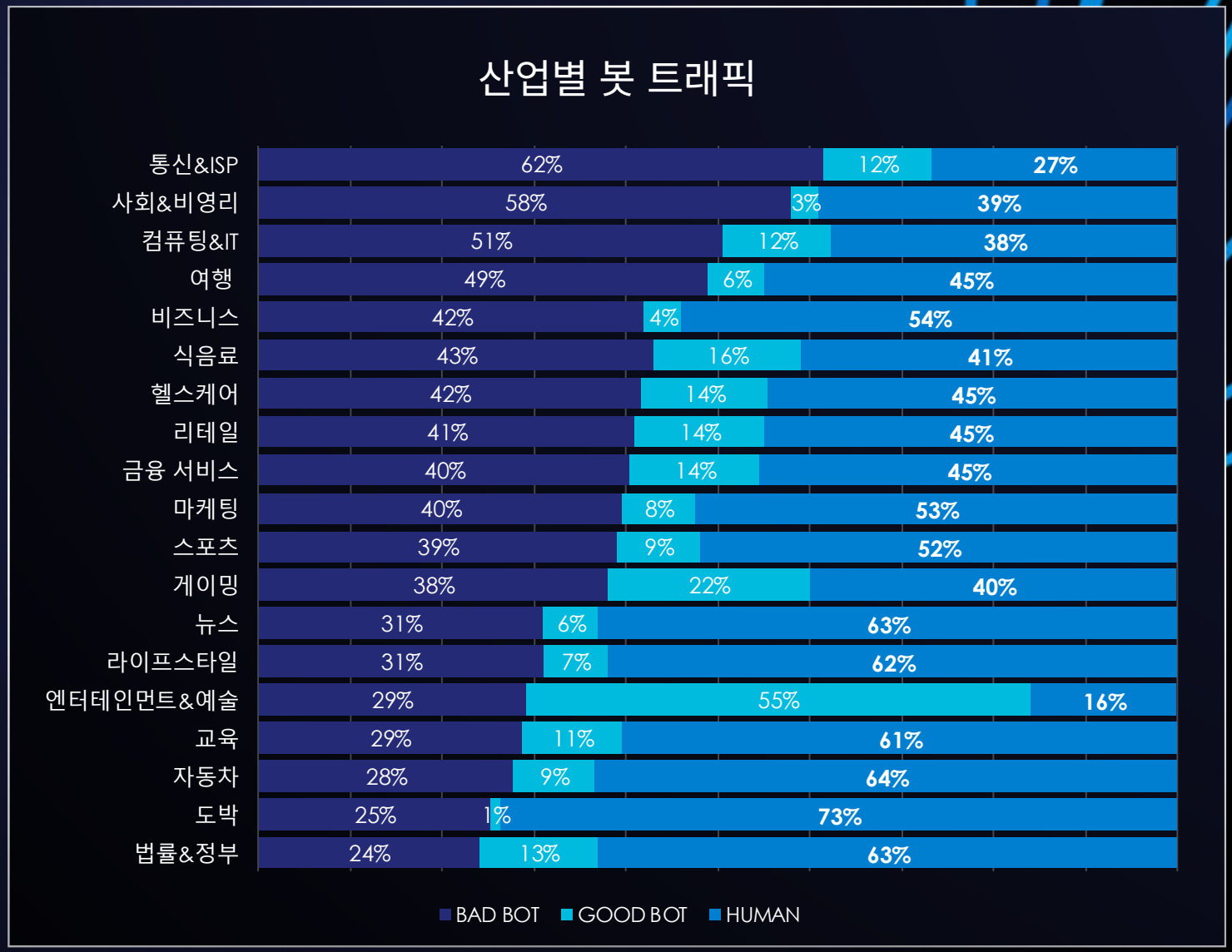
봇은 핵심 금융 운영을 지원하는 동일한 API를 직접 공격합니다.

THALES
CYBERSECURITY

#2026악성봇보고서

산업별 봇 트래픽-(악성/정상/휴먼)

- 통신 및 ISP 사이트 트래픽의 62%가 악성 봇
- 비영리 및 사회단체 사이트 트래픽의 58%가 악성 봇
- 엔터테인먼트 및 예술 사이트 트래픽의 55%가 정상 봇

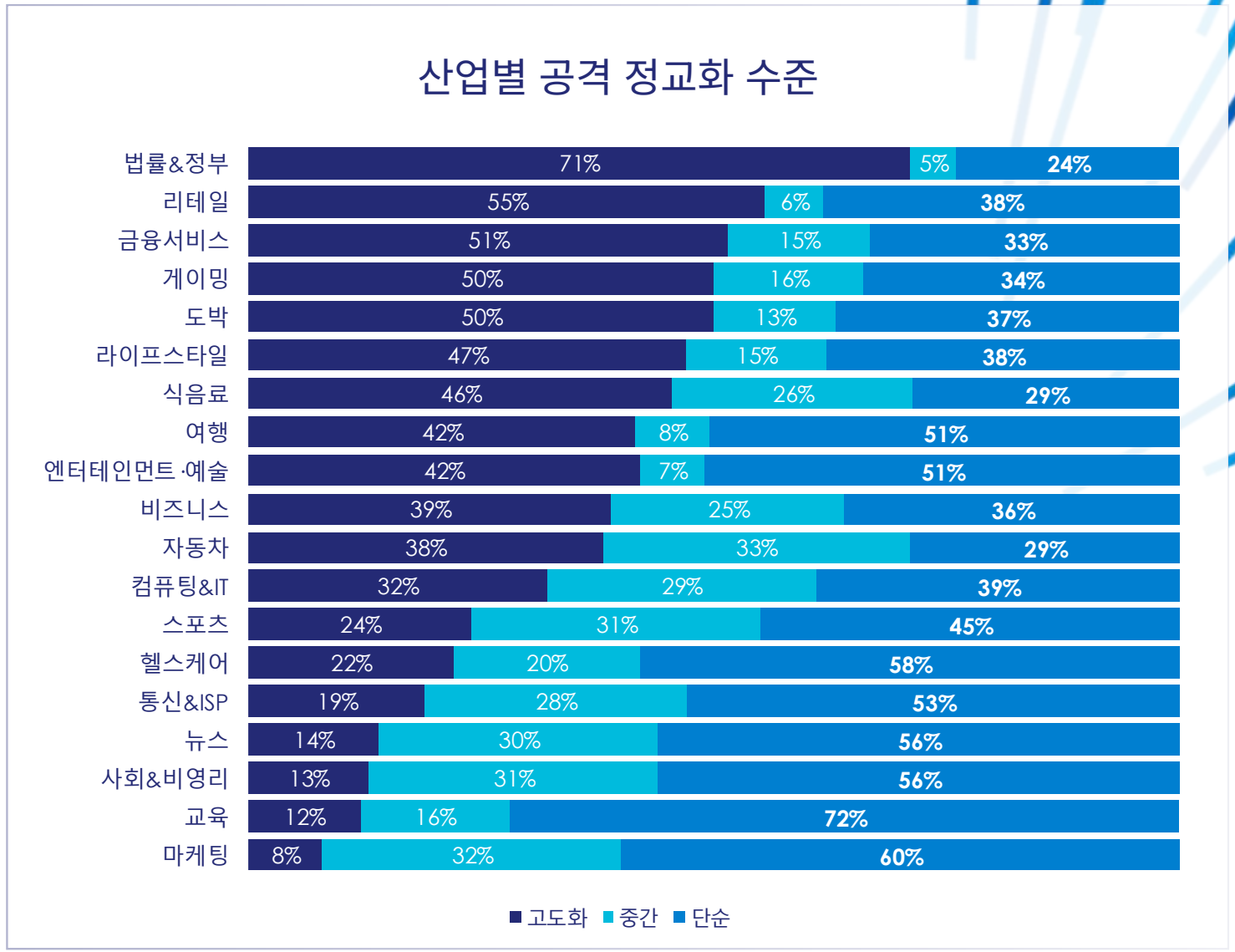


THALES
CYBERSECURITY

#2026악성봇보고서

산업별 공격 정교화 수준

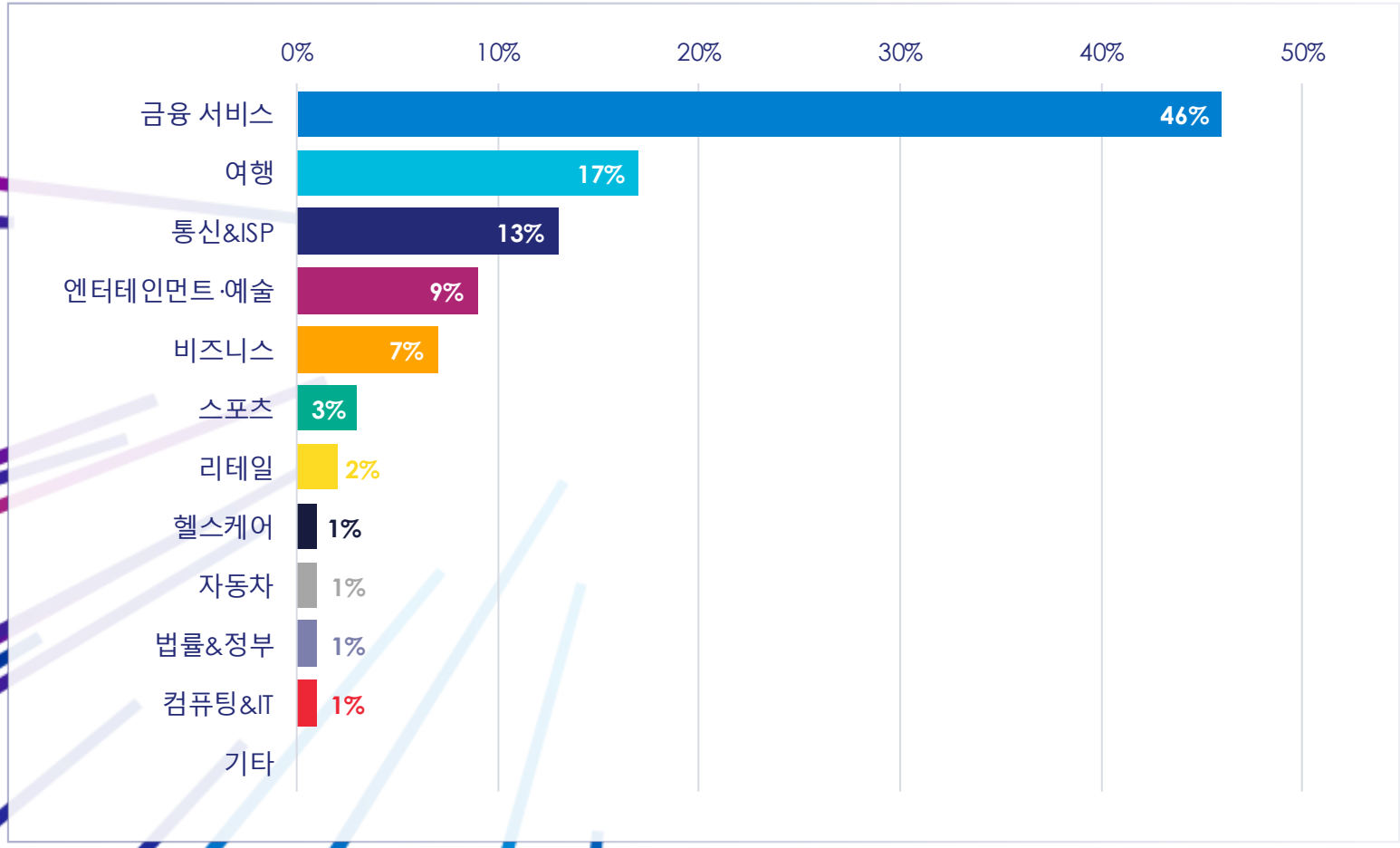
- 법률·정부 사이트 공격의 71%가 고도화된 공격
- 리테일 사이트 공격의 55%가 고도화된 공격
- 교육 사이트 공격의 72%가 단순 봇 공격



THALES
CYBERSECURITY

#2026악성봇보고서

산업별 계정 탈취 공격 대상

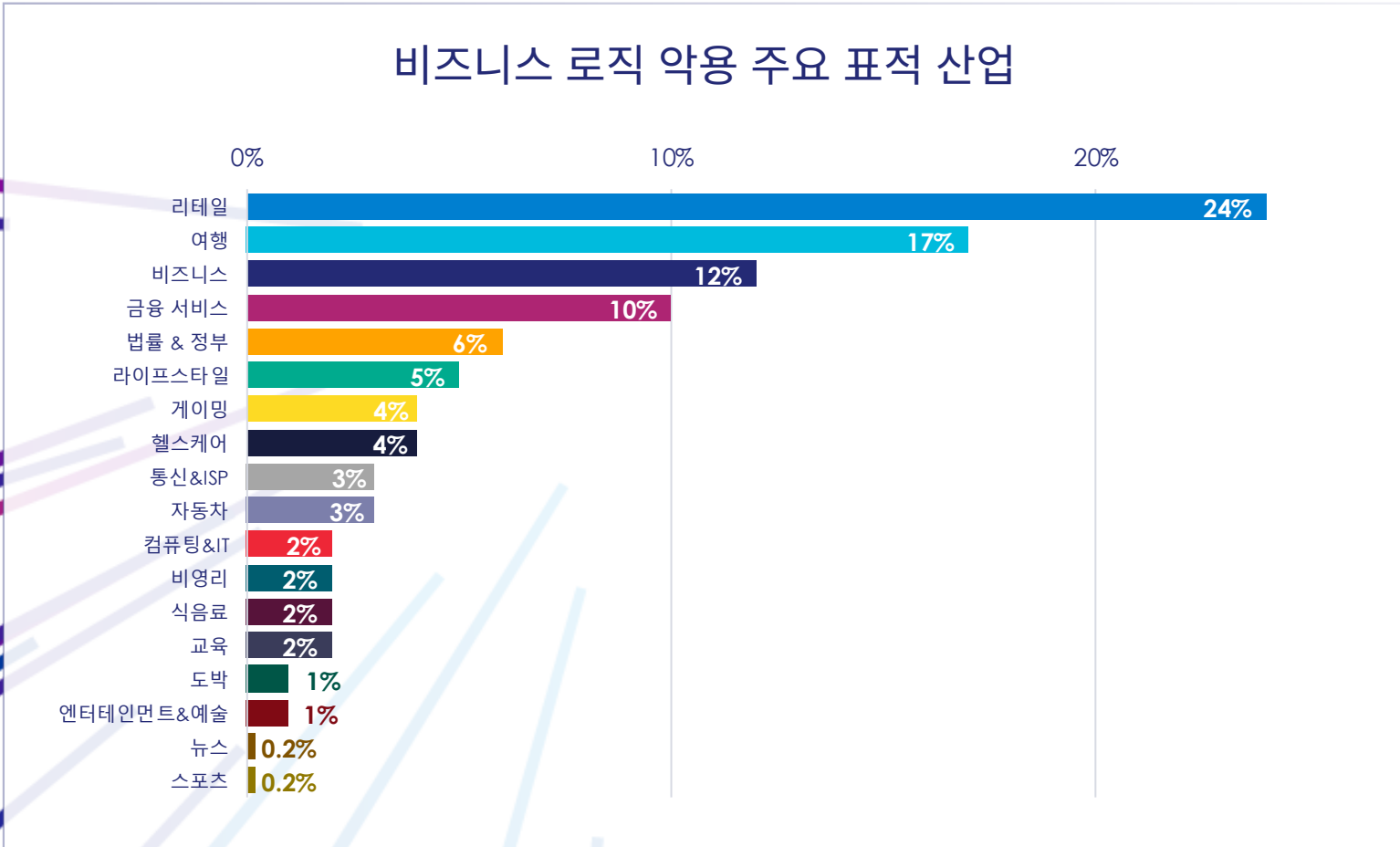


봇은 돈이 있는 곳을 노립니다. - 전체 계정 탈취 공격의 절반에 가까운 수가 금융 서비스를 겨냥합니다.

THALES
CYBERSECURITY

#2026악성봇보고서

비즈니스 로직 악용의 주요 표적 : 리테일·여행



AI 서비스가 도입된 리테일·여행 업계에서 공격자들은 합법적인 AI 에이전트로 위장할 수 있습니다.

.

THALES
CYBERSECURITY

#2026악성봇보고서

문의하기

Name + job title

Phone number

Email

THALES
CYBERSECURITY

감사합니다.

cpl.thalesgroup.com/bad-bot-report

THALES
CYBERSECURITY