imperva

Thales 계열사

2024년

악성 봇 보고서

imperva
Thales 계열사

2024년
악성 봇 보고서

목차

Imperva 악성 봇 보고서에 대하여 03

정의 04

핵심 요약 06

계정 탈취 공격 11

악성 봇 환경 16

- 산업별 악성 봇 트래픽 16
- 산업별 악성 봇의 정교화 21
- 봇 공격의 가장 큰 표적이 되는 산업 22
- 모바일 Chrome 및 Android 브라우저의 인기 상승 23
- 모바일 사용자 에이전트가 봇 트래픽의 거의 절반을 차지 25
- 주거용 프록시의 부상 26
- 모바일 및 주거용 ISP에서 발생하는 악성 봇 트래픽이 상위 자리 차지 26
- 전 세계 악성 봇 27
- 봇 공격의 가장 큰 표적이 된 국가는 미국과 네덜란드였습니다 29

인공지능 시대의 악성 봇 30

권장 사항 33

부록 38

- 악성 봇 사용 사례 38
- 산업별 악성 봇 41

Imperva 위협 연구 42

Imperva 애플리케이션 보안에 대하여 43

악성 봇 보고서

Imperva 악성 봇 보고서의 11번째 연례판에서는 주로 자동화된 봇 공격인 자동화된 인터넷 트래픽의 특성을 살펴보고 조사합니다.

이러한 공격은 날이 갈수록 더욱더 정교해지고 있으며, 기존의 탐지 방법을 우회하여 인터넷에 혼란을 일으키고 있습니다. 이 보고서는 2023년 Imperva 글로벌 네트워크에서 수집된 데이터를 분석하는데, 여기에는 수천 개의 도메인 및 산업에서 익명화된 약 6조 건의 차단된 악성 봇 요청이 포함됩니다.

이 보고서의 목적은 봇의 특성과 영향에 대한 의미 있는 정보를 제공하여 봇 트래픽이 적절하게 관리되지 않을 경우 발생할 수 있는 위험을 조직이 더 잘 이해할 수 있도록 하는 것입니다.

이 보고서는 OSI 모델의 애플리케이션 계층(계층 7)에서의 악성 봇 활동에 초점을 맞춥니다. 이러한 봇 사용 사례는 하위 수준의 네트워크 프로토콜을 조작하는 볼륨형 DDoS 공격과는 완전히 다릅니다.

악성 봇은 정당한 사용자를 모방하는 방식으로 애플리케이션과 상호 작용하므로 탐지 및 차단하기가 더 어렵습니다. 이들은 애플리케이션의 기술적 취약성보다는 애플리케이션의 의도된 기능과 프로세스를 악용하여 비즈니스 로직을 악용합니다. 악성 봇은 웹사이트, 모바일 앱 및 API에서 고속 남용, 오용 및 공격을 용이하게 합니다. 이를 통해 봇 운영자, 공격자, 악의적인 경쟁업체 및 사기범이 악의적인 활동에 참여할 수 있습니다.

웹 스크래핑, 경쟁적 데이터 마이닝, 개인 및 금융 데이터 수집, 무차별 로그인 시도, 스캘핑, 디지털 광고 사기, 서비스 거부 공격, 스팸, 거래 사기 및 기타 유사한 활동은 비즈니스에 해를 끼칠 수 있습니다. 이러한 활동은 대역폭을 소비하고, 서버를 느리게 하며, 민감한 데이터를 훔쳐 회사에 재정적 손실과 평판 훼손을 초래합니다.

정의

04

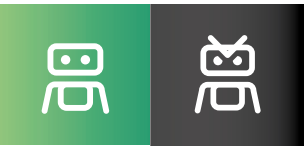
데이터를 깊이 파고들기 전에 이 보고서에서 광범위하게 사용할 주요 용어를 정의해 보겠습니다.

봇이란 무엇입니까?

인터넷의 맥락에서 봇은 자동화된 작업을 실행하는 소프트웨어 애플리케이션을 말합니다. 이러한 작업은 양식 작성과 같은 간단한 작업부터 웹사이트에서 데이터를 스크래핑하는 것과 같은 보다 복잡한 기능에 이르기까지 다양합니다.

악성 봇이란 무엇입니까?

악성 봇은 악의적인 의도로 자동화된 작업을 수행하는 소프트웨어 애플리케이션입니다. 이러한 봇은 허가 없이 웹사이트에서 데이터를 추출하여 재사용하고 경쟁 우위를 확보할 수 있습니다. 이는 종종 스캘핑에 사용되며, 스캘핑은 제한된 수량의 품목을 구매하여 더 높은 가격에 재판매하는 것을 의미합니다. 악성 봇은 애플리케이션을 표적으로 삼는 분산 서비스 거부(DDoS) 공격을 생성하는 데 사용될 수도 있습니다. 일부 악성 봇은 사기나 노골적인 절도와 같은 범죄 활동을 수행합니다. 한 가지 예는 가장 두드러진 봇 공격 유형 중 하나인 자격 증명 스터핑을 수행하는 봇입니다. 오픈 웹 애플리케이션 보안 프로젝트(OWASP)는 자동화된 위협 핸드북[1] 에서 21개의 봇 공격에 대한 포괄적인 목록을 제공합니다.



좋은 봇과 악성 봇의 차이점은 무엇입니까?

인터넷에서 발견된 모든 봇이 모두 악성 봇은 아닙니다. 또한 가치 있는 기능을 제공하는 좋은 봇도 있습니다. 예를 들어, 일부 봇은 검색 엔진에 대해 웹사이트를 인덱스화하거나 웹사이트 성능을 모니터링합니다. Googlebot과 Bingbot은 검색 가능한 웹 페이지 인덱스를 생성하고 유지하는 데 도움이 되는 검색 엔진 크롤러의 예입니다. 이러한 봇은 웹 페이지를 인덱싱함으로써 사람들이 자신의 검색어와 가장 잘 맞는 웹사이트 집합을 찾는 데 도움을 줍니다. 이러한 봇은 온라인 비즈니스에 필수적이며 잠재 고객이 웹사이트, 제품 및 서비스를 쉽게 찾고 액세스할 수 있도록 합니다.

1 https://owasp.org/www-project-automated-threats-to-web-applications/

좋은 봇조차도 우려의 원인이 될 수 있습니다

좋은 봇은 특정 페이지가 실제보다 더 인기 있는 것처럼 보이게 만들 수 있으므로 웹 분석 보고서에 상당한 영향을 미칠 수 있습니다. 예를 들어, 좋은 봇은 귀하가 광고하는 웹사이트의 페이지에 대한 노출을 생성할 수 있지만, 해당 광고 클릭이 판매 유입경로로 이어지지는 않습니다. 이로 인해 광고주의 실적이 저하되고 마케팅 분석이 왜곡되어 결국 잘못된 의사 결정으로 이어질 수 있습니다. 따라서 정보에 입각한 비즈니스 결정을 내리기 위해서는 정당한 인간 사용자, 좋은 봇 및 악성 봇이 생성하는 트래픽을 정확하게 구별하는 것이 중요합니다.

악성 봇 분류

Imperva는 정교함 수준에 따라 악성 봇을 분류하는 다음과 같은 분류 시스템을 만들었습니다.

단순형

ISP가 할당한 단일 IP 주소에서 연결하는 이 봇은 자동화된 스크립트를 사용하여 사이트에 연결합니다. 이 봇은 브라우저로 자체 보고하지 않습니다.

중간

보다 복잡한 이 봇은 JavaScript 실행 기능을 포함하여 브라우저 기술을 시뮬레이션하는 “헤드리스 브라우저” 소프트웨어를 사용합니다.

고급

가장 정교한 봇으로서 마우스의 움직임이나 클릭과 같은 인간 사용자 행동을 에뮬레이션하여 봇 탐지를 스푸핑합니다. 이들은 브라우저 자동화 소프트웨어를 사용하거나, 실제 브라우저에 설치된 맬웨어를 사용해 사이트에 접속합니다.

회피형

정교한 봇 운영자는 매우 결단력 있고 지속적입니다. 오늘 봇 관리 솔루션이 이를 차단하더라도, 이들은 아마도 왜 차단당했는지 알아내고 내일은 감지를 피할 수 있는 새로운 기술을 가지고 돌아올 것입니다. 이러한 공격자들은 회피 기법의 발전으로 인해 탐지하기가 점점 더 어려워지고 있는 고급 악성 봇을 사용하고 있습니다. 이들은 보통 중간 및 고급 악성 봇이 공유하는 다양한 기술을 사용합니다. 따라서 우리는 악성 봇 트래픽 분석에 대한 새로운 관점을 제공하기 위해 중간 수준의 봇과 고급 수준의 봇을 그룹화했습니다.

회피형 봇은 랜덤 IP를 통한 순환, 익명 프록시를 통한 진입, 주거용 프록시 사용, 신원 변경, 인간의 행동 모방, 요청 지연, CAPTCHA 질문 돌파와 같은 복잡한 전술을 사용합니다. 그들은 탐지를 피하고 더 적은 수의 요청으로 중요한 공격을 수행하기 위해 "낮고 느린" 접근 방식을 사용합니다. 이 방법은 많은 악성 봇 캠페인에서 발생하는 “노이즈”를 줄여 감지하기 어렵게 만듭니다.

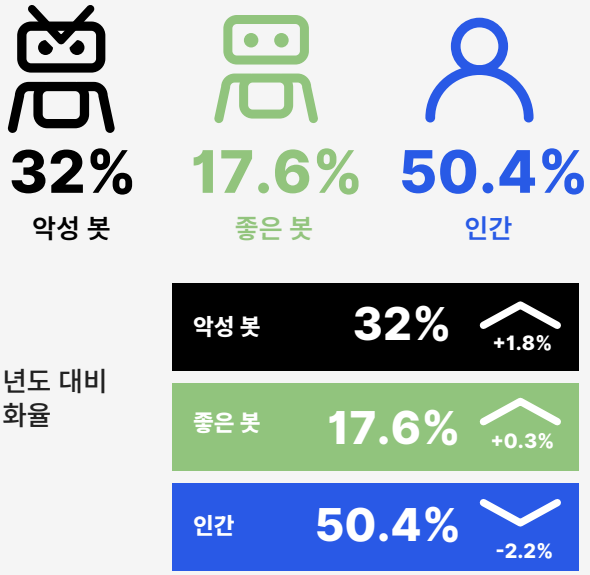
핵심 요약

06

악성 봇 트래픽 수준이 계속 상승하고 있음

악성 봇 트래픽 수준은 5년 연속 증가하여 우려스러운 추세를 보였습니다. 이러한 증가는 부분적으로 인공 지능(AI)과 대규모 학습 모델(LLM)의 인기가 높아졌기 때문입니다. 2023년에 악성 봇은 전체 인터넷 트래픽의 **32%**를 차지했으며, 이는 2022년 대비 **1.8%** 증가한 수치입니다. 좋은 봇 트래픽의 비중도 2022년 모든 의도 트래픽의 **17.3%**에서 2023년 **17.6%**로 증가했지만, 그 정도는 다소 약했습니다. 2023년 전체 인터넷 트래픽 중 합쳐서 **49.6%**는 인간이 아닌 트래픽이었고, 인간 트래픽 수준은 전체 트래픽의 **50.4%**로 감소했습니다.

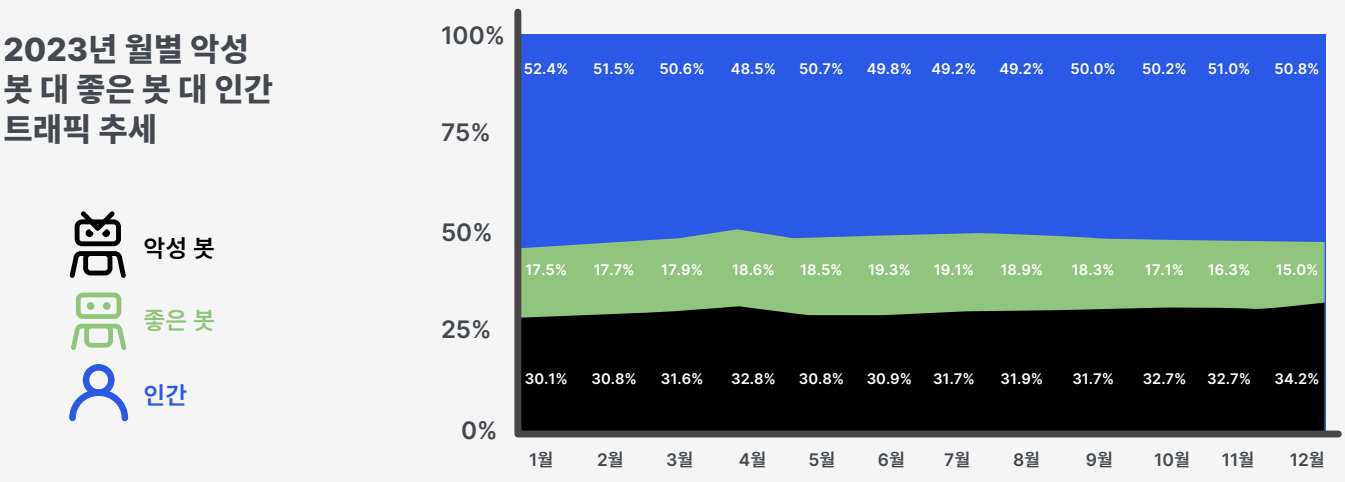
2023년 악성 봇 대 좋은 봇 대 인간 트래픽



월간 악성 봇 트래픽 수준

아래 차트는 인터넷 트래픽 프로필의 월별 추세 분석을 보여줍니다. 흥미로운 점은, 자동화된 트래픽이 연간 서로 다른 네 개의 달에서 인간 트래픽을 앞지른 것입니다. 12월에 악성 봇 트래픽이 **34.2%**나 증가한 것은 그 달에 기록된 공격 건수가 증가했고, 휴가 시즌 동안 인간 활동이 약간 줄었기 때문일 수 있습니다.

2023년 월별 악성 봇 대 좋은 봇 대 인간 트래픽 추세

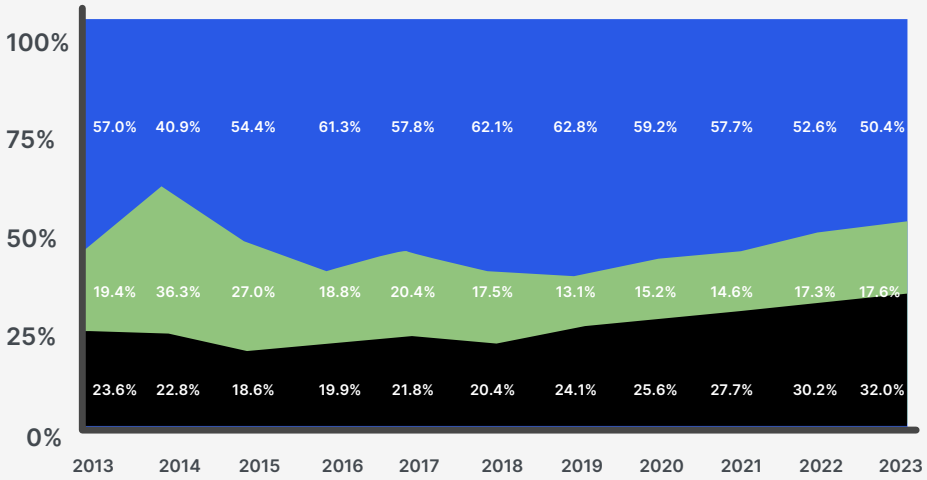


수년간의 악성 봇 트래픽

Imperva는 10년 이상 악성 봇과의 싸움을 주도해 왔습니다. 아래 차트는 지난 11년간의 좋은 봇과 악성 봇 및 인간 트래픽의 추세를 보여줍니다.

2013년에 인터넷 트래픽은 악성 봇이 **23.6%**, 좋은 봇이 **19.4%**, 인간 트래픽이 **57%**를 차지했습니다. 특히 2014년에는 좋은 봇 트래픽이 **20.98%**에서 **36.32%**로 크게 증가했는데, 이는 검색 엔진의 보다 공격적인 인덱싱의 영향으로 추정됩니다. 2015년에는 특히 중국, 인도, 인도네시아의 신규 사용자가 급증함에 따라 인간 트래픽이 **54.4%**에 도달하면서 악성 봇 트래픽이 감소하여 역대 최저치를 기록했습니다. 또한 2016년과 2018년에는 악성 봇 활동이 각각 **19.9%**와 **20.4%**로 감소했습니다. 그러나 2019년부터 2023년까지 악성 봇 트래픽은 꾸준히 증가하여 2023년에는 전체 인터넷 트래픽의 **32.0%**에 도달했으며, 이는 역대 최고 수준입니다.

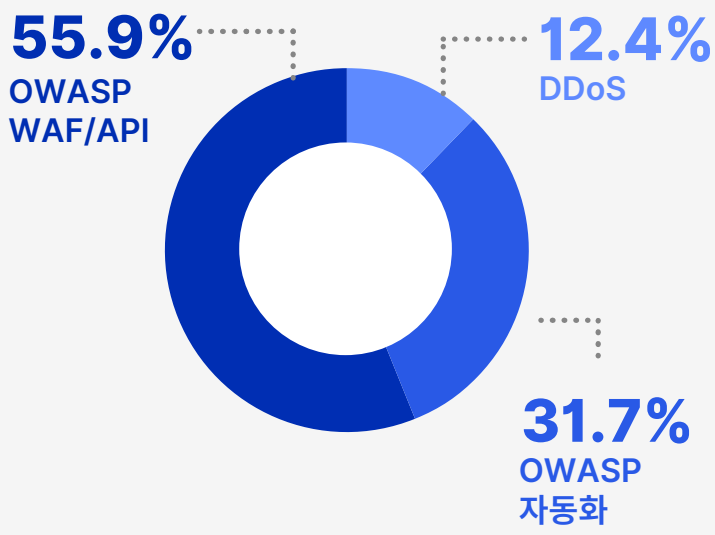
2013~2023년 악성 봇 대 좋은 봇 대 인간 트래픽 추세



OWASP 자동화 위협은 모든 공격의 거의 3분의 1을 차지합니다

지난 해 Imperva에 의해 기록되고 완화된 모든 공격 중 31.7%는 OWASP에서 정의한 자동화된 위협이었습니다. 공격 유형을 자세히 살펴보면 완화된 공격 중 **25%**가 비즈니스 로직을 악용하려는 정교한 악성 봇인 것으로 나타났습니다.

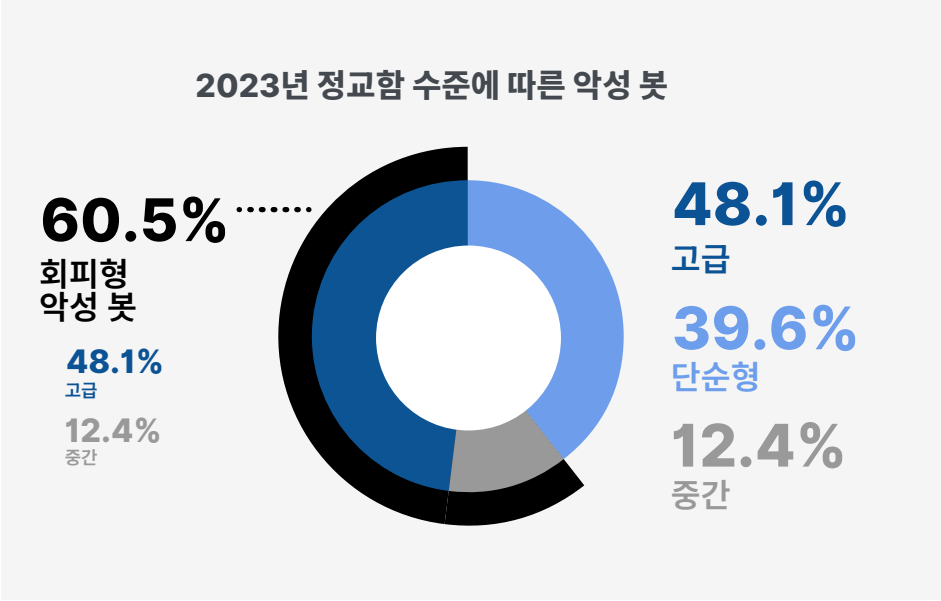
2023년 카테고리별 완화된 공격



중간 수준의 악성 봇은 멸종될까요?

AI 기술의 채택이 증가함에 따라 인터넷 상의 악성 봇의 양과 그 정교함 수준도 영향을 받습니다. 이는 고급 악성 봇을 배포할 수단과 리소스를 갖춘 정교한 공격자와, AI 쿼리와 같은 기본 도구로 봇 스크립트를 생성하는 공격자 간에 뚜렷한 구분을 만들었습니다. 결과는? 2023년에는 간단한 악성 봇이 증가하는 것을 볼 수 있는데, 이는 악성 봇 트래픽의 **39.6%**를 차지하며, 2022년의 **33.4%** 및 5년 전의 **26.3%**에 비해 증가한 수치입니다. 두 번째 흥미로운 추세는 중간 수준의 악성 봇의 인기가 2022년 **15.3%**에서 2023년 **12.4%**로 감소했다는 것입니다. 이러한 추세가 계속되면 이러한 특정 유형 봇의 유행이 점차 감소하는 모습을 볼 수 있을 것입니다.

고급 봇은 2022년 악성 봇 트래픽의 **51.2%**에서 2023년 **48.1%**로 증가했습니다. 이러한 변화로 인해 회피형 악성 봇(보통과 고급 봇 트래픽 수준의 조합)이 모든 악성 봇 트래픽의 **60.5%**를 차지하게 되었습니다. 이는 전년**(66.6%)**보다 감소한 수치입니다. 악성 봇 트래픽은 여전히 매우 정교하고, 날로 새로운 기술이 발전하고 새로운 회피 기술이 도입되고 있습니다.



API는 봇 공격의 가장 인기 있는 벡터입니다

지난 한 해 동안 자동화된 위협으로 인해 API 공격의 **30%**가 발생했습니다. 그중 **17%**는 비즈니스 로직의 취약점을 악용하는 악성 봇이었고, **13%**는 다른 유형의 자동화된 위협이었습니다. 비즈니스 로직 공격은 애플리케이션의 설계 및 구현 내에서 결함을 악용하여 공격자가 정당한 기능을 조작하고 잠재적으로 민감한 데이터 또는 사용자 계정에 액세스할 수 있도록 합니다.

다양한 애플리케이션과 서비스 간의 원활한 통신을 위한 API의 사용이 증가하면서 API는 소프트웨어 개발의 중요한 요소가 되고 있습니다. API는 기계가 읽을 수 있는 특성을 가지고 있기 때문에 악성 봇 공격에 점점 더 취약해지고 있으며, API 트래픽에 대한 가시성이 부족하여 이를 감지하기란 어렵습니다. 그러나 API가 널리 사용되면서 악성 봇의 매력적인 표적이 되기도 했습니다. 악성 봇은 API를 악용하는데, API는 종종 민감한 데이터에 대한 직접적인 경로로 사용되므로 비즈니스 로직 남용 및 사기에 취약합니다. API는 공격 표면을 증가시켜 자동화된 공격에 더 많은 진입점을 제공합니다. 조직들은 API에 계속 크게 의존하고 있기 때문에 이러한 정교한 위협으로부터 보호하기 위해 강력한 보안 조치를 구현하는 것이 필수적입니다.

악성 봇 문제는 산업 간, 기능 간의 문제입니다

악성 봇은 다양한 산업과 조직 기능에 심각한 위협을 가합니다. 이들은 인간의 능력을 초월하는 속도와 규모로 악의적인 활동을 수행할 수 있으므로 남용, 오용 및 공격을 위한 도구로 선호됩니다.

콘텐츠 스크래핑 및 계정 탈취와 같은 일부 악성 봇 사용 사례는 산업 전반에서 흔히 볼 수 있지만, 스캘핑과 같은 다른 사례는 일반적으로 온라인 리테일 및 엔터테인먼트(티켓팅)와 같은 특정 부문에 영향을 미칩니다. 항공사와 같은 일부 산업에는 '좌석 스피닝' 공격과 같은 고유한 사용 사례가 있습니다(자세한 내용은 "산업별 악성 봇 트래픽" 섹션 참조).

2023년 업계별 악성 봇 트래픽의 가장 큰 점유율

게임	57.2%
통신 및 ISP	49.3%
컴퓨팅 및 IT	45.9%
여행	44.5%
커뮤니티 및 사회	42.2%

2023년 산업별 고급 악성 봇 트래픽 최대 점유율

법률 및 정부	75.8%
엔터테인먼트	70.8%
금융 서비스	67.1%
여행	60.9%
게임	52.3%

주거용 프록시는 고급 봇 운영자가 보유한 최신 무기입니다

주거용 프록시에서 발생한 악성 봇 트래픽은 전체 악성 봇 트래픽의 4분의 1을 차지했습니다. 주거용 프록시를 사용하면 봇 운영자가 트래픽 출처를 합법적이고 ISP에서 할당한 주거용 IP 주소인 것처럼 보이게 만들어 감지를 피할 수 있습니다. 그렇게 하면 웹사이트와 온라인 플랫폼에서 정당한 사용자 상호 작용과 악성 봇 동작을 구별하기가 더 어려워집니다.

악성 봇 운영자 사이에서 모바일 브라우저의 인기는 계속 증가하고 있습니다. 2023년에는 악성 봇의 **44.8%**가 모바일 브라우저로 위장하여 탐지를 회피하려고 시도했습니다. 모바일 ISP도 여전히 인기를 끌고 있으며, 공격의 **18.3%**를 차지하고 있습니다.

모바일 사용자 에이전트로 보고된 악성 봇 (모바일 Safari, 모바일 Chrome 등)	44.8%
주거용 ISP에서 시작된 악성 봇	25.8%
모바일 ISP에서 시작된 악성 봇	18.3%

전 세계 악성 봇

미국은 수년 간의 공격 감소 이후 작년에 공격 건수가 증가하여 전 세계 전체 봇 공격의 **47%**를 차지했는데, 이는 2022년 **41.8%**에서 증가한 수치입니다. 올해 상위 5위에 새롭게 진입한 네덜란드는 호주를 제치고 2위를 차지했으며, 네덜란드를 타겟으로 한 봇 공격이 전체의 **9%**를 차지했습니다. 호주는 3위로 떨어졌으며, 공격의 **8.4%**를 차지하고 전년 대비 **16.4%** 감소한 수치로 예년과 비슷한 수준입니다.

상위 5위
가장 많이 타겟팅된 악성 봇별 국가

미국	47%
네덜란드	9%
호주	8.4%
영국	5.1%
프랑스	3.1%

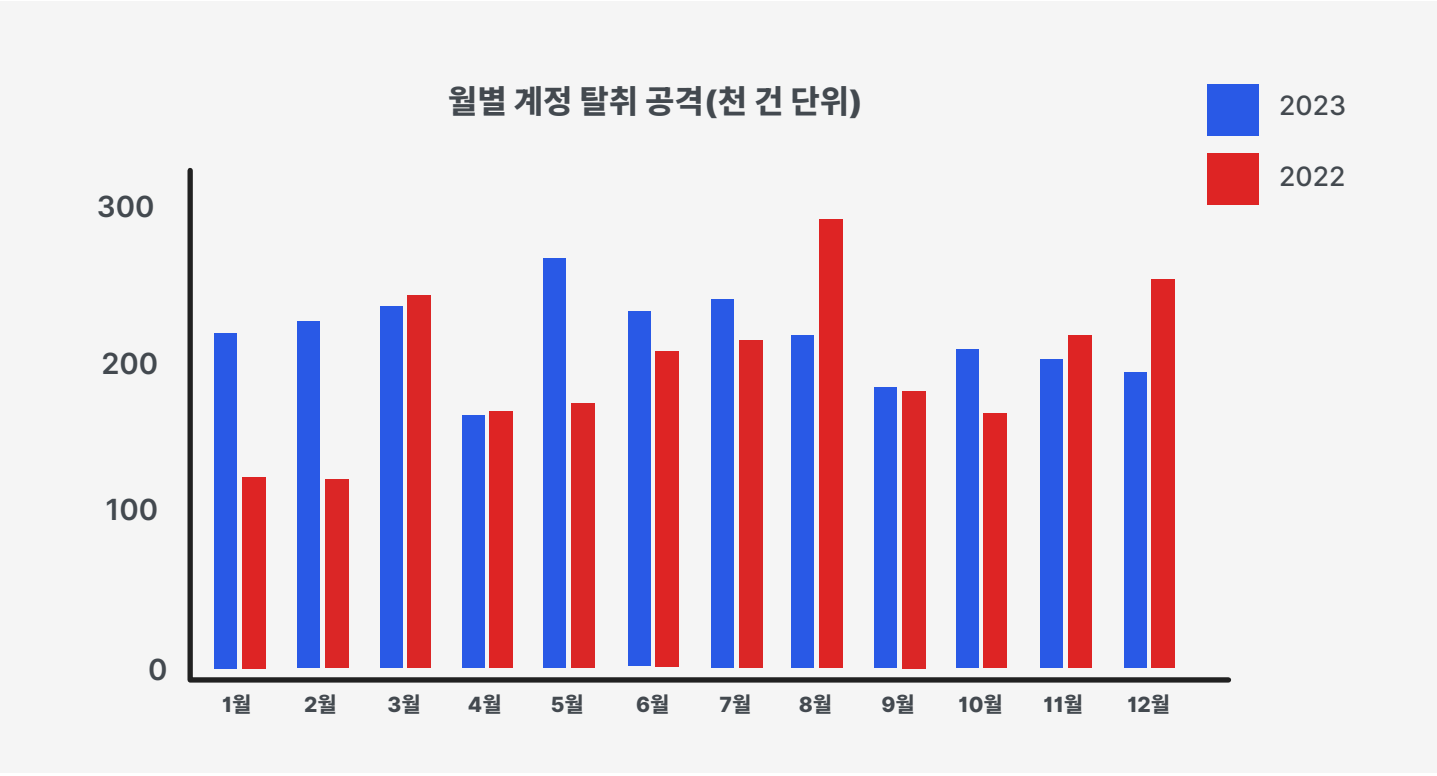
계정 탈취 공격

11

계정 탈취(ATO) 공격은 가장 흔한 자동화된 위협 중 하나입니다. 이러한 공격에는 봇을 사용한 자격 증명 스터핑 및 자격 증명 크래킹 기술을 통해 사용자 계정에 대한 무단 액세스 및 탈취를 시도하는 것이 포함되며, 이로 인해 디지털 신원이 도용되고 조직에 상당한 손실이 발생합니다. Aite Group[2] 에 따르면 신원 도용으로 인한 손실은 2023년에 6,354억 달러에 달할 것으로 추정됩니다.

다음 차트는 지난 2년 동안 Imperva가 기록한 월별 ATO 공격을 나타냅니다. 2022년과 2023년 사이에 **공격이** 10% 증가했습니다. 공격 횟수는 계속 증가하고 있지만, 1월과 2월에 각각 **77%**와 **86%**의 큰 폭으로 증가했음에도 불구하고 그 증가 폭은 예년에 비해 크지 않습니다. 또한 5월과 10월에는 2022년 대비 공격이 증가했습니다**(각각 56%, 25%)**. 2023년은 공격 횟수가 더 적은 해로 마무리되었습니다.

2022년 8월에는 지난 2년 동안 가장 많은 공격이 발생했습니다. 이러한 증가는 작년 보고서에서 다룬 바와 같이 전 세계 데이터 침해가 당시 **70%** 증가했기 때문일 가능성이 높습니다.



2 https://aite-novarica.com/us-identity-theft-stark-reality#:~:text=Aite%20Group%20projects%20that%20losses%20from%20all%20identity,it%20from%20a%20simple%20fraudulent%20credit%20card%20transaction.

ATO 공격의 거의 절반이 API를 직접 타겟으로 삼음

API를 타겟으로 하는 계정 탈취 공격은 Imperva가 기록한 전체 ATO 공격의 44%를 차지했으며, 이는 **작년의** 35%에 비해 크게 증가한 수치입니다. 모바일 및 웹 애플리케이션의 확산으로 인해 API가 널리 채택되면서, 사용자 계정을 침해하려는 공격자에게 매력적인 진입점이 되었습니다. 이러한 API는 중요한 신원 확인 프로세스를 처리하므로 아주 좋은 타겟이 됩니다. 그러나 최신 IT 환경의 복잡성과 온라인 플랫폼의 상호 연결된 특성으로 인해 보안 조치를 구현하기가 어렵습니다. 그 결과, 사이버 범죄자들은 인증 API의 취약점을 악용하여 사용자 계정에 무단으로 액세스합니다. 이들은 자격 증명 스터핑, 무차별 공격 또는 API 남용과 같은 기법을 사용합니다. 인증 API를 타겟으로 하는 계정 탈취 공격의 빈도가 증가함에 따라, 조직에서는 API 보안 조치를 강화하고 오늘날의 가장 정교한 자동화 공격으로부터 보호해야 할 필요성이 강조되고 있습니다.

숫자로 본 계정 탈취 공격

10% 2022년과 2023년 사이 계정 탈취 공격 증가

11% 모든 로그인 중 계정 탈취 시도 비율

44% API를 타겟으로 한 계정 탈취 공격의 비율

모든 로그인 중 ATO 비율이 가장 높은 산업

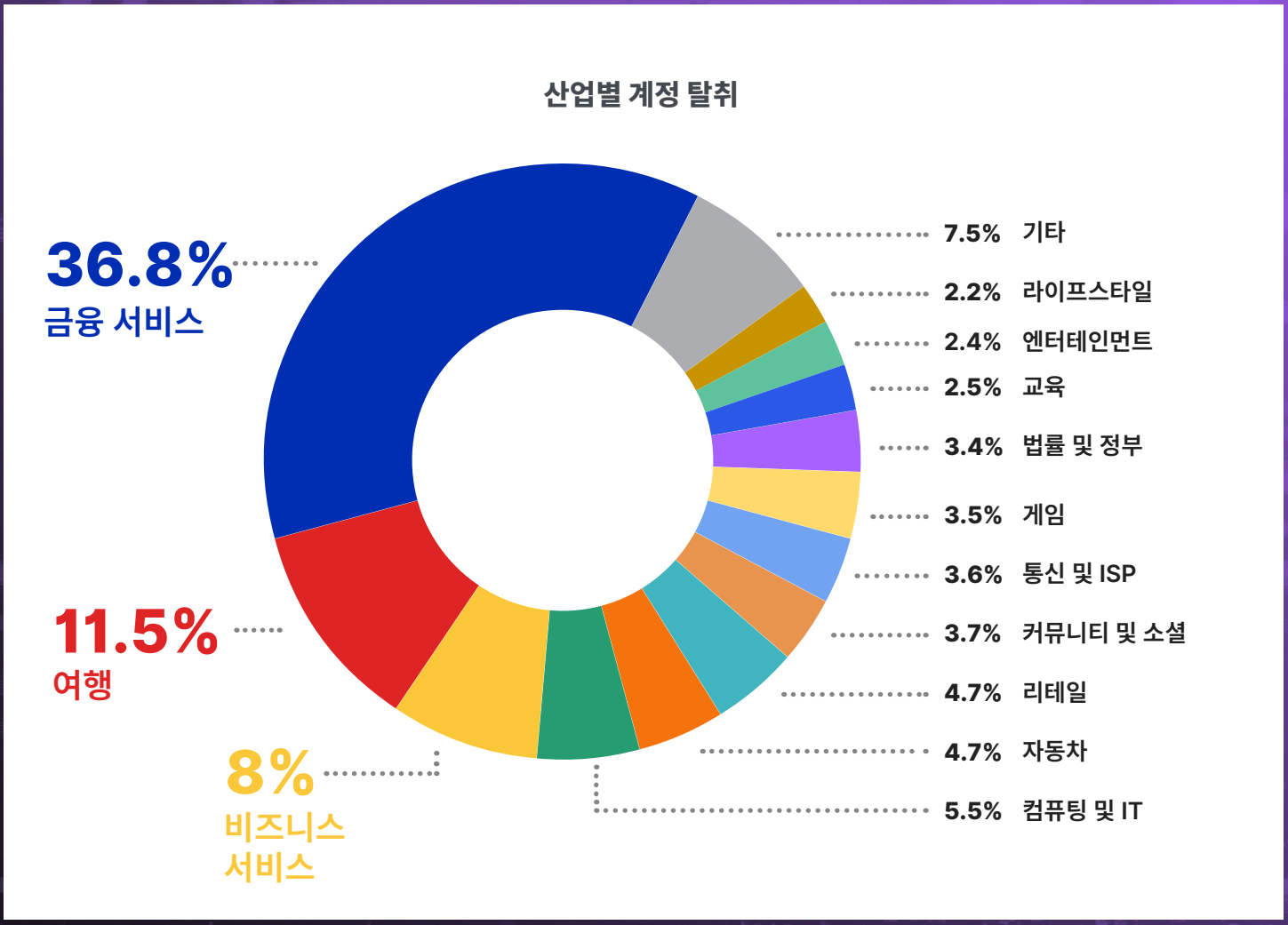
비즈니스 서비스	38%
스포츠	35%
음식 및 식료품	33%
컴퓨팅 및 IT	24%
의료	18%
여행	17%

ATO 공격의 가장 타겟이 되는 국가

미국	40%
영국	7%
독일	7%
호주	5%
스페인	5%
태국	4%

가장 많이 공격을 받는 산업

모든 로그인 중 악성 로그인 비율이 가장 높은 산업과는 달리, 다음 차트는 2023년에 어떤 산업이 가장 많은 양의 ATO 공격을 경험했는지 보여줍니다. 사용자 계정의 인센티브를 감안하면, 작년과 마찬가지로 금융 서비스가 가장 많이 타겟이 되어 모든 공격 중 **36.8%**를 차지한 것은 놀라운 일이 아닙니다. 여행 산업이 2위**(11.5%)였으며**, 그 다음으로 비즈니스 서비스**(8%)**, 컴퓨팅 및 IT**(5.5%)**, 자동차**(4.7%)**, 리테일**(4.7%) 순**이었습니다.



계정 탈취에 대한 보호가 없는 경우의 비용

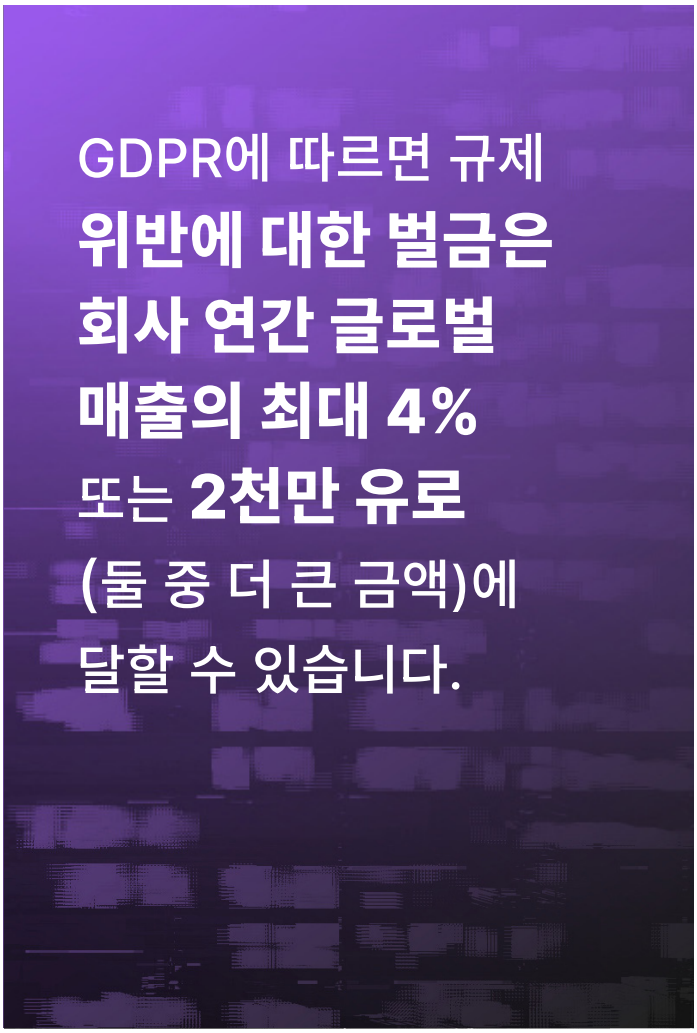
로그인 페이지가 있는 경우 계정 탈취 공격의 대상이 될 가능성이 높습니다. 사용자 계정에 귀중한 정보나 재정적 인센티브가 첨부되어 있는 경우 가능성이 더 높아집니다. 그럼에도 불구하고 많은 조직이 ATO 공격을 사전에 예방하는 데 어려움을 겪고 있으며, 이로 인한 비용은 엄청날 수 있습니다. 예를 들어, 유럽 연합(EU)에서 비즈니스를 수행하는 웹사이트에 대한 ATO 공격이라는 가상 시나리오를 생각해 보겠습니다. 잠재적 피해액은 수백 만 달러로 급증할 수 있습니다.

GDPR에 따르면 규제 위반에 대한 벌금은 회사 연간 글로벌 매출의 최대 **4%** 또는 2천만 유로(둘 중 더 큰 금액)에 달할 수 있습니다. 연간 글로벌 매출액이 1억 달러인 기업의 경우, 최대 벌금은 4백만 달러에 달할 수 있습니다.

하지만 그 비용은 거기서 끝나지 않습니다. 침해 피해자가 집단 소송을 제기할 경우, 피해 고객 10,000명에 대해 고객당 평균 500달러의 손해배상 청구가 발생한다면 총 잠재적 손해액은 5백만 달러에 달할 수 있습니다.

평판 손상은 정량화하기 어려운 또 다른 중요한 비용입니다. 고객 신뢰 상실은 매출 감소 및 주식 가치 하락으로 이어질 수 있습니다. 연간 글로벌 매출액이 1억 달러인 회사의 다음 해 매출액이 **10%** 감소하면 손실액은 별도로 1천만 달러에 달할 수 있습니다. 시가총액이 2억 달러인 회사의 주식 가치가 **5%** 하락하면 1천만 달러의 손실에 해당합니다.

마지막으로, 통지 비용, 법률 및 컨설팅 수수료, 보안 조치 강화, 영향을 받는 고객에 대한 신용 모니터링 서비스와 같은 추가 비용을 고려해야 합니다. 이로 인해 250만 달러까지 더 추가될 수 있습니다.



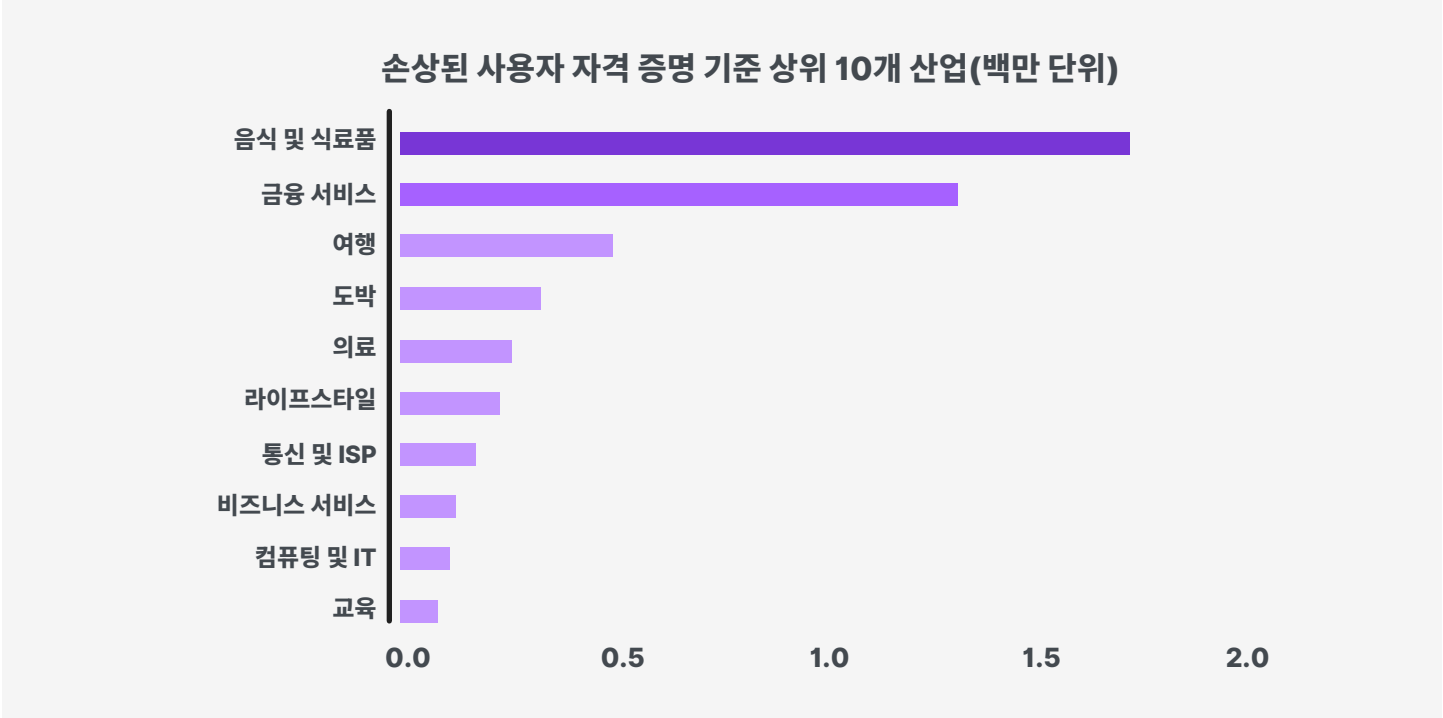
패스키는 계정 탈취 공격의 확산에 어떤 영향을 미칠까요?

패스키[3,4]의 도입은 온라인 사용자 경험을 개선하고 계정 탈취 사기의 위험을 줄이는 것을 목표로 합니다. 패스키는 비밀번호보다 편리하고 안전한 대안입니다. 이러한 솔루션은 모든 주요 플랫폼과 브라우저에서 작동하며, 사용자는 지문, 얼굴 인식 또는 로컬 PIN으로 컴퓨터 또는 모바일 장치의 잠금을 해제하여 로그인할 수 있습니다. 이를 통해 기존 비밀번호로 인한 사용자의 부담을 덜어 주며, 여러 계정에 대한 강력한 비밀번호를 선택하고 기억해야 하는 문제를 완화합니다.

인증 프로세스에 패스키를 통합함으로써 조직은 계정의 취약성을 줄여 계정 탈취 시도를 예방하고 보안 태세를 강화하여 사용자 정보를 보호할 수 있습니다. 그러나, 다양한 온라인 플랫폼 및 서비스에 걸쳐 패스키를 광범위하게 채택하는 것은 패스키의 효과를 높이는 데 필수적입니다. 조직에서는 인증 프로세스에 패스키 시스템을 구현하고 통합하기 위한 공동의 노력이 필요합니다. 더 많은 조직이 이 기술을 채택함에 따라, 계정 탈취 공격의 확산에 미치는 영향을 살펴보는 것도 흥미로울 것입니다. 공격 건수 증가세가 둔화되고 있다는 초기 징후가 있지만 아직 확실한 결론을 내리기에는 아직 이릅니다. 한 가지 분명한 것은 현재 보안 상태에서 계정 탈취는 여전히 조직과 최종 사용자에게 심각한 위협이 되고 있다는 점입니다. 잠재적 공격으로부터 보호하기 위해서는 경계와 사전 예방적인 조치가 매우 중요합니다.

손상된 사용자 계정

온라인 데이터 침해로 인해 손상된 사용자 계정을 탐지하면 조직이 보안 조치를 강화하고 임박한 계정 탈취 공격을 방지하는 데 도움이 될 수 있습니다. 아래 차트는 Imperva가 가장 많이 유출된 계정을 식별하고 경고한 상위 10개 산업을 보여줍니다.

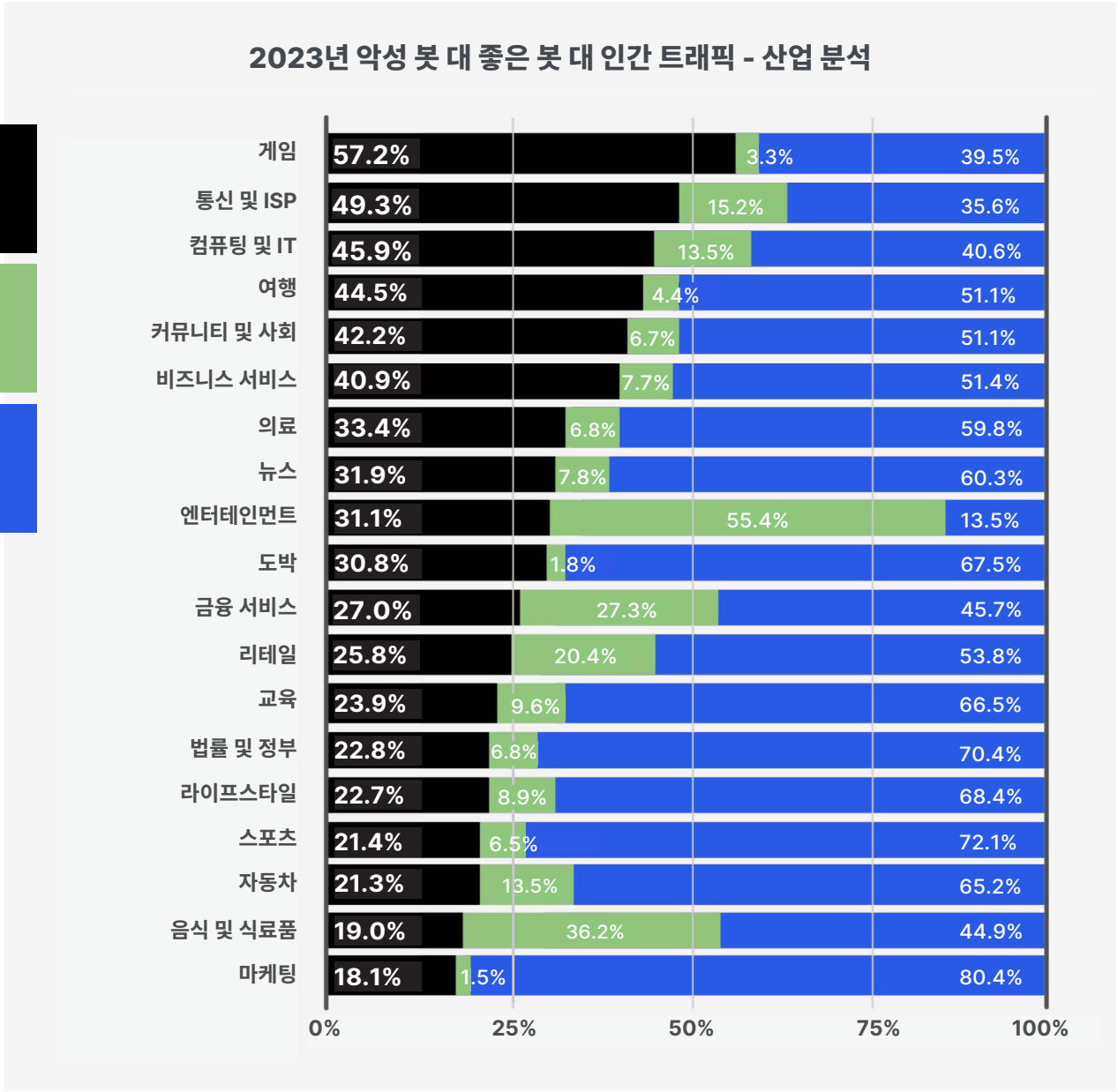


3 https://fidoalliance.org/passkeys/
4 https://developers.google.com/identity/passkeys

악성 봇 환경

산업별 악성 봇 트래픽

각 부문마다 다른 악성 봇 문제가 존재합니다. 다음 차트는 2023년에 Imperva가 산업별 분석 보기에서 기록한 트래픽 프로필을 나타내며, 전반적인 악성 봇 트래픽 수준의 증가가 각 산업에 어떤 영향을 미쳤는지 자세히 살펴봅니다.



게임 및 비디오 게임 웹사이트는 올해의 악성 봇 보고서에서 다시 최상위에 올랐습니다. 작년과 유사하게**(58.7%)**, 게임 사이트의 트래픽 중 상당 비율**(57.2%)**이 악성 봇에 의해 생성됩니다. 봇은 사용자 계정을 탈취하고, 혜택을 악용하기 위해 가짜 계정을 만들고, 부정행위를 하는 등 문제를 일으킬 수 있습니다. 게임과 고속 상호 작용을 수행하여 인간 플레이어를 이긴다거나, 가상 화폐, 아이템 또는 경험치(XP)를 지속적으로 파밍하는 것과 같이 인간 플레이어에게 어렵거나 불가능한 일을 수행합니다. 이러한 행동으로 인해 실제 인간 플레이어는 결국 이탈하게 되며 이로 인해 활성 플레이어 수와 참여도가 감소하여 수익 손실을 초래합니다.

컴퓨팅 및 IT 산업은 2023년에 악성 봇 트래픽이 증가하여 전체 트래픽의 **45.9%**를 차지했으며, 이는 전년도 수준인 **40%보다 높습니다.** 악성 봇은 업계에 피해를 끼쳐 기술적 문제, 사기, 보안 위험을 초래합니다. 악성 봇이 이 분야를 표적으로 삼는 가장 흔한 방법 중 하나는 분산 서비스 거부(DDoS) 공격으로, 많은 봇이 웹사이트 서버를 요청으로 가득 채우는 것입니다. 또한 악성 봇은 로그인 자격 증명 및 개인 정보와 같은 민감한 데이터를 스크래핑하여 잠재적인 데이터 침해 및 신원 도용을 초래할 수 있습니다. 또한 공격자는 취약점 스캐닝과 클릭 사기에 봇을 사용하여 지표 왜곡 및 수익 손실을 초래합니다.

통신 및 ISP 부문에서는 악성 봇으로 인한 트래픽이 약간 증가했습니다. 2022년에 악성 봇 트래픽 비율은 **47.7%**였으며, 2023년에는 **49.3%**로 증가했습니다. 이 부문은 모바일 ISP, 주거용 ISP, 호스팅 제공업체 등을 포함합니다. 악성 봇은 민감한 고객 데이터를 스크래핑하고 사용자 계정을 탈취하기 위한 무차별 로그인 공격을 포함하여 악의적인 다양한 활동을 통해 이 산업을 표적으로 삼습니다. 이 산업은 가용성에 크게 의존하고 가동 중단 시간에 민감하기 때문에, 악성 봇이 분산 서비스 거부(DDoS) 캠페인을 실행하여 인프라에 과부하를 일으키고 서비스를 중단시킬 수 있습니다. 이런 봇은 종종 정당한 사용자처럼 위장하기 때문에 진짜 트래픽과 가짜 트래픽을 구별하기 어렵습니다. 또한 봇 트래픽은 웹사이트 분석을 왜곡하여 잘못된 의사 결정을 초래할 수 있습니다.

여행 산업은 몇 년 동안 이어진 어려운 상황에서 완전히 회복되었습니다. 그 어느 때보다 많은 사람들이 여행을 하고 있습니다[5,6]. 안타깝게도 이로 인해 봇의 관심도 커졌으며, 따라서 여행 웹사이트에서는 올해 악성 봇 트래픽이 크게 증가하여 전체 웹 트래픽 중 **37.4%**에서 **44.5%**로 **증가했습니다**. 여행 업계는 악의적인 공격자가 여행 애플리케이션에서 비즈니스 로직이 다양하게 사용되는 방식을 악용할 수 있기 때문에 항상 복잡한 봇 문제로 어려움을 겪었습니다.

여행 부문 내에서는 특히 **항공사**가 표적이 됩니다. 가장 큰 문제는 항공사의 웹사이트, 모바일 앱, API를 포함한 온라인 플랫폼에서 비롯됩니다. 이러한 플랫폼은 고객이 항공편 정보에 액세스하고 구매 결정을 내리며 항공편을 예약하는 곳입니다. 안타깝게도 봇은 이러한 플랫폼을 표적으로 삼아 데이터를 스크래핑하고 서비스를 중단하며 때로는 사기를 저지르는 경우가 많습니다.

항공사들이 직면한 주요 문제는 허가 없이 웹 속성에 액세스하는 많은 수의 스크래핑 봇입니다. 이러한 봇은 온라인 여행사(OTA), 애그리게이터 및 경쟁업체 등 다양한 출처에서 제공됩니다. 대량의 봇이 항공편 정보를 스크래핑할 경우, 예약 대비 조회 비율과 같은 비즈니스 통찰력이 손상되고 제3자 예약 공급업체의 수수료가 증가하는 등 많은 문제가 발생합니다. 작년에 우리는 항공편 정보를 얻기 위해 봇이 항공사의 검색 API를 대량으로 스크래핑한 사례를 공유했습니다. 그 결과 제3자 공급업체의 API 요청에 대해 매월 50만 달러 이상의 비용이 청구되었습니다. 올해 다른 항공사를 겨냥한 유사한 공격이 발생하고 있습니다.

예약 대비 조회 비율이 갑자기 변경되는 것은 봇 트래픽이 항공편 정보를 적극적으로 스크래핑하고 있음을 나타낼 수 있습니다. 이는 많은 항공사에 중요한 문제입니다. 승인된 OTA 및 애그리게이터는 합의된 조건에 따라 데이터를 스크래핑할 수 있지만, 승인되지 않은 OTA 및 애그리게이터는 봇을 사용하여 합의 없이 가격 및 항공편 정보를 스크래핑합니다. 이러한 무단 활동은 항공사의 약관을 위반하고 중요한 비즈니스 지표와 통찰력을 왜곡합니다.

경쟁 항공사 역시 실시간 시장 정보를 수집하기 위해 봇을 활용합니다. 봇은 경쟁사의 가격, 좌석 재고 및 할인 요금을 스크래핑하여 봇 트래픽의 양을 늘리고, 피해 항공사에게는 아무런 가치 있는 목적을 제공하지 않습니다.

가장 피해가 큰 봇 활동은 로열티 보상 프로그램을 손상시키기 위해 봇을 실행하는 범죄자들로부터 발생합니다.

가장 피해가 큰 봇 활동은 로열티 보상 프로그램을 손상시키기 위해 봇을 실행하는 범죄자들로부터 발생합니다. 이러한 봇은 로그인 페이지에서 무차별 대입 자격 증명 스터핑 및 크랙 공격을 실행하여 계정에 액세스하고 로열티 포인트를 훔치며 사기성 구매를 실행합니다.

항공 산업에서만 볼 수 있는 봇의 나쁜 사용 사례 중 하나는 좌석 스피닝입니다. 이 문제는 아시아 태평양 지역에 특히 만연합니다. 좌석 스피닝 봇은 결제 없이도 최대 24시간까지 좌석을 확보해 둡니다. 이러한 봇을 통해 승인되지 않은 OTA 등의 운영자는 투자 없이 예약을 보류하고 재판매할 수 있습니다. 그 영향은 출발 시간이 가까워질수록 가장 두드러지게 나타나는데, 마치 예약이 꽉 찬 듯 보였던 항공편이 갑자기 빈 좌석이 점점 늘어나게 됩니다. 좌석 스피닝은 수익 손실과 항공사의 평판 손상으로 이어집니다.

전반적으로 봇이 항공 산업에 미치는 영향은 광범위합니다. 이러한 행위는 허가받지 않은 스크래핑, 좌석 스피닝 및 사기로 이어집니다. 이러한 활동은 고객 경험을 방해하고 항공사의 명성을 훼손합니다. 이를 방치하면 웹사이트 성능이 저하되고 심지어 다운타임이 발생할 수 있습니다.

5 https://www.washingtonpost.com/climate-environment/2023/11/23/pandemic-flying-normal-emissions/
6 https://www.euronews.com/travel/2023/04/21/post-covid-revenge-travel-has-gone-big-and-the-revenge-is-sweet

커뮤니티 및 사회 웹사이트는 악성 봇 트래픽 중 **42.2%**를 차지했으며, 이는 작년의 **41.4%**에서 약간 증가한 수치입니다. 가장 일반적인 유형의 악성 봇 중 하나는 가짜 뉴스 스팸 및 댓글 스팸으로도 알려진 스팸 봇입니다. 이러한 봇은 가짜 뉴스를 퍼뜨리고, 선전을 증폭시키며, 낚시성 링크 내에 멀웨어와 같은 악성 콘텐츠를 숨깁니다. 이 문제는 웹사이트에서 기부금을 받는 비영리 단체에서도 널리 발생합니다. 봇은 기부 페이지를 악용하여 도난당한 신용카드 번호를 테스트하기 때문에 비영리 단체에 많은 재정적 부담을 줍니다.

의료 부문에서는 악성 봇 트래픽이 증가했는데, 웹사이트 트래픽의 **33.4%**가 악성 봇에서 비롯된 것으로 나타났으며, 이는 전년 대비 **31.7%** 증가한 수치입니다. 의료 부문을 표적으로 하는 악성 봇은 일반적으로 민감한 고객 데이터를 얻는 것을 목표로 하며, 이는 데이터 침해를 초래할 수 있습니다. 또한 이러한 봇은 사용자 계정을 제어하여 의료 기록에 액세스하거나 환자 기록, 병력 및 보험 세부 정보와 같은 기밀 건강 정보를 수집할 수 있습니다. 이러한 도난당한 데이터는 이익을 위해 다크 웹에서 판매되거나 사기 행위에 사용될 수 있습니다. 또한 의료 분야의 악성 봇은 분산 서비스 거부(DDoS) 공격을 통해 시스템에 과부하를 일으켜 위협을 가하고, 이로 인해 환자와 의료 서비스 제공자가 중요한 정보와 서비스에 접근하는 데 어려움을 겪습니다.

금융 서비스에서는 2023년에 악성 봇이 사이트 트래픽의 **27%**를 차지하는 것으로 나타났습니다. 흥미롭게도, 거의 동일한 비율의 트래픽이 좋은 봇에서 발생했습니다. 이는 금융 애그리게이터 및 기타 서비스 제공자가 봇을 사용하여 최종 사용자에게 귀중한 정보와 통찰력을 제공하는 데서 비롯될 수 있습니다. 그러나 악성 봇으로 인해 이 부문은 계정 탈취 공격이라는 중대한 위협에 직면해 있습니다. 악성 봇은 자격 증명 스터핑 또는 자격 증명 크래킹과 같은 무차별적 로그인 기술을 사용하여 사용자 계정에 대한 불법 액세스를 시도합니다. 다른 일반적인 위협으로는 신용카드 사기, 빈번한 이자율 변경과 같은 맞춤형 콘텐츠 도용이 있습니다. 업계를 표적으로 삼는 또 다른 자동화된 위협은 암호화폐 거래소와 NFT 시장을 타겟으로 삼는 차익거래 봇입니다. 이러한 봇은 웹 스크래핑을 사용하여 서로 다른 거래소와 마켓플레이스 간의 가격 불균형을 식별합니다. 이들은 운영자가 한 거래소나 마켓플레이스에서 다른 거래소나 마켓플레이스로 암호화폐와 NFT를 거래하는 데 도움을 주며, 서로 다른 거래소의 동일한 코인이나 코인 쌍 간의 가격 차이를 이용해 수익을 냅니다.

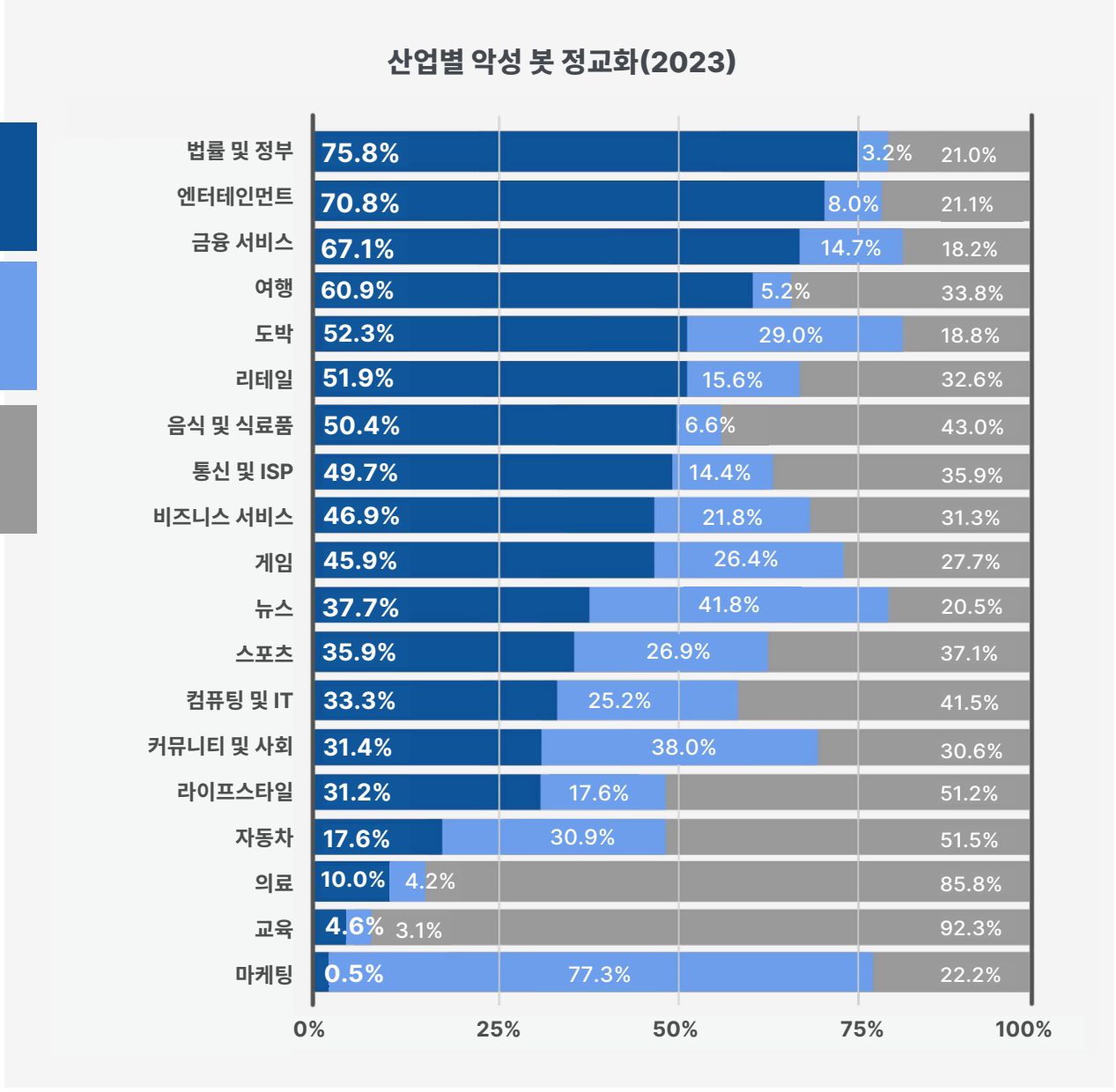
리테일 업계 웹사이트 트래픽의 4분의 1**(25.8%)**이 악성 봇에서 비롯되었습니다. 이는 전년도의 **22.7%**에서 증가한 수치입니다. 작년과 마찬가지로 온라인 리테일 업체도 많은 양의 봇 트래픽 **(20.4%)**을 경험했습니다. 이는 검색 엔진과 웹사이트에서 사용되는 가격 비교 크롤러의 보편화 때문일 가능성이 높습니다. 온라인 리테일 업체는 비즈니스에 부정적인 영향을 미치고 고객 경험과 운영을 방해하는 다양한 형태의 자동화된 위협에 직면합니다. 악성 봇은 경쟁자의 데이터 스크래핑, 고가에 재판매하기 위해 제한된 수량의 품목을 취득(스캘핑), 분산 서비스 거부(DDoS) 공격 수행, 신용카드 해킹, 카딩, 기프트 카드 해킹, 계정 탈취(ATO)와 같은 범죄 활동 등 다양한 악의적 활동에 사용됩니다. 올해 연말연시 기간 동안 계정 탈취(ATO) 공격이 증가했습니다. ATO 공격은 9월부터 증가했으며, 11월 8일, 14일, 24일(블랙 프라이데이)에 공격 활동이 크게 급증했습니다. 블랙 프라이데이에 발생한 공격 건수는 무려 **85%**나 증가했는데, 이는 2022년 블랙 프라이데이에 발생한 ATO 공격이 **66%** 증가한 것과 비교됩니다. 또한 이러한 공격의 강도도 높아지고 있으며, 악의적인 로그인 요청의 수는 10월에서 11월 사이에 **82%**나 급증했습니다.

엔터테인먼트 부문에는 티켓팅 플랫폼, 스트리밍 서비스, 제작사 및 이벤트 장소가 포함됩니다. 지난해와 마찬가지로, 해당 산업에서는 좋은 **(55.4%)** 자동화와 나쁜**(31.1%)** 자동화를 모두 합쳐서 매우 많은 양의 자동화가 발생했으며, 전체 트래픽의 **83.4%**에서 **86.5%**로 증가했습니다. 좋은 봇이 많은 이유는 다양한 제3자가 엔터테인먼트 웹사이트를 스크래핑하여 가격 비교, 가용성 정보 및 소비자에게 추천을 제공하는 것과 관련이 있을 수 있습니다. 이 부문에서 가장 많이 타겟팅되는 웹사이트는 티켓팅 사이트입니다. 엔터테인먼트는 악성 봇의 첫 번째 표적이 된 산업 분야 중 하나였습니다. 스캘핑 봇, 좌석 재고 확인기, 사용자 계정에 액세스하는 자격 증명 스터핑 봇은 이러한 사이트에서 가장 널리 사용되는 봇입니다.

산업별 악성 봇의 정교화

다음 차트는 정교함 수준에 따른 악성 봇 트래픽의 분석 결과를 보여줍니다. 고급 악성 봇의 비율이 높을수록 업계의 봇 문제가 더 복잡해집니다. 이 포괄적인 분석은 올해 다양한 산업이 직면했던 악성 봇 위험에 대해 더 자세히 설명합니다.

악성 봇 트래픽의 정교함과 트래픽 볼륨 자체 사이에 반드시 상관 관계가 있는 것은 아니라는 점을 이해하는 것이 중요합니다. 다시 말해, 많은 양의 악성 봇 트래픽이 발생하는 업계에서는 모든 봇을 단순 봇으로 분류할 수 있습니다. 그러나 고급 봇 트래픽은 볼륨이 아무리 작더라도 상당한 위험을 초래한다는 점을 기억하는 것이 중요합니다. 이는 고급 악성 봇이 간단한 악성 봇보다 적은 요청으로 목표를 달성할 수 있고 지정된 목표를 훨씬 더 지속적으로 유지할 수 있기 때문입니다.

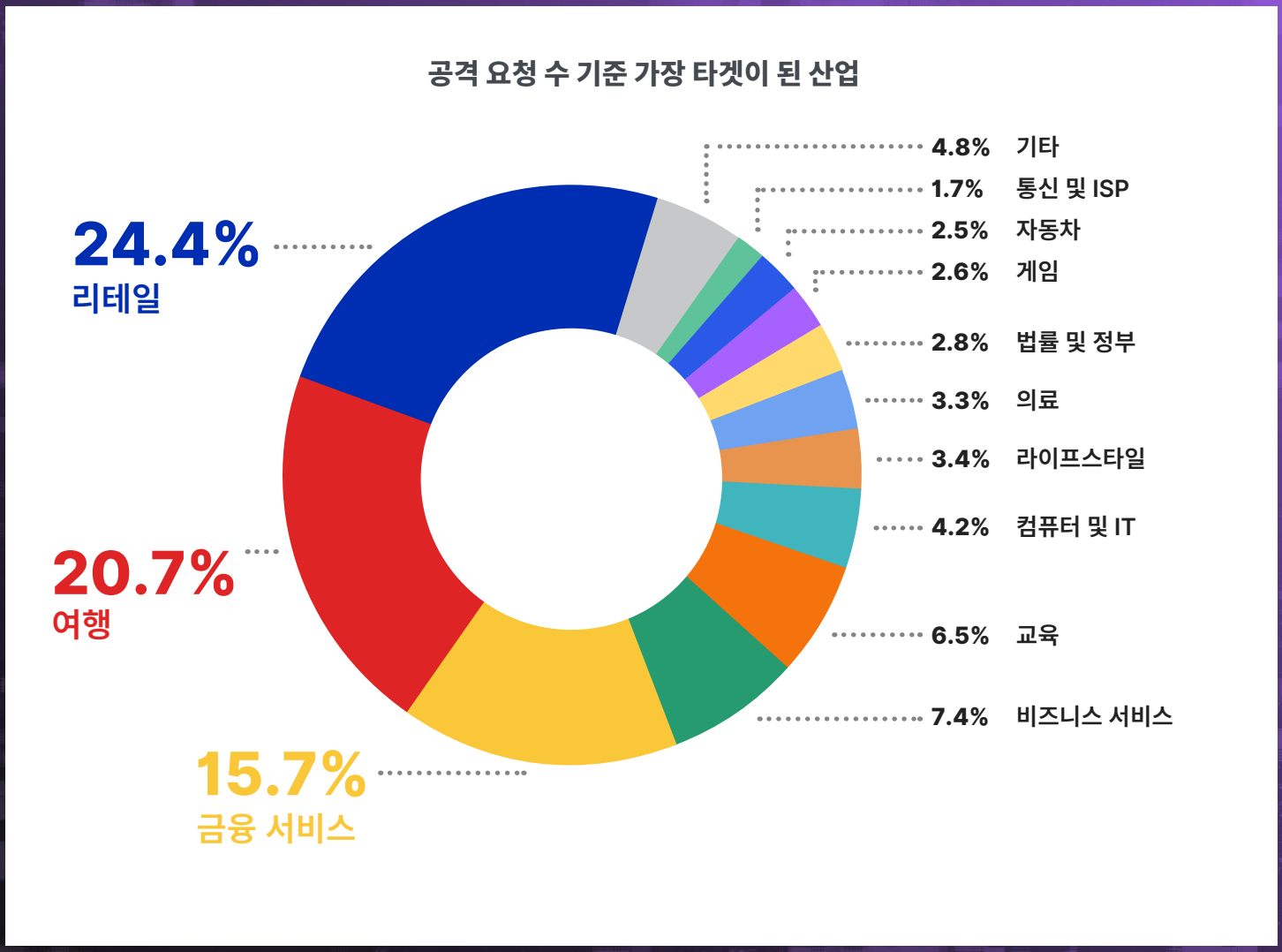


봇 공격의 가장 큰 표적이 되는 산업

각 산업에 대한 트래픽 프로필 분석에는 모든 트래픽에 대한 봇 트래픽의 비율이 표시됩니다. 반면, 산업 전반에 걸친 봇 공격의 분포는 다른 관점을 제공합니다. 이는 어떤 산업이 봇 공격의 가장 큰 비중을 차지했는지를 나타냅니다. 작년과 마찬가지로 리테일, 여행 및 금융 서비스는 가장 많이 표적이 된 상위 3개 산업입니다.

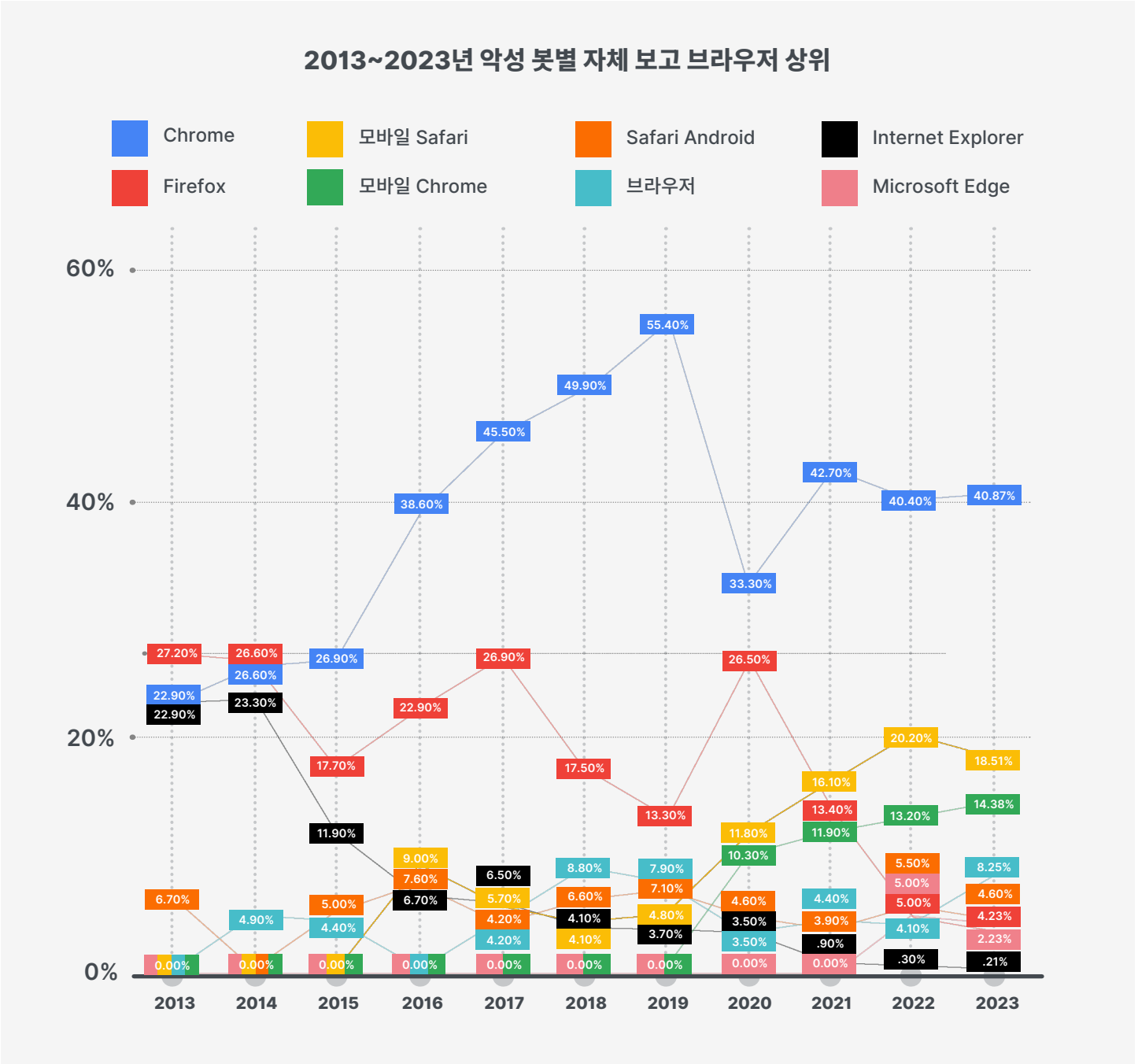
이전 섹션에서 자세히 설명했듯이 이러한 산업은 복잡한 봇 문제에 직면해 있으며, 다양한 봇 사용 사례가 최종 수익을 위협하고 있습니다. 세 가지 모두 사이트에서 봇의 정교함에서 높은 순위를 차지하고 있습니다.

악성 봇 비율이 높은 산업이 반드시 다른 산업에 비해 공격 대상이 더 많거나 적다는 것을 의미하는 것은 아니라는 점을 알아두는 것이 중요합니다. 어떤 업계는 일 년 내내 상당한 인간 트래픽을 겪었기 때문에 봇 트래픽 비율이 낮을 수 있습니다. 또는, 원하는 결과를 얻기 위해 더 적은 요청이 필요한 더욱 진보된 악성 봇의 표적이 되었을 수도 있습니다.



모바일 Chrome 및 Android 브라우저의 인기 상승

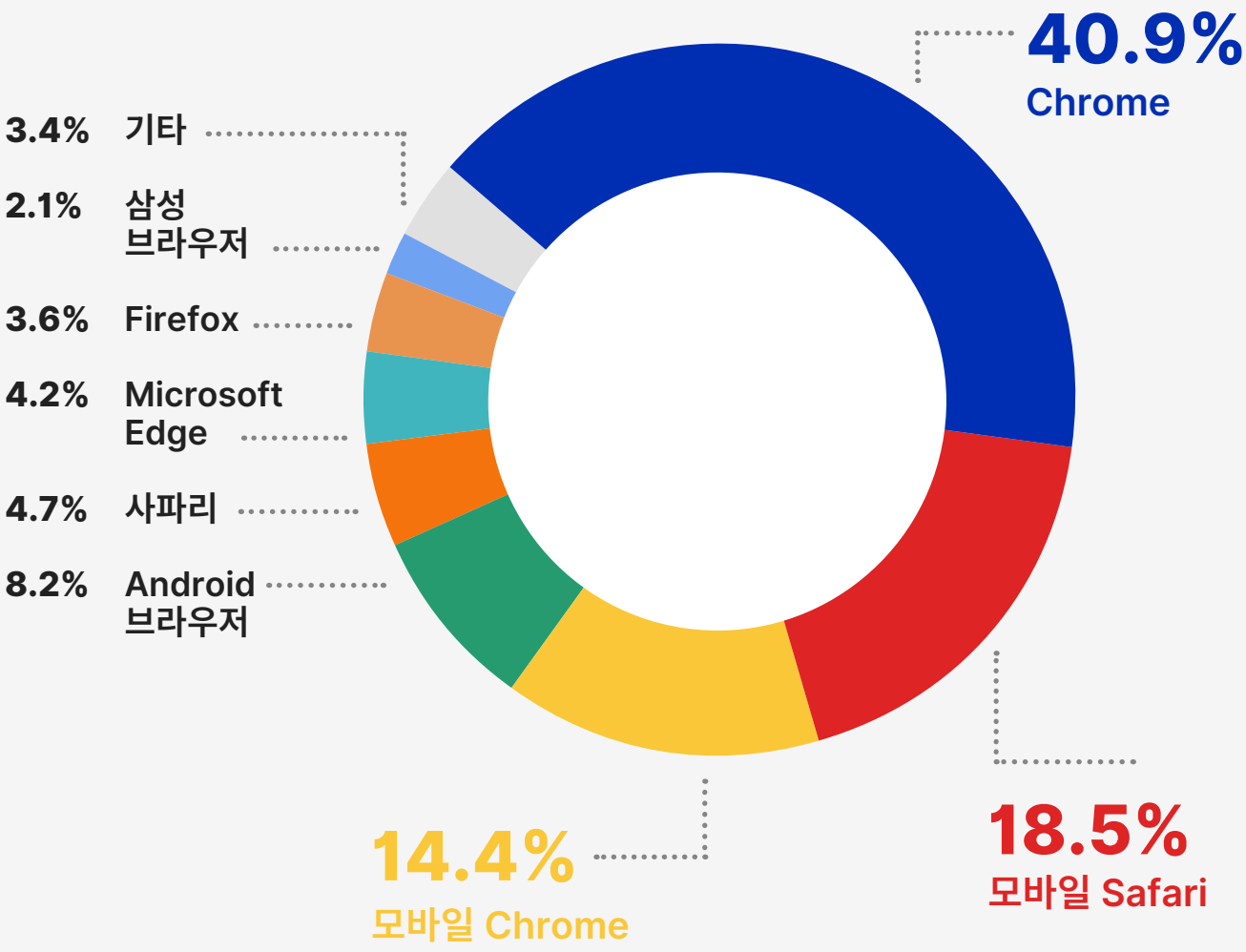
악성 봇은 탐지를 회피하기 위해 다양한 기법을 사용하며, 그 중 하나는 인간이 일반적으로 사용하는 웹 또는 모바일 브라우저로 출처를 보고하여 정당한 사용자로 위장하는 것입니다. 그들은 브라우저 자동화 소프트웨어를 사용하여 이를 달성합니다. 이 기법은 한때는 고급 회피 방법이었지만 대부분의 악성 봇에서 흔해졌습니다. 흥미롭게도 지난 10년 동안 악성 봇 간의 브라우저 인기 추세가 변화하였는데, 이는 인간 사용자의 선호도 변화와 봇이 탐지를 회피하는 데 도움이 되는 다른 추세를 반영한 것입니다. 예를 들어, Internet Explorer는 한때 사람과 악성 봇 사이에서 인기 있는 브라우저였지만, 지금은 더 이상 그렇지 않습니다.



지난 2년 동안, 우리는 악성 봇들 사이에서 모바일 웹 브라우저의 인기가 증가하는 것을 목격했습니다. 이는 모바일 Safari**(18.51%)**를 기본 브라우저로 선택한 악성 봇의 인기가 높아지면서 시작되었지만, 모바일 Chrome**(14.38%)**과 Android 브라우저**(8.25%)**로 빠르게 확장되었습니다.

악성 봇이 Chrome을 사용하는 비율은 모든 악성 봇 트래픽의 **40.87%**로 동일하게 유지된 반면, Firefox는 인기도**(3.57%)**를 계속 잃고 있습니다.

공격 요청 수 기준 가장 타겟이 된 산업



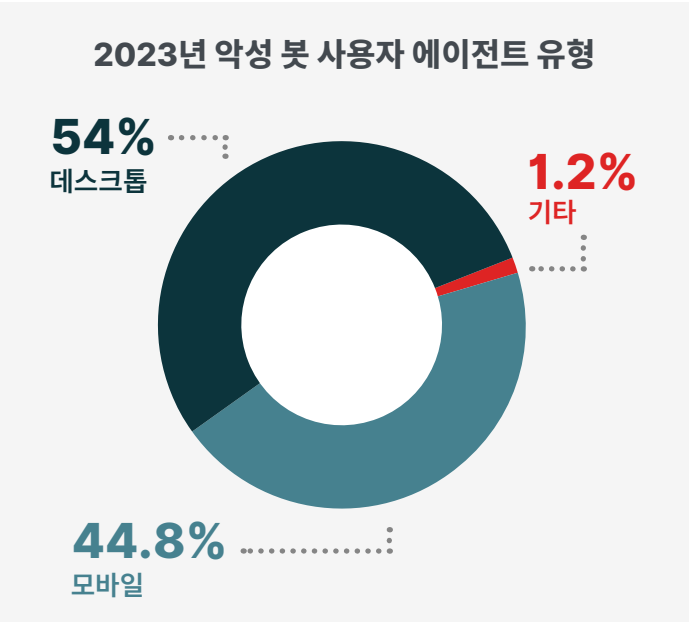
모바일 사용자 에이전트가 봇 트래픽의 거의 절반을 차지

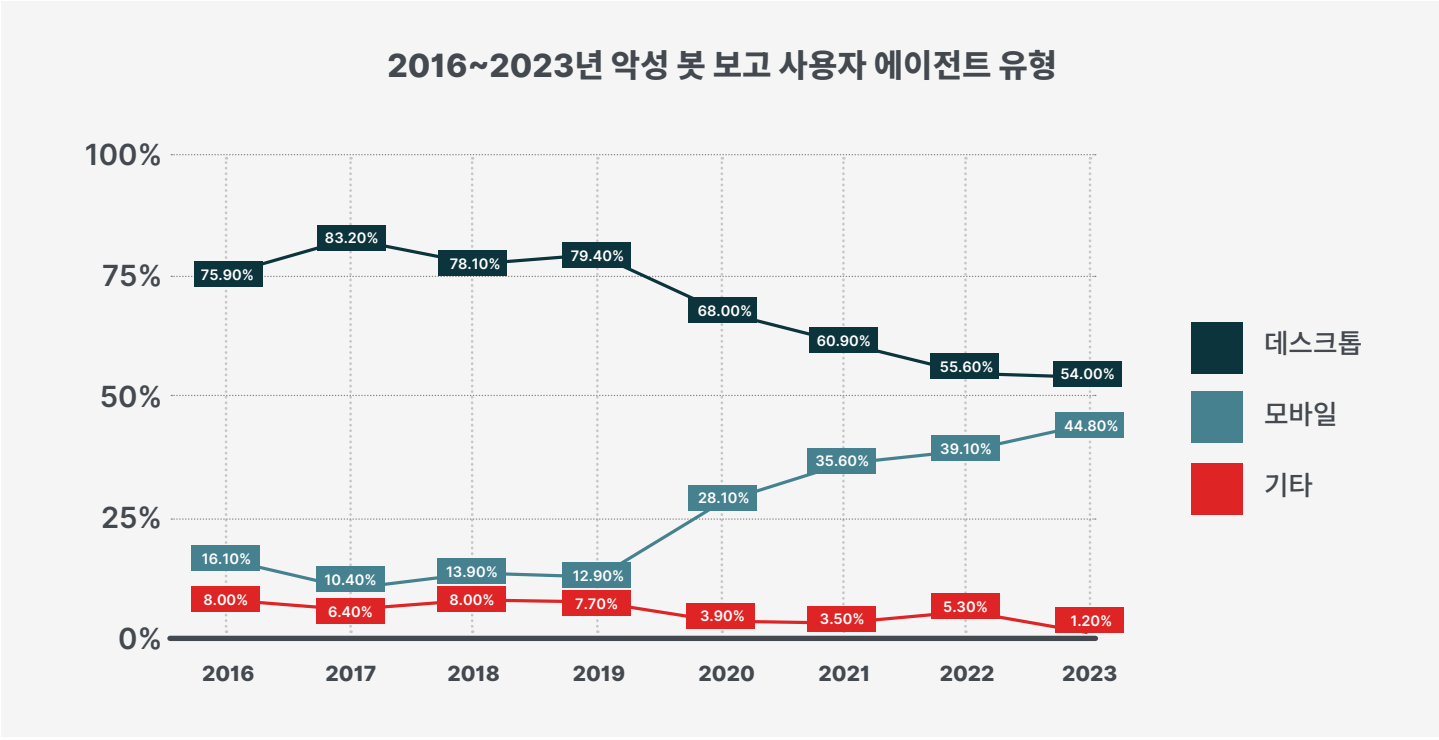
모바일 사용자 에이전트로 위장한 악성 봇은 모든 악성 봇 트래픽의 **44.8%**를 차지했습니다. 이들의 인기는 2020년 **28.1%**에서 2023년 **44.8%**로 크게 증가했습니다. 이렇게 인기가 증가하는 주된 이유는 두 가지가 있습니다. 첫째, 악성 봇은 인간의 트래픽 특성을 긴밀히 모방하려고 시도합니다. 2024년 2월 현재, 인터넷 트래픽의 **55%** 이상이 모바일 기기에서 발생합니다[7]. 우리 중 많은 사람들이 휴대폰을 사용하여 인터넷을 검색하므로, 봇이 인간 트래픽에 섞이기 위해 동일한 작업을 수행하는 것은 당연합니다. 악성 봇 트래픽을 살펴보면 모바일 기반 에이전트와 데스크톱 기반 에이전트 간의 격차는 매우 가깝습니다.

두 번째 이유는 개인정보 보호와 관련이 있습니다. 모바일 Safari와 같은 일부 웹 브라우저에는 악성 봇이 자신의 진짜 정체를 숨기는 것을 더 쉽게 만들어 주는 추가적인 개인정보 제어 및 기능이 있습니다. 이러한 브라우저는 웹사이트의 출처에 더 적은 속성을 전송할 수 있으므로, 기기의 정확한 지문을 생성하는 것이 더 어려워질 수 있기 때문입니다.

Chrome, Firefox, Safari 또는 Edge와 같이 데스크톱 기반 사용자 에이전트로 자체 보고하는 악성 봇의 비율은 2020년 **68%**에서 2023년 **54%**로 감소했습니다.

나머지 악성 봇 트래픽인 **1.2%**는 자신을 다른 사용자 에이전트(예: Playstation, Nintendo, Smart TV 등)로 보고했습니다.





7 https://explodingtopics.com/blog/mobile-internet-traffic

주거용 프록시의 부상

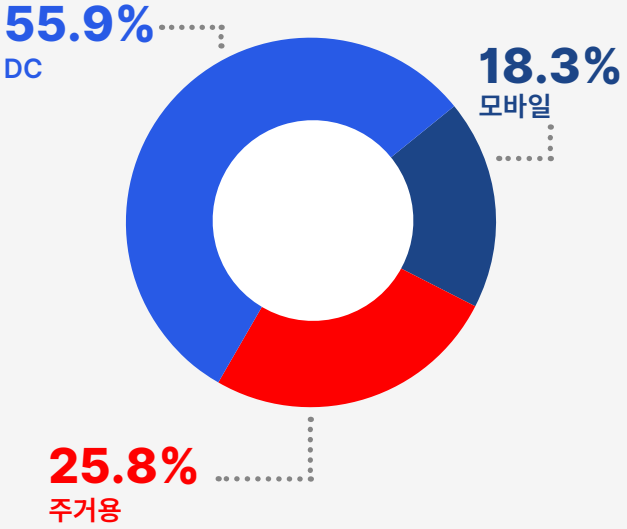
올해 주거용 ISP에서 발생한 악성 봇 트래픽은 전체 악성 봇 트래픽의 **25.8%**를 차지했으며, 이는 작년의 **17.4%**보다 증가한 수치입니다. 과거에는 합법적인 사용자가 일반적으로 사용하는 사용자 에이전트(브라우저)로 위장하여 정당한 인간 사용자로 위장하는 것이 고급 회피 기법으로 간주되었지만, 이제는 흔한 일이 되었습니다. 모바일 또는 주거용 프록시를 사용하여 요청의 출처를 숨기면 다른 차원의 진위성을 추가함으로써 문제가 해결됩니다. 이러한 유형의 봇 행동은 목표를 달성할 수단과 역량을 갖춘 정교하고 끈기 있고 결단력 있는 적대자와 그렇지 않은 적대자를 구분해 줍니다.

Imperva 위협 연구팀은 봇 프로그래머가 관리형 소프트웨어 제품(예: 올인원 봇) 및 협업 지식 기반 내에서 주거용 IP 프록시 통합을 점점 더 많이 사용하고 있음을 발견했습니다. 당사는 이러한 회피 기술을 탐지하고 이에 대응하기 위한 표적 탐지 메커니즘을 개발해 왔습니다.

데이터 센터는 여전히 대부분의 봇 공격 트래픽의 소스 **(55.9%)**이지만, 작년에 놀라울 정도로 급증했던 트래픽이 올해는 감소했습니다. 2020년 데이터 센터는 악성 봇 트래픽의 **54%**를 차지했지만 2021년에는 **45.1%**로 감소했습니다. 그리고 2022년에는 모든 악성 봇 트래픽의 **58.6%**로 크게 증가했습니다. 그러나 올해는 그 수가 감소했습니다.

모바일 ISP에서 발생하는 트래픽은 2022년 **24.1%**에서 2023년 **18.3%**로 감소했습니다.

2023년 ISP 유형별 악성 봇 트래픽



모바일 및 주거용 ISP에서 발생하는 악성 봇 트래픽이 상위 자리 차지

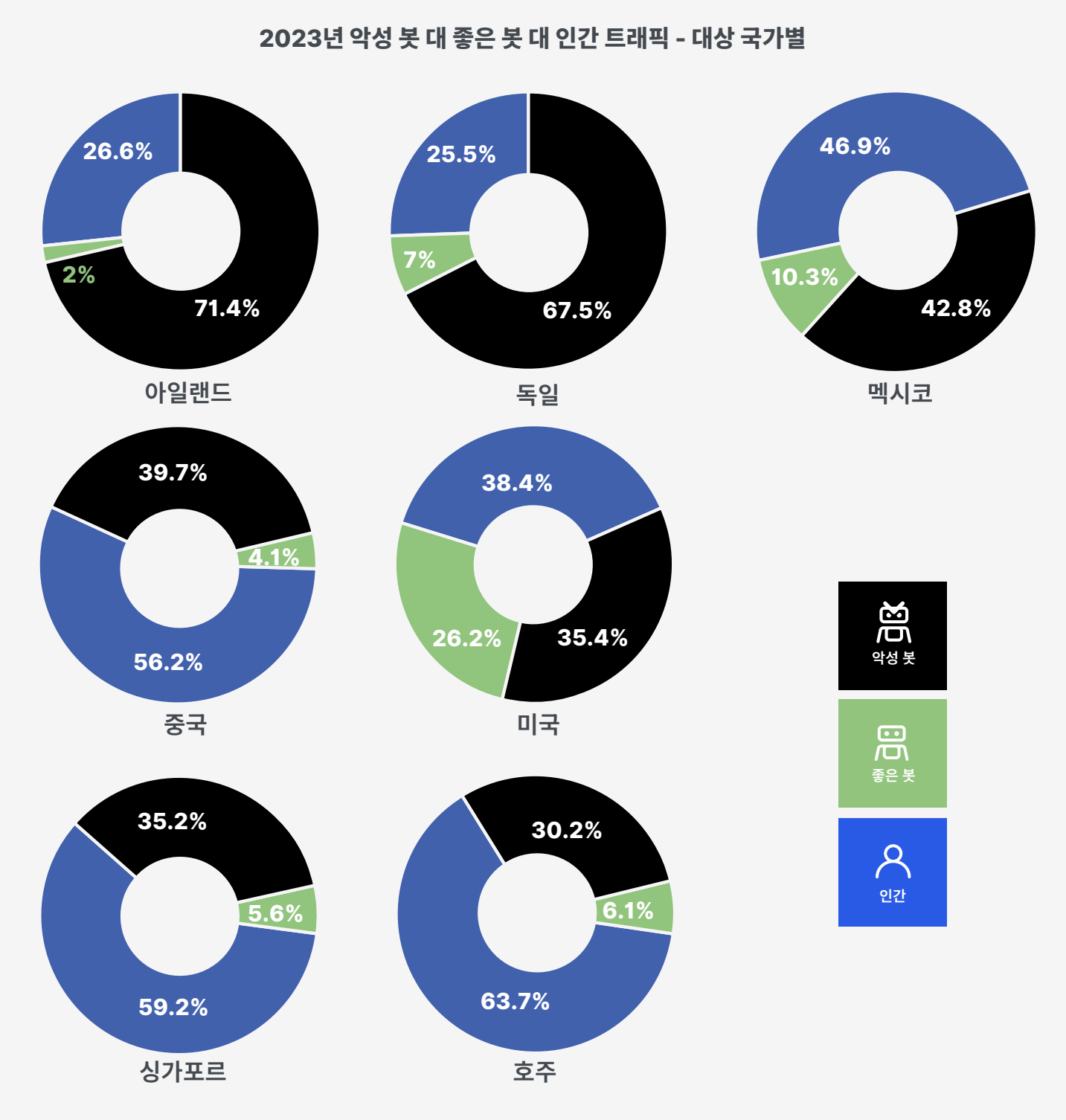
방금 살펴본 것처럼, 모바일 및 주거용 프록시는 악성 봇 운영자 사이에서 점점 더 인기를 얻고 있습니다. China Telecom은 2위를 차지했으며 Comcast는 4위, Spectrum은 6위입니다. 그러나 Amazon은 여전히 봇 트래픽의 17.01%를 차지하며 1위 자리를 유지하고 있습니다.

상위 봇 발생 ISP

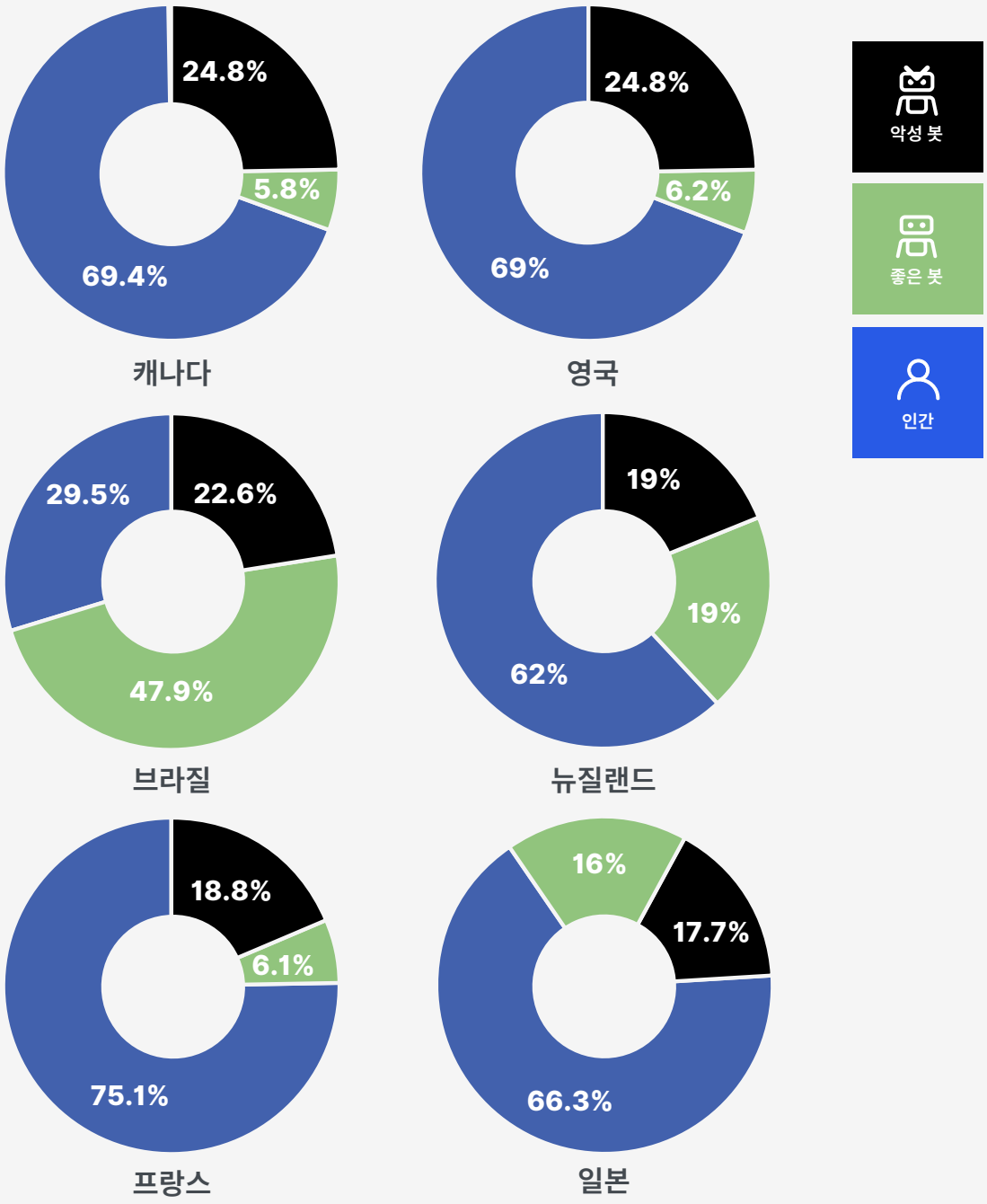
ISP	봇 트래픽의 %
Amazon.com	17.01%
China Telecom	3.42%
Digital Ocean	2.78%
Comcast Cable	1.76%
Microsoft Azure	1.63%
Spectrum	1.60%
Safaricom	1.51%
Google Cloud	1.51%
Jio	1.34%
Contabo GmbH	0.99%

전 세계 악성 봇

국가 차원에서 트래픽 분포를 살펴보겠습니다. 13개국을 대상으로 조사를 실시한 결과 13개국 중 6개 국가가 평균 이상의 악성 봇 트래픽을 경험한 것으로 나타났으며, 이는 전 세계 평균 **32%를 초과하는 수치입니다**. 올해도 독일과 아일랜드는 악성 봇으로 인한 트래픽이 **60%**가 넘는 것으로 기록되었습니다. 마찬가지로, 미국은 전체 트래픽의 **35.4%**가 악성 봇에서 발생하여 전 세계보다 약간 높은 악성 봇 트래픽 비율을 보였습니다.



2023년 악성 봇 대 좋은 봇 대 인간 트래픽 - 대상 국가별



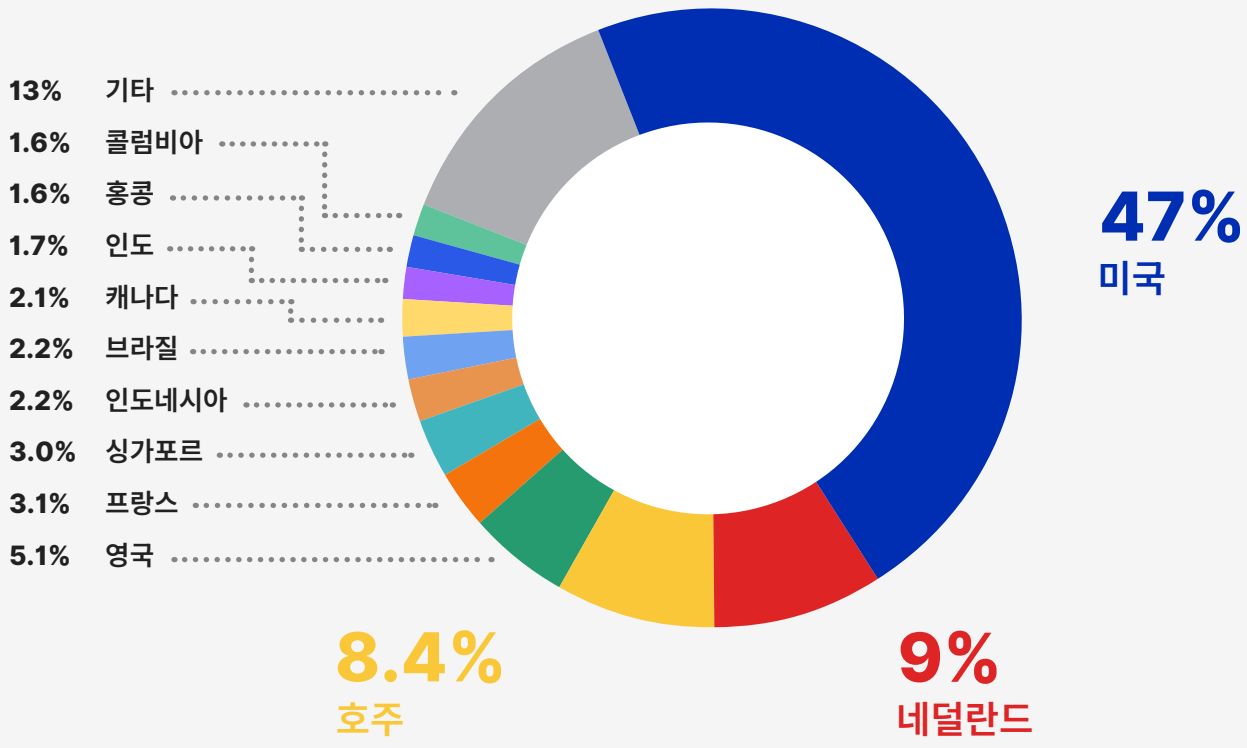
봇 공격의 가장 큰 표적이 된 국가는 미국과 네덜란드였습니다

봇 공격은 계속해서 미국을 표적으로 삼고 있으며, 미국은 여전히 최우선 타겟으로 남아 있습니다. 전체 공격의 **47%**가 미국 기반 웹사이트를 대상으로 이루어집니다. 이 비율은 봇 공격의 **41.1%**가 미국에 집중되었던 작년 대비 증가한 수치입니다. 네덜란드는 올해 호주를 근소한 차이로 제치고 봇 공격의 **9%**를 차지하며 2위를 차지했습니다. 호주는 봇 공격의 **8.4%**를 받았으며, 이는 작년**(16.4%)**의 절반에 가깝지만 과거와 비슷한 수준입니다**(2021년 6.8%)**. 영국은 공격의 **5.1%**로 4번째로 많이 타겟이 된 국가였으며, 그 뒤를 이어 프랑스가 **3.1%**로 타겟이 되었습니다.

Top 10
악성 봇에 의해 가장 많이 공격받는 상위 10개국

1. 미국
2. 네덜란드
3. 호주
4. 영국
5. 프랑스
6. 싱가포르
7. 인도네시아
8. 브라질
9. 캐나다
10. 인도

대상 국가별 봇 공격 분포(2023)



인공지능 시대의 악성 봇

30

인공지능(AI)과 대규모 학습 모델(LLM)의 등장은 우리가 헤아릴 수 없을 만큼 다양한 방식으로 우리 삶을 변화시키고 있습니다. 비즈니스 운영을 강화하는 것부터 일상 생활을 더욱 편리하게 만드는 것까지, 이러한 기술은 판도를 바꾸고 있습니다. 그러나 AI와 LLM의 부상은 많은 도전과제를 불러일으킵니다.

우리는 이미 보고서 전반에 걸쳐 이 문제가 인터넷 트래픽 프로필에 미치는 개괄적인 영향을 다루었습니다. 이러한 영향에는 자동화된 트래픽 수준 증가 및 단순한 악성 봇과 고급 악성 봇 간의 명확한 구분이 포함되며, 이 모든 것이 요약에 포함되어 있습니다. 그러나 웹 스크래핑의 합법성에 대한 논쟁이 다시 제기되는 등, 더욱 복잡한 문제도 존재하며 이는 수년 간 논쟁의 여지가 있는 문제입니다.

AI와 LLM 덕분에
웹 스크래핑이 다시 주목받게 되었습니다.

웹사이트에서 데이터를 추출하기 위해 봇을 사용하는 관행인 웹 스크래핑은 새로운 것이 아닙니다. 그러나 AI와 LLM의 출현으로 이 문제가 다시 주목받게 되었습니다. 이러한 고급 기술은 훈련을 위해 방대한 데이터에 크게 의존하며, 이는 종종 웹 스크래핑을 통해 수집됩니다. 이러한 관행은 AI 개발을 촉진할 수 있지만, 상당한 법적 및 윤리적 우려를 야기합니다.

웹 스크래핑의 합법성은 주로 관할권과 특정 상황에 따라 달라집니다. 그러나 AI의 등장으로 인해 이 문제는 더욱 복잡해졌습니다. 어떤 사람들은 AI 기술을 발전시키기 위해 데이터가 필요하다고 주장하지만, 다른 사람들은 이러한 데이터가 저작권법과 개인정보 보호 권리를 침해한다고 주장합니다.

논쟁의 핵심은 AI 모델의 훈련에 독점 콘텐츠와 데이터를 사용하는 데 있습니다. 많은 조직들은 허가 없이 자사 데이터를 수집할 경우 지적 재산권이 침해된다고 주장합니다. 반면, 웹 스크래핑을 지지하는 사람들은 AI 및 머신 러닝 기술을 발전시키는 데 이 관행이 필수적이라고 주장합니다.

혁신과 개인정보 보호 사이의 이러한 줄다리기 때문에 웹 스크래핑의 합법성을 둘러싼 논쟁이 다시 일어났습니다. 이 관행을 관장하는 법률은 종종 구식이며 국가마다 상당히 다르기 때문에 복잡한 문제입니다. AI와 LLM이 계속 진화함에 따라 기술 발전을 촉진하고 독점 콘텐츠와 데이터를 보호하는 데 균형을 맞춘 업데이트된 법률과 규정이 절실히 필요합니다.

The New York Times는 획기적인 법적 소송에서 OpenAI와 Microsoft를 상대로 소송을 제기하며 AI 모델 훈련을 위해 웹 스크래핑을 통해 저작권을 침해했다고 주장했습니다. OpenAI는 자사의 행위가 미국 저작권법의 "공정 사용" 원칙에 따라 보호된다고 주장합니다. 동시에 The Times는 OpenAI의 콘텐츠 사용이 공정한 사용에 필요한 "변혁적" 기준을 충족하지 않는다고 주장합니다. 이 소송의 결과는 저작권법과 AI의 경계를 재정의하여 저작권이 있는 자료를 AI 훈련에 사용하는 것의 합법성에 대한 선례가 될 수 있습니다. 또한 콘텐츠 제작자의 권리와 AI 혁신의 요구 사이에 균형을 맞추는 업데이트된 저작권법의 시급한 필요성을 강조합니다. 이 사례는 AI 시대에 웹 스크래핑으로 인해 발생하는 복잡한 법적, 윤리적 문제를 강조하여 기업이 디지털 자산을 사전에 보호해야 할 필요성을 강조합니다.

AI가 계속 진화함에 따라 저작권법과 개인정보 보호 권리와 관련하여 데이터에 대한 요구와 균형을 이루는 명확한 법적 가이드라인의 필요성이 그 어느 때보다 중요해졌습니다. 이러한 논쟁은 끝나지 않았으며, 우리가 앞으로 나아감에 따라 기업, 법률 시스템 및 기술 리더들은 이 복잡한 상황을 신중하고 책임감 있게 헤쳐나가야 합니다.

뜨거운 인기로 부상한 레스토랑 예약

스캘핑 봇에는 간단한 경험칙 또는 방정식이 존재합니다. 수요가 높고 가용성이 제한적이면 봇에 대한 관심이 높아진다는 것입니다. 이러한 봇 운영자는 매우 기회주의적이며 공급이 부족하고 수요가 높은 모든 상황을 이용합니다. 2020년부터 2022년까지 팬데믹으로 인한 적체로 인해, 전 세계에서 여권과 비자, 운전면허 시험 예약을 낚아채는 봇들도 나타났습니다.

따라서 이들이 이제 레스토랑 업계를 표적으로 삼아 주요 시간대 예약을 확보하고 제3자 플랫폼에서 엄청난 가격으로 판매하는 것은 놀라운 일이 아닙니다. 편의성이 무엇보다 중요한 디지털 시대에, 온라인 예약은 좋아하는 식당에서 자리를 잡기 위한 표준으로 자리잡았습니다.

최고급 레스토랑에서 특별한 저녁 식사를 계획했는데, 예약이 오픈된 지 불과 0.1초 만에 모든 예약이 사라진다는 걸 발견하는 상황을 상상해 보십시오. 더 나쁜 점은 이러한 예약이 나중에 재판매 플랫폼에 나타나서, 최초에는 무료로 가능했던 자리를 확보하기 위해 최대 340달러를 지불해야 한다는 것입니다. 오늘날 많은 식당 손님이 이런 현실을 겪고 있는데, 이는 바로 악성 봇의 사악한 활동 때문입니다.

높은 수요와 제한된 가용성

=

봇에 대한 관심

이들 봇은 콘서트 티켓과 수집용 스니커즈를 거래했듯이 이 시스템을 이용해 수익을 내기 때문에, 실제 고객이 인기 있는 시설에서 예약을 확보하는 것은 사실상 불가능해졌습니다. 이는 고객을 좌절하게 할 뿐만 아니라 레스토랑 사업에도 해를 끼칩니다. 봇으로 예약된 좌석이 채워지지 않으면 레스토랑은 빈 테이블, 그리고 유효하지 않은 신용카드로 청구된 취소 수수료로 인해 잠재적인 수익을 잃게 됩니다.

이에 대응하여 레스토랑과 예약 플랫폼은 이러한 사이버 위협에 맞서 전쟁을 벌이고 있습니다. 그들은 이메일 주소가 뒤섞인 계정이나 전화번호가 연결되지 않은 계정에서의 예약 등 의심스러운 활동을 탐지하고 차단하기 위한 조치를 시행하고 있습니다. 일부는 온라인 예약 횟수를 줄이고 있으며, 그 대신에 방문 예약을 더 많이 받기로 했습니다.

팬데믹 이후 시대의 티켓 스캘핑 급증

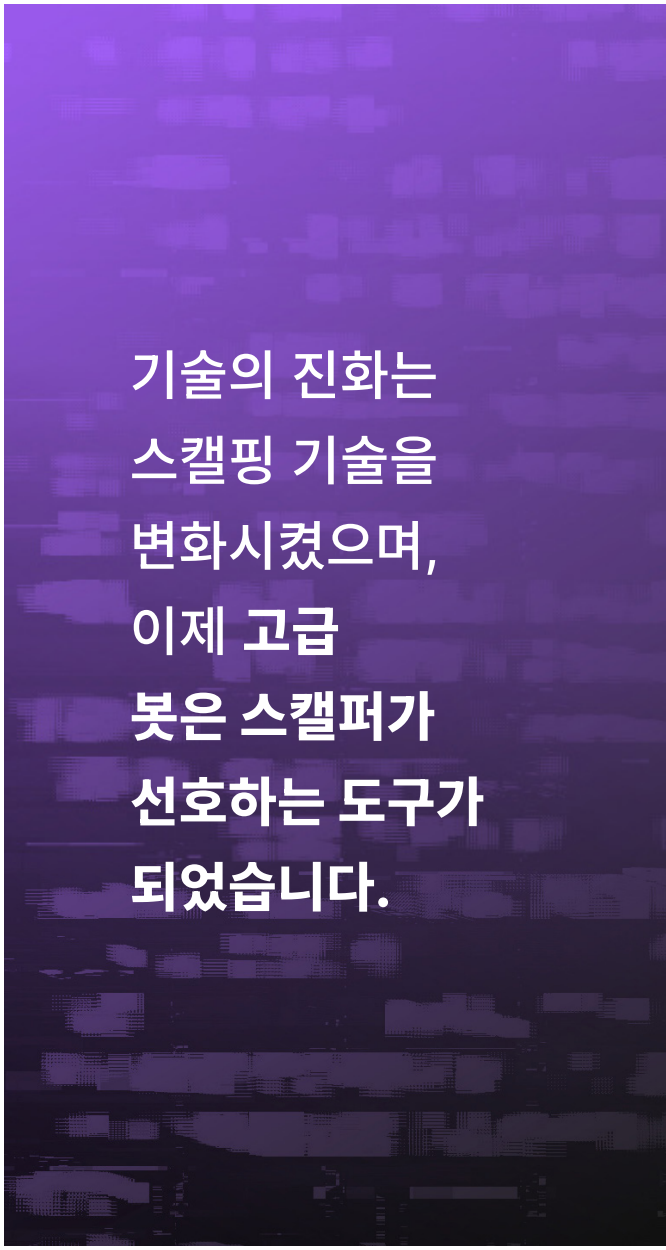
라이브 이벤트는 지난 몇 년 동안 전 세계적으로 콘서트 티켓에 대한 수요가 매우 높아지면서 엄청난 수익을 거두었습니다. 앞서 언급한 바와 같이, 높은 수요와 제한된 가용성은 봇에 대한 관심을 의미합니다. 실제로 티켓 스캘핑(이벤트 티켓을 대량으로 구매해 높은 가격으로 재판매하는 행위)이 상당히 다시 급증했습니다. 오늘날 자동화(일명 봇)를 기반으로 하는 이 오래된 관행은 팬데믹 이후 시대에 새로운 활력을 얻었습니다.

기술의 발전으로 스캘핑 기술이 변화하면서 고급 봇은 이제 스캘퍼가 선호하는 도구가 되었습니다. 티켓팅 플랫폼이 범주화되는 엔터테인먼트 웹사이트는 지난해 **70.8%**로 두 번째로 높은 고급 악성 봇 비율을 보였습니다('산업별 악성 봇 정교화' 섹션 참조).

이러한 봇은 일반적으로 올인원(AIO) '솔루션'으로, 운영자가 구매 프로세스를 완전히 자동화할 수 있도록 합니다. 이러한 공격은 종종 여러 가지 회피 기술과 CAPTCHA 해결 기능을 통합합니다. 이로 인해 소비자들의 좌절감이 널리 확산되고 있으며, 기업과 라이브 엔터테인먼트 산업에 상당한 어려움을 안겨 주고 있습니다.

실제 고객은 원래 가격으로 티켓을 구매할 수 없어 기업은 잠재적인 매출 손실에 직면하게 되며, 이는 기업의 평판과 고객 충성도에 손상을 입힙니다. 반대로 소비자는 과도한 가격과 이벤트에 대한 제한된 접근성으로 인해 시장에 대한 불만과 잠재적 불신을 겪어야 합니다.

팬데믹 제약이 완화됨에 따라 라이브 엔터테인먼트에 대한 수요가 급증하면서 티켓 스캘핑이 다시 급증하고 있습니다. 이로 인해 여러 국가에서 이 문제를 해결하기 위한 법적 조치를 시행하고 있습니다. 그러나 웹 스크래핑의 적법성과 마찬가지로, 기업도 봇 트래픽으로 인한 위험을 완화하기 위해 사전 조치를 취해야 하므로 법적 조치가 마련되기를 기다릴 수 없다는 것은 분명합니다.



권장 사항

33

기업은 봇과 온라인 사기로부터 어떻게 자신을 보호해야 합니까? 각 사이트의 고유한 취약점과 공격 벡터를 고려할 때 보편적인 솔루션을 찾기 어려울 수 있습니다. 그럼에도 불구하고 다면적인 보안 조치를 구현하여 선제적인 접근 방식을 채택하면 위험을 크게 완화할 수 있습니다. 여기에는 고급 봇 탐지 및 사이버 보안 관리 솔루션 구축이 포함됩니다. 이러한 전략을 함께 사용하면 끊임없이 변화하는 온라인 사기 및 봇 관련 보안 위협에 대항하는 포괄적인 방어 메커니즘이 형성됩니다.

악성 봇 활동 및 자동 사기 감지를 위한 보안 권장 사항

1. 위험 식별

봇 트래픽을 막는 것은 웹사이트의 잠재적 위험을 식별하는 것으로 시작됩니다:

A. 마케팅 및 전자상거래 이니셔티브는 특히 수요가 많은 제품을 한정 수량으로 출시할 때 봇이 더 많이 활용되는 경우가 많습니다. 최신 스니커즈, 차세대 게임 콘솔 또는 독점 수집가 아이템 등, 이러한 제품의 출시일을 지정하는 것은 봇에게 신호탄이 될 수 있습니다. 이처럼 자동화된 개체는 실제 고객보다 먼저 상품을 확보하여 접근을 독점하고 판매 노력을 훼손할 가능성이 있습니다. 트래픽 급증을 효과적으로 관리하기 위해 웹사이트의 방어를 강화하여 정당한 소비자와 제품 출시를 탈취하려는 회피형 봇을 구분할 수 있도록 하는 것이 중요합니다. 고급 트래픽 분석, 실시간 봇 탐지 메커니즘 및 강력한 인증 조치를 구현하면 플랫폼을 보호하고 실제 고객에게 공평한 접근을 보장하는 데 도움이 됩니다.

B. 사이트의 잠재적 취약성을 인식하는 것은 효과적인 봇 관리 전략의 중요한 요소입니다. 특정 웹사이트 기능은 특히 악성 봇 활동에 취약합니다. 예를 들어, 로그인 기능을 통합하면 자격 증명 스터핑 및 자격 증명 크래킹 공격이 발생할 수 있으며, 공격자는 도난당한 자격 증명을 사용하여 무단 액세스 권한을 얻을 수 있습니다. 마찬가지로 체크아웃 양식이 존재할 경우 카딩 또는 카드 크래킹으로 알려진 신용카드 사기의 위험이 증가할 수 있습니다. 또한 기프트 카드 기능을 구현하면 사기를 저지르려는 봇을 유인할 수 있습니다. 이러한 위험을 완화하기 위해서는 강화된 보안 조치를 적용하고 이러한

페이지에 더 엄격한 규칙을 적용하는 것이 필수적입니다. 다단계 인증, CAPTCHA 및 의심스러운 활동에 대한 지속적인 모니터링을 구현하면 이러한 자동화된 위협에 대한 사이트의 방어를 크게 강화할 수 있습니다.

2. 취약성 감소

노출된 API 및 모바일 애플리케이션을 보호하는 것은 웹사이트를 보호하는 것만큼이나 중요하며, 모든 디지털 접점을 포괄하는 종합적인 사이버 보안 전략의 필요성을 강조합니다. 이를 위해서는 웹사이트의 보안에만 집중하는 것 이상의 작업이 필요합니다. API와 모바일 앱은 종종 웹 애플리케이션과 민감한 데이터에 대한 게이트웨이 역할을 하여 사이버 위협에 대한 추가적인 경로가 됩니다. 이러한 플랫폼 전반에 강력한 보안 대책을 구현하고 시스템 간 차단을 하는 것은 취약성을 줄이는 데 필수적입니다. 이러한 통합 접근 방식은 잠재적 공격에 대한 통합 방어 메커니즘을 보장하여 모든 디지털 진입점을 통해 웹 애플리케이션과 중요 데이터에 대한 무단 액세스 위험을 최소화합니다.

3. 위협 감소: 사용자-에이전트

많은 봇 도구 및 스크립트에는 오래된 브라우저 버전의 사용자 에이전트 문자열이 포함되어 있습니다. 반면, 인간은 브라우저를 최신 버전으로 자동 업데이트해야 합니다. 오래된 브라우저 버전을 차단하기 위한 단계를 따르십시오.

	차단 3년 이상 수명 종료	**CAPTCHA** 2년 이상 수명 종료
Chrome 버전	<95	<105
Firefox 버전	<95	<105
Safari 버전	<13	<14
Internet Explorer 버전	<11	<11

4. 위협 감소: 프록시

공격자들이 정당한 사용자 행동을 시뮬레이션하기 위해 이러한 서비스를 이용함에 따라, 악성 봇이 활동을 숨기기 위해 프록시 서비스를 사용하는 사례가 증가하고 있습니다. 대량 IP 서비스의 IP 순환을 활용하면 실제 출처를 가릴 수 있어 탐지 작업이 복잡해집니다. 이러한 위협을 완화하기 위한 전략적 접근 방식에는 알려진 대량 IP 데이터 센터의 액세스를 제한하여 봇넷 트래픽이 네트워크에 침투할 가능성을 크게 줄이는 것이 포함됩니다. 이러한 프록시 기반 공격의 주요 출처로는 Host Europe GmbH, Dedibox SAS, Digital Ocean, OVH SAS 및 Choopa, LLC와 같은 데이터 센터 및 클라우드 서비스 제공업체가 있습니다. 이러한 개체에서 발생하는 트래픽에 대한 액세스 제어 및 모니터링을 구현하면 봇이 생성한 트래픽을 선제적으로 식별하고 차단하여 이러한 프록시 지원 공격과 관련된 위험을 최소화함으로써 보안 태세를 강화할 수 있습니다.

5. 위협 감소: 자동화

Puppeteer, Selenium 및 WebDriver와 같은 최신 툴은 공격자가 온라인에서 인간의 행동을 모방하기 위해 오용하는 경우가 많아 대량 계정 등록 및 데이터 유출과 같은 유해한 활동을 수행할 수 있습니다. 이러한 악의적인 노력을 정당한 트래픽과 구별하려면 부자연스럽게 빠른 상호 작용 또는 비정상적인 탐색 패턴과 같은 자동화 징후에 대한 탐지 전략을 구현해야 합니다. 이러한 행동을 파악함으로써 조직은 자동화된 공격을 효과적으로 탐지하고 차단하여 정당한 사용자 상호 작용을 보호할 수 있습니다.

6. 트래픽 평가

A. 명시적인 지표 없이 봇 트래픽을 식별하는 것은 어려운 일이지만, 특정 패턴은 종종 봇 트래픽의 존재를 암시합니다. 높은 이탈률과 낮은 전환율은 인간이 아닌 트래픽의 징후일 수 있습니다. 또한, 트래픽이 갑자기 설명 없이 급증하거나 특정 URL을 타겟으로 하는 요청이 비정상적으로 많아지는 것은 봇 활동을 나타내는 신호일 가능성이 큽니다. 이러한 이상 징후를 모니터링하면 조직에서는 잠재적인 봇 트래픽에 플래그를 지정하여 추가 조사와 적절한 대응 조치를 통해 원치 않는 방해를 완화할 수 있습니다.

B. 특정 엔드포인트로의 트래픽이 갑자기 급증하면 봇이 특정 이벤트나 작업을 타겟으로 삼고 있음을 나타낼 수 있습니다. 이러한 급증이 봇으로 인한 것인지 평가하려면 트래픽 증가의 출처를 분석하십시오. 일반적인 수준을 크게 넘는 트래픽 수준을 생성하는 단일 IP 주소, ISP 또는 특정 URL과 같은 패턴을 찾습니다. 이러한 출처를 식별하면 봇 활동에 대한 명확한 증거를 얻을 수 있으며, 이를 통해 타겟이 된 조치를 취할 수 있습니다. 예를 들어, 트래픽이 주로 단일 IP 또는 좁은 범위의

IP에서 발생하는 경우, 이는 자동화된 액세스 시도를 나타내는 강력한 지표입니다. 이러한 통찰력은 봇 공격에 대한 효과적인 대응책을 구축하여 디지털 자산을 보호하는 데 매우 중요합니다.

7. 트래픽 모니터링

A. 로그인 페이지에서 실패한 로그인 시도 기준을 정의한 다음, 이상 징후나 급증 현상을 모니터링합니다. 문제가 발생할 경우 자동으로 알림을 받을 수 있도록 알림을 설정합니다. “낮고 느린” 고급 공격은 사용자 또는 세션 수준의 경보를 트리거하지 않으므로 전역 임계값을 설정해야 합니다.

B. 결제 및 기프트 카드 검증 페이지에서 실패 횟수나 트래픽이 증가하는 것은 카드 공격의 신호이거나 GiftGhostBot과 같은 봇이 기프트 카드 잔액을 훔치려 한다는 신호일 수도 있습니다.

8. 인식

전 세계적인 데이터 침해 및 유출에 대한 경계를 유지하는 것이 중요합니다. 공격자가 이러한 침해로부터 자격 증명 덤프를 구매하거나 봇 인프라를 임대하여 공격을 자동화하는 것이 매우 간단하기 때문에 위협이 가시적인 위험으로 높아집니다. 봇은 새로 손상된 자격 증명을 자주 악용하여 스터핑 공격 및 계정 탈취(ATO)를 수행하는 경우가 많은데, 이러한 자격 증명은 활성 상태를 유지할 가능성이 높기 때문입니다. 이 전략은 플랫폼에서 사용자 계정을 성공적으로 침해할 가능성을 크게 높입니다. 이러한 침해에 대한 정보를 지속적으로 파악하고 그 영향을 파악하면 사전에 방어를 강화하여 사이트가 이러한 자동화된 위협의 표적이 될 가능성을 줄이는 데 도움이 될 수 있습니다.

9. 봇 보호 솔루션 평가

봇 공격 환경이 크게 변화함에 따라 봇 보호 솔루션을 평가하는 것이 매우 중요합니다. 악성 봇을 방어하기에 충분했던 단순한 조치는 이제 효과가 없습니다. 이 보고서에서 수집된 통찰력은 최신 봇의 정교함과 적응성이 이전 수준을 능가하며, 사용 편의성과 효과성 덕분에 사이버 범죄자들이 선호하는 도구임을 강조합니다. 이러한 봇은 빠르게 진화하여 기존의 탐지 방법을 쓸모없게 만들지만, 그 어느 때보다 인간의 행동을 더 가까이 모방하기 때문에 정당한 사용자와 구별하기가 어렵습니다. 이러한 환경에서는 공격자가 높은 보상과 낮은 위험의 이점을 위해 봇을 활용하기 때문에 이러한 위협에 단독으로 대응하려는 시도가 거의 불가능합니다.

동적 방어 전략의 필요성은 그 어느 때보다 더 시급합니다. 이는 단순히 악성 봇을 식별하는 것이 아니라 복잡성이 증가하는 상황에서 유익한 봇과 구별하는 것입니다. 포괄적인 봇 방지 솔루션에는 사용자 행동 분석, 프로파일링, 지문 인식을 포함한 계층적 방어 접근 방식이 통합되어야 합니다. 이 전략은 정당한 봇의 이점을 유지할 뿐만 아니라 악의적인 활동을 효과적으로 걸러냅니다. 이러한 미묘한 접근 방식에는 새로운 위협의 속도에 맞춰 방어 시스템을 발전시킬 수 있는 전담 팀의 전문성이 필요합니다.

악성 봇 사용 사례

악성 봇 문제	정의	비즈니스에 어떻게 피해를 주는가	증상	표적 산업
가격 스크래핑	일반적으로 경쟁자를 깎아내리고 판매를 촉진하기 위해 봇을 사용하여 가격 정보를 불법적으로 모니터링하고 추적함	경쟁업체가 가격을 스크래핑하고, 가격을 인하하여 시장에서 자사를 이기는 경우 매출 손실 발생 스크래핑된 데이터가 회사의 가격이나 제품을 허위로 나타내는 방식으로 사용됨으로써 평판이 훼손됨 고객의 평생 가치가 악화됨 웹사이트 성능에 영향을 미침	전환율 감소 SEO 순위 하락 설명되지 않는 웹사이트 속도 저하 및 다운타임 (일반적으로 공격적인 스크래퍼로 인해 발생)	가격을 표시하는 모든 사업체: • 리테일 • 게임 • 항공사 • 여행
콘텐츠 스크래핑	봇을 사용하여 웹사이트에서 콘텐츠 및 데이터 추출	자사의 콘텐츠 또는 데이터가 다른 곳에 게시되어 원래 사이트를 방문하거나 제품 또는 서비스를 구매하는 사람이 줄어들어 수익 손실 중복 콘텐츠로 SEO 순위 손상 브랜드 평판 훼손 웹사이트 성능에 영향을 미침	자사 콘텐츠가 다른 사이트에 표시됨 SEO 순위 하락 설명되지 않는 웹사이트 속도 저하 및 다운타임(일반적으로 공격적인 스크래퍼로 인해 발생)	가격 스크래핑과 유사하지만, 추가로: • 구인란 • 광고란 • 시장 • 재무 • 티켓팅
계정 탈취 *(자격 증명 스터핑, 자격 증명 크래킹)*	봇을 사용하여 다른 사람의 사용자 계정에 불법 액세스 일반적으로 자격 증명 스터핑 또는 자격 증명 크래킹과 같은 무차별 로그인 기술을 사용하여 달성	브랜드 충성도와 평판에 대한 직접적인 영향, 부정적인 홍보 계정 잠금, 데이터 도난 또는 사기, 이탈률 증가로 인한 고객 불만 웹사이트 성능, 가용성 및 신뢰성에 영향을 미침 개인정보 보호 규정 미준수 위험 지원 및 사기 비용 증가	로그인 실패율 증가 고객 계정 잠금 및 고객 서비스 티켓 증가 사기 증가(로열티 포인트 손실, 신용카드 도난, 무단 구매) 지불 거절 증가	로그인 페이지가 있는 모든 비즈니스

악성 봇 문제	정의	비즈니스에 어떻게 피해를 주는가	증상	표적 산업
계정 생성 *(일명 계정 집계, 신규 계정 사기)*	봇을 사용하여 대량 계정 생성을 자동화합니다. 이러한 계정은 다양한 형태의 사기, 스팸 콘텐츠 또는 전파를 수행하는 데 오용될 수 있습니다	스팸 메시지를 보내거나 선전을 확대하는 데 사용되는 봇 계정에 대한 특정 플랫폼 및 웹사이트의 신뢰도 감소 신규 계정 프로모션 크레딧(금전, 포인트, 무료 플레이)을 악용하는 봇으로 인한 수익 손실 봇에서 발생하는 사용자 계정 또는 소셜 미디어 상호 작용에 기반한 모든 지표는 잘못된 의사 결정으로 이어질 수 있음	신규 계정 생성의 비정상적인 증가 댓글 스팸 증가 신규 계정에서 유료 고객으로의 전환율 하락	메시징 플랫폼 • 소셜 미디어 • 데이트 사이트 커뮤니티 가입 프로모션 남용 • 게임 • 재무
신용카드 사기 *(카딩, 카드 크래킹)*	도난당한 신용카드 번호의 유효성을 대량으로 확인하거나 누락된 세부 정보(CVV, 만료일 등)를 추측하기 위해 봇을 사용하는 경우	플랫폼에서 발생하는 사기 행위에 대한 기업의 책임으로 인한 재정적 손실: 비용이 많이 드는 지불 거절부터 소비자 신뢰 감소로 인한 수익 손실까지 브랜드 평판 손상 사업의 사기 점수 손상 사기성 지불 거절 처리를 위한 고객 서비스 비용 증가 데이터 개인정보 보호 규정(PCI-DSS, GDPR 등) 미준수	신용카드 사기 증가 고객 지원 통화 증가 지불 거절 처리 증가	결제 처리업체가 있는 모든 사이트: • 리테일 • 비영리/자선 • 항공사 • 여행 • 티켓팅 • 재무 • 게임
서비스 거부	봇을 사용하여 웹사이트에 요청을 너무 많이 보내 파일 시스템, 메모리, 프로세스, 스레드, CPU, 인적 또는 재정적 자원 등의 리소스가 고갈되는 상황	웹사이트 성능을 저하시켜 브라운아웃 또는 가동 중단 시간 발생 웹사이트 이용 불가로 인한 매출 손실 브랜드 평판 손상 잠재적 고객 이탈	특정 리소스(로그인, 등록, 제품 페이지 등)의 트래픽이 비정상적이고 설명할 수 없이 급증 고객 서비스 불만 증가	모든 산업
기프트 카드 잔액 확인 및 남용	봇을 사용하여 잔액 확인 페이지에 대한 잠재적 기프트 카드 번호의 열거를 자동화하여 기프트 카드 잔액을 훔침	신용카드 사기와 유사하게, 기프트 카드 사기는 기프트 카드에서 돈을 훔치는 봇으로 인한 금전적 손실을 초래함 사기성 지불 거절 처리를 위한 고객 서비스 비용 증가 고객 평판 저하 및 향후 매출 손실	기프트 카드 잔액 페이지에 대한 요청 급증 잔액 손실에 대한 고객 서비스 통화 증가	결제 옵션으로 기프트 카드를 제공하는 모든 비즈니스 - 주로 리테일

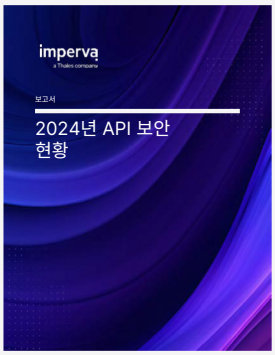
악성 봇 문제	정의	비즈니스에 어떻게 피해를 주는가	증상	표적 산업
재고 거부	봇을 사용하여 실제로 구매를 완료하지 않고 장바구니에 품목을 보관함으로써 실제 소비자들이 물품을 살 수 없게 만드는 행위	봇이 장바구니에 보관하는 미판매 품목으로 인한 매출 손실 낮은 전환율 장바구니 포기율 증가 부도덕한 중간자가 다른 곳에서 재판매될 때까지 모든 재고를 보유하기 때문에 고객 평판이 훼손됨	장바구니에 보관된 버려진 품목 증가 전환율 감소 재고 부족에 대한 고객 불만 증가	희소하거나 시간에 민감한 품목을 제공하는 비즈니스: • 항공사 • 티켓 • 리테일 • 의료
스캘핑	실제 소비자에 비해 부당한 이점을 얻고 제한된 가용성 및/또는 선호되는 상품/서비스를 얻기 위해 봇을 사용하는 것	고객 평판 손상 웹사이트 성능을 저하시켜 브라운아웃 또는 다운타임을 야기하고 수익 손실을 초래 봇이 추가 품목을 위해 정기적으로 돌아오지 않기 때문에 수명 가치(LTV)가 낮음 봇이 추가 품목을 구매하는 경향이 있는 정당한 소비자와는 반대로 단일 제품을 타겟으로 하기 때문에 평균 장바구니 가치(ABV)가 낮음	설명되지 않는 웹사이트 속도 저하 및 다운타임 (보통 공격적인 스캘핑 봇으로 인해 발생) 전환율 감소 재고 부족에 대한 고객 불만 증가	재고 거부와 유사: • 항공사 • 티켓 • 리테일 예: 스니커즈, 콘솔, 컴퓨터 하드웨어, 한정판 제품. 의료
좌석 스피닝	결제 없이도 봇을 사용하여 종종 최대 24시간 동안 항공편 좌석 확보	판매되지 않은 좌석으로 인한 수익 손실 실제 소비자가 원하는 항공편을 예약할 수 없기 때문에 평판이 훼손됨	출발 시간이 다가오면서, 예약이 꽉 찬 것처럼 보였던 항공편에 갑자기 빈 좌석이 늘어나는 현상이 나타남	항공사

산업별 악성 봇

산업	어떤 비즈니스가 포함됩니까?	악성 봇은 어떤 역할을 합니까?
자동차	렌터카, 제조업체, 대리점, 차량 시장	가격 스크래핑, 데이터 스크래핑, 재고 확인
비즈니스 서비스	부동산, 리테일 플랫폼, CRM 시스템, 비즈니스 지표와 같은 제3자 공급업체	API를 타겟으로 하는 공격, 데이터 스크래핑, 계정 탈취
컴퓨팅 및 IT	IT 서비스, IT 제공업체, 서비스 및 기술 제공업체	계정 탈취, 스크래핑
교육	온라인 학습 플랫폼, 학교, 대학, 대학교	학생 및 교수진에 대한 계정 탈취, 수업 가용성, 독점 연구 논문 및 데이터 스크래핑
엔터테인먼트	스트리밍 서비스, 티켓팅 플랫폼, 제작사, 장소	계정 탈취, 가격 스크래핑, 재고 스크래핑, 스캘핑
금융 서비스	은행, 보험, 투자, 암호화폐	계정 탈취, 카딩, 카드 크래킹, 맞춤형 콘텐츠 스크래핑
음식 및 식료품	식품 배달 서비스, 온라인 식료품 쇼핑, 식음료 브랜드 사이트	신용카드 사기, 기프트 카드 사기, 계정 탈취
게임	온라인 게임, 카지노, 스포츠 베팅	계정 탈취, 배당 스크래핑, 프로모션 남용을 위한 계정 생성
정부	법률 및 정부 웹사이트, 시민 서비스, 주, 지방 자치 단체, 대도시	계정 탈취, 사업자 등록 목록의 데이터 스크래핑, 투표자 등록, 예약 스크래핑 및 일정 수립
의료	보건 서비스, 약국	계정 탈취, 콘텐츠 스크래핑, 예약 가용성을 위해 스크래핑하는 “유용한” 봇
라이프스타일	라이프스타일 매거진, 블로그	독점 콘텐츠 스크래핑
마케팅	마케팅 대행사, 광고 대행사	독점 콘텐츠 스크래핑, 광고 사기, 서비스 거부, 왜곡
뉴스	뉴스 사이트, 온라인 잡지	독점 콘텐츠 스크래핑, 광고 사기, 댓글 스팸
리테일	전자상거래, 시장, 중고품	계정 탈취, 스캘핑, 재고 거부, 신용카드 사기, 기프트 카드 사기, 데이터 및 가격 스크래핑, 분석 왜곡
커뮤니티 및 사회	비영리 단체, 신앙 및 신념, 로맨스 및 관계, 온라인 커뮤니티, LGBTQ, 족보	콘텐츠 및 데이터 스크래핑, 계정 탈취, 계정 생성, 기부 페이지에서 도난당한 신용카드 테스트
스포츠	스포츠 업데이트, 뉴스, 라이브 스코어 서비스	데이터 스크래핑(라이브 스코어, 배당률 등)
통신 및 ISP	통신 제공업체, 모바일 ISP, 호스팅 제공업체	계정 탈취, 경쟁사 가격 스크래핑
여행	항공사, 호텔, 휴가 예약	가격 및 데이터 스크래핑, 예약 대비 조회 비율 왜곡, 서비스 거부, 가격 스크래핑, 계정 탈취, 좌석 스피닝

Imperva 위협 연구

2024년 API 보안 현황



주요 발견

오늘날 모든 웹 트래픽의 71%는 API와 관련이 있습니다.

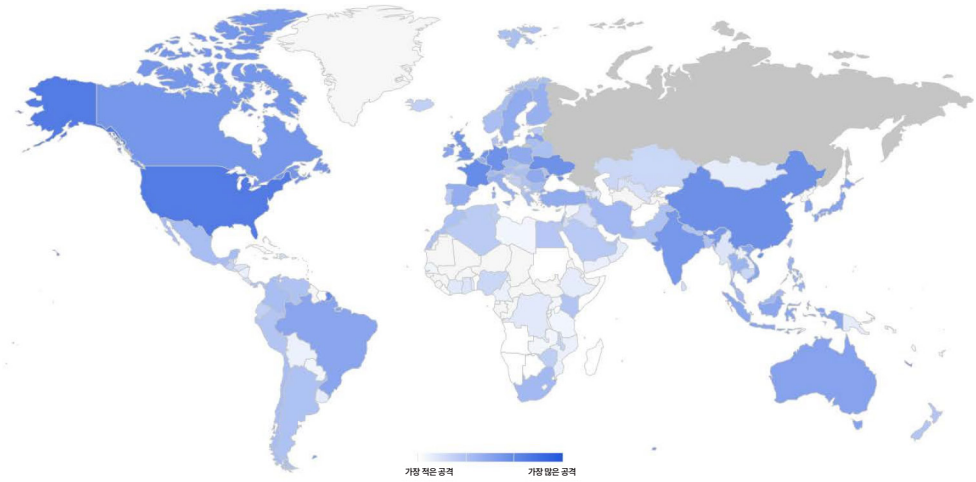
최신 애플리케이션 보안에서 클라이언트 측 보호의 역할

주요 발견

평균적으로 최신 웹 애플리케이션은 언제든지 209개의 클라이언트측 리소스를 로드합니다.

사이버 위협 지수

사이버 위협 지수는 글로벌 사이버 위협 상황을 매달 측정하고 분석한 자료입니다. 이는 사이버 위협 수준을 추적하고 지속적으로 추세를 관찰할 수 있는 이해하기 쉬운 점수를 제공합니다.



Imperva 애플리케이션 보안에 대하여

43

Imperva는 사이버 보안 분야의 리더로서, 조직이 중요한 애플리케이션, API 및 데이터를 어디서나, 규모에 맞게, 그리고 가장 높은 ROI로 보호할 수 있도록 지원합니다. Imperva 애플리케이션 보안 플랫폼은 오탐을 최소화하면서 가장 지능적인 공격을 가장 효과적으로 차단합니다. 높은 효율성 덕분에 조직은 신속하게 온보딩하여 규모에 맞게 자산을 보호할 수 있습니다. Imperva 위협 연구팀과 글로벌 인텔리전스 커뮤니티의 도움으로, Imperva는 진화하는 위협 환경에 앞서 최신 보안, 개인정보 보호 및 규정 준수 전문 지식을 솔루션에 원활하게 통합할 수 있습니다.

Imperva 애플리케이션 보안 플랫폼은 클라우드, 온프레미스 또는 하이브리드 구성 등 어디에 있든 애플리케이션을 심층적으로 보호할 수 있는 최고 수준의 솔루션을 결합합니다:

- 가장 중요한 웹 애플리케이션 보안 위험을 차단하기 위한 온프레미스 및 클라우드 웹 애플리케이션 방화벽(WAF) 솔루션.
- 심층 탐색 및 분류를 사용하여 모든 API를 지속적으로 보호하기 위한 API 보안.
- 오늘날의 가장 정교한 자동화 위협으로부터 웹사이트, 모바일 애플리케이션 및 API를 보호하기 위한 고급 봇 보호 기능.
- 클라이언트 측 공격으로부터 웹사이트를 보호하고 PCI DSS 4.0의 규정 준수를 간소화하기 위한 클라이언트 측 보호.
- 웹사이트, 네트워크 및 DNS에 대한 DDoS 보호를 통해 가동 시간을 보장하면서 비즈니스 연속성을 보장.
- 알려진 취약점 및 제로데이 취약점에 대한 보안을 기본적으로 제공하는 런타임 애플리케이션 자체 보호(RASP).
- 탁월한 속도와 성능으로 전 세계 애플리케이션을 안전하게 전송하기 위한 콘텐츠 제공 네트워크.

악성 봇으로부터 애플리케이션을 보호하려면 지금 바로 애플리케이션 보안 무료 평가판 사용을 시작하십시오.