imperva
a Thales company

2024

Imperva DDoS 위협 환경 보고서

imperva
a Thales company

2024

Imperva DDoS 위협 환경 보고서

목차

2024 Imperva

DDoS 위협 환경 보고서 소개

03

2024년 Imperva DDoS 위협 환경 보고서에서는 2024년 상반기 동안 분산 서비스 거부(DDoS) 공격 활동을 검토하고, 올해 가장 주목할 만한 DDoS 사건에 대한 인사이트를 제공하며, 내년 권장 사항을 제시합니다.

DDoS 공격은 오랫동안 존재했으며 사라질 조짐이 보이지 않습니다. 정치적 이유나 일반적인 핵티비즘 명목으로 일상의 혼란을 야기하려는 사이버 범죄자들은 종종 첫 번째 수단으로 DDoS 공격을 이용합니다.

특히, 기술적 전문 지식이 부족한 개인도 상당한 규모의 공격을 수행할 수 있는 DDoS 도구를 쉽게 구할 수 있게 되면서 공격 규모가 커지고 있습니다. 이러한 도구가 자동화되면서 진입 장벽이 더욱 낮아져 더 많은 사이버 범죄자들이 DDoS 공격에 가담할 수 있게 되었습니다.

국가 행위자나 활동가들이 DDoS 공격과 같은 수단을 통 정치적 메시지를 전달하거나 향후의 행동을 예고하는 경우가 많아 정치적 긴장이 고조되면 DDoS 공격이 확산합니다. 따라서 효과적인 방어 전략을 세우기 위해서는 DDoS 공격의 동기와 그 방법을 알고 있어야 합니다.

이 보고서는 Imperva가 해결한 애플리케이션 및 네트워크 수준 DDoS 공격 사례에 관한 데이터를 기반으로 Imperva 위협 연구소에서 제공하는 인텔리전스를 제공합니다. 또한 올해 전 세계적으로 발생한 DDoS 공격에서 파악된 정보도 제시합니다.

이 보고서에서 제공하는 인사이트와 권장 사항은 진화하는 DDoS 위협 환경에 대비하여 사이버 보안 태세를 강화하려는 조직에 필수적인 정보입니다.

DDoS 공격이란?

04

DDoS(분산 서비스 거부) 공격은 볼륨 기반 공격, 프로토콜 공격, 애플리케이션 계층 공격, 이렇게 세 가지 유형으로 분류합니다.

1990년대 초에 처음 시작된 후, DDoS 공격의 동기는 사이버 폭력이나 복수에서 핵티비즘, 사이버 전쟁, 갈취/랜섬 DDoS(RDoS)로 진화했습니다. 동시에 DDoS 공격에 사용되는 방법도 더욱 발전했습니다.

DDoS 공격은 인터넷에 분산된 여러 대의 장치에서 동시에 시작되며, 공격에 개입된 장치 수가 많아 문제를 해결하기 어렵습니다. 이러한 대규모 DDoS 공격에는 명령 및 제어 센터(Command & Control Center, C&C)에서 원격으로 제어되는 손상된 장치의 네트워크인 봇넷이 사용되는 경우가 많습니다.

DDoS 공격 유형 및 해결 방법에 대한 자세한 목록은 여기에서 확인할 수 있습니다.

공격자는 **정치적 핵티비즘을 포함하여 기타 악의적인 의도**와 다양한 목적으로 DDoS 공격을 감행합니다.

핵심 요약

05

보고서 하이라이트

111%

Imperva가 해결한 DDoS 공격 건수 증가. Imperva는 2024년 상반기에 전년 동기 대비 111% 증가한 DDoS 공격을 성공적으로 해결했으며, 이는 강력한 보안 조치가 필요함을 시사합니다.

470 만 RPS

470만 RPS가 발생한 애플리케이션 계층 DDoS 공격. 2024년 상반기에 가장 주목할 만한 사례 2월에 발생한 애플리케이션 계층 DDoS 공격으로, 초당 요청 수(RPS)가 470만에 달했습니다.

215%

DNS 공격 215% 급증: 2024년 상반기와 2023년 같은 기간을 비교했을 때 DNS 공격 건수는 215% 증가했습니다.

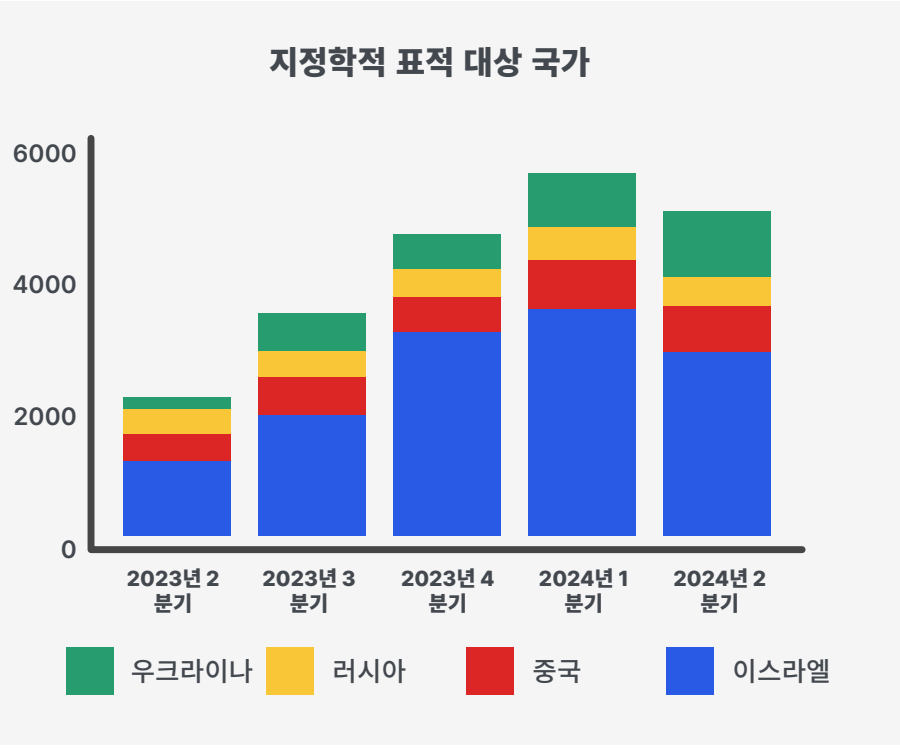
483%

DNS 증폭 공격 규모 증가. 2023년 하반기 DNS 증폭 공격의 평균 규모는 상반기에 비해 483% 증가했습니다.

지정학적 긴장이 DDoS 공격 사례를 증가시키는 원인

지정학적 긴장으로 인해 지난 한 해 동안 DDoS 공격이 크게 증가했습니다. 주요 해당 지역은 다음과 같습니다.

중동 불안	**118%** 이스라엘에 대한 공격 증가	+118%
러시아-우크라이나 갈등	**519%** 우크라이나에 대한 공격 급증	+519%
사이버 보안 경쟁	**84%** 중국에 대한 공격 증가	+84%



89%

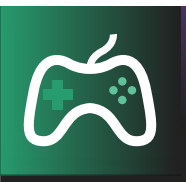
스포츠 경기 전후로 DDoS 공격 증가.
주요 스포츠 경기와 관련된 산업을 표적으로 한 DDoS 공격이 89% 급증했으며, 이는 유명 이벤트의 진행을 방해하여 관심을 받으려는 사이버 범죄자들에게 대형 이벤트가 관심의 대상임을 보여줍니다.

548%

통신 및 ISP에 대한 공격 증가.
통신 및 인터넷 서비스 사업자(ISP) 부문은 인터넷 연결 유지에 중요한 역할을 하는 만큼 서비스 중단에 따른 피해가 크다는 점을 노린 DDoS 공격이 무려 548%나 증가했습니다.

236%

의료 부문에 대한 공격 증가.
의료 기관에 대한 공격이 236% 증가했으며, 이 부문의 취약성과 중요한 의료 서비스 및 환자 데이터에 잠재적으로 치명적인 영향을 미칠 수 있음을 시사합니다.



208%

게임 산업에 대한 공격 증가. 온라인 도박 플랫폼을 포함하여 고부가가치 표적인 게임 산업에 대한 공격이 208% 증가했습니다. 이를 통해 중단 사태로 인해 게임 경험뿐만 아니라, 관련 금융 거래에 영향을 미칠 수 있는 취약성이 드러났습니다.

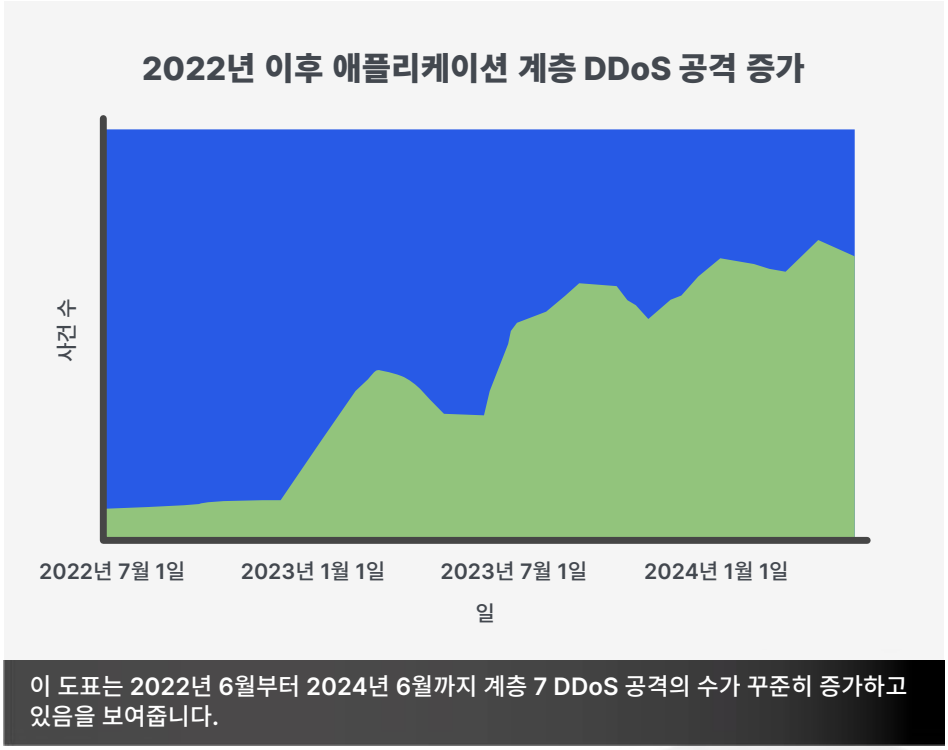
DDoS 공격 횟수와 규모 증가

07

DDoS 공격 횟수 증가

보고된 총 DDoS 공격 건수는 전년도에 비해 111% 급증했습니다. 이러한 현저한 증가세는 위협 환경이 확대되고 있으며 강력한 DDoS 방어 전략이 점점 중요해지고 있음을 보여줍니다.

2월 24일 470만 RPS에 이르는 사태를 위시하여, 애플리케이션 계층 공격은 전년 대비 110% 증가했습니다.



이 도표는 2022년 6월부터 2024년 6월까지 계층 7 DDoS 공격의 수가 꾸준히 증가하고 있음을 보여줍니다.

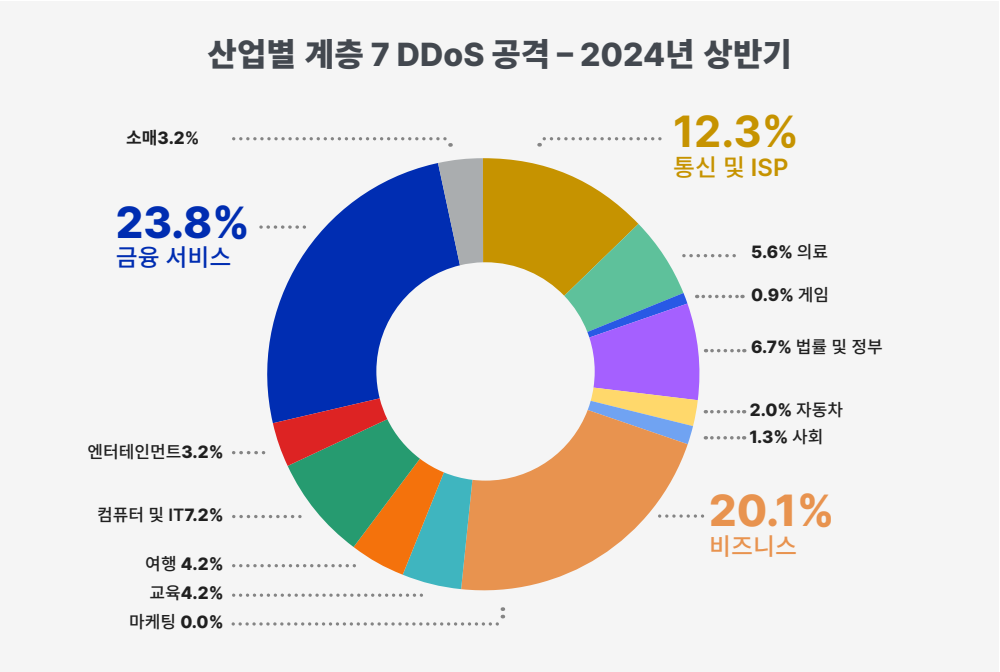
DDoS 공격 규모 확대

DDoS 공격의 규모가 크게 확대되는 추세입니다. 다음은 그중 주목할 만한 사건입니다.

- **2024년 2월:** 가장 심각한 계층 7 DDoS 공격은 인도네시아 게임 사이트를 표적으로 자행되어 캐나다, 인도, 미국의 1,700개 IP에서 470만 RPS가 발생했습니다.
- **2024년 3월,** 루마니아의 한 온라인 리테일 사이트에 대한 400만 건의 RPS 규모의 대규모 공격을 해결한 바 있으며, 이 400만이라는 수치는 루마니아에서 발생한 DDoS 공격의 이전 기록보다 2,000% 증가한 수치입니다.
- **2024년 4월:** 한 중국 엔터테인먼트 사이트가 중국과 미국의 2,600개 IP로부터 거의 5시간 동안 420만 RPS 공격을 받았습니다.

주요 표적 산업

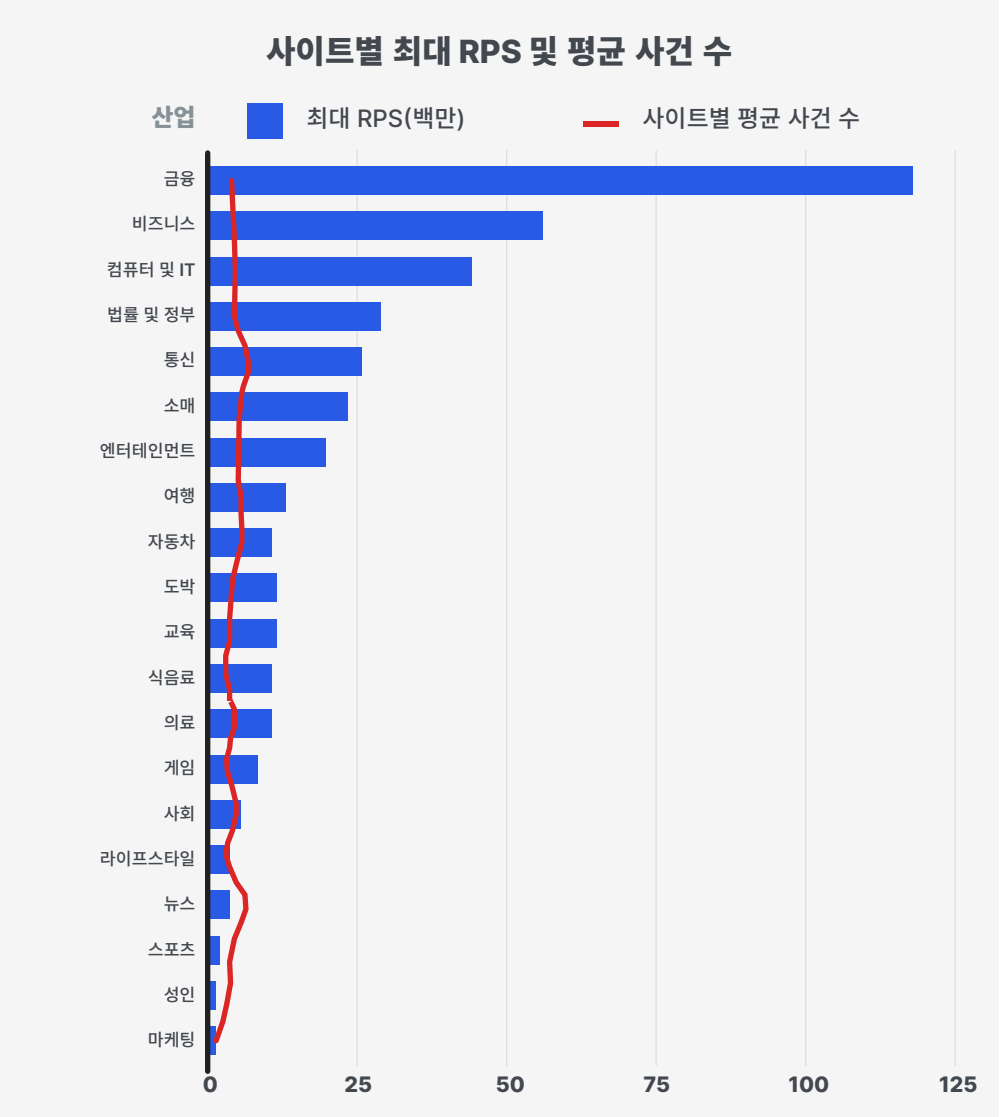
2024년 상반기에 금융 서비스(23.8%), 비즈니스(20.1%), 통신 및 ISP(12.3%) 분야가 가장 많이 공격의 표적이 되었으며, 전체 계층 7 DDoS 공격의 약 60%를 차지했습니다.



가장 강력한 DDoS 공격이 표적으로 삼은 산업

금융 부문은 DDoS 공격자들의 표적 대상 1순위일 뿐만 아니라, 초당 요청 수(RPS) 측면에서도 가장 강력한 DDoS 공격의 표적이 되고 있습니다. DDoS 공격을 시도하는 사이버 공격자는 잠재적 이익이 가장 큰 곳에서 성공하기 위해 더 많은 노력을 기울이는 경향을 보입니다.

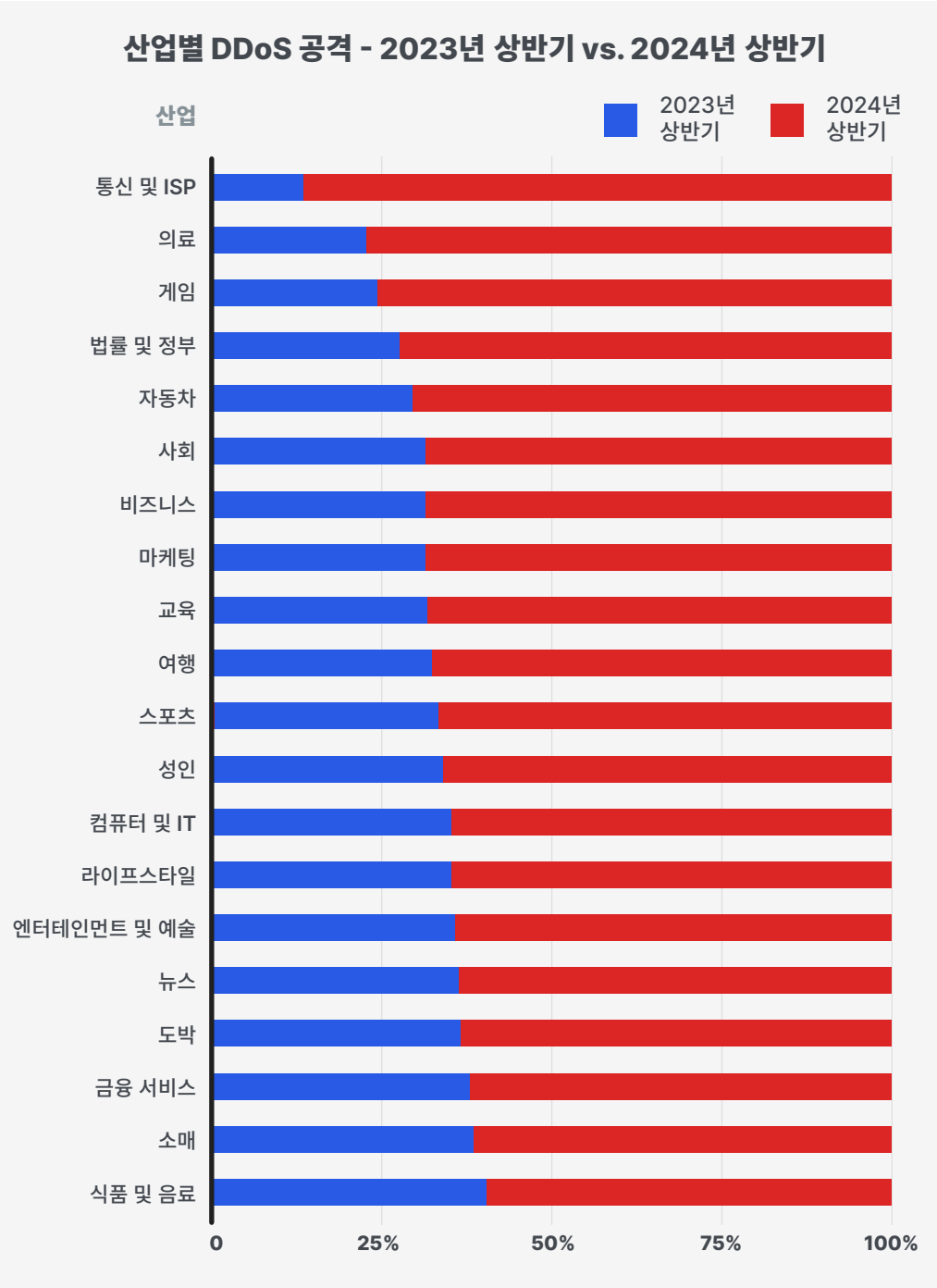
당연히 금융 서비스 부문에 대한 공격이 24년 상반기에 총 1억 1,800만 RPS에 달했으며, 비즈니스와 IT 부문이 각각 2위와 3위를 차지했습니다.



DDoS 공격이 가장 많이 증가한 산업

작년 동기 대비 2024년 상반기에는 여러 산업에서 DDoS 공격이 크게 증가했습니다. 통신 및 ISP 산업은 애플리케이션 계층 DDoS 공격이 548% 증가하면서 전년 대비 가장 높은 증가율을 보였습니다. 의료 산업은 236%, 게임 산업은 208% 공격이 증가했습니다.

인터넷 서비스 사업자(ISP)에 대한 사이버 공격은 조직과 공공 기관에 심각하고 지속적인 위협이 되고 있습니다. ISP는 기업과 개인에게 인터넷 서비스를 제공하여 다양한 인터넷 기반 서비스 제공뿐만 아니라, 경제 분야가 돌아가도록 하는 국가 핵심 인프라입니다. 이러한 이유로 ISP는 최대한의 혼란을 야기하려는 사이버 범죄자들의 주요 표적이 되고 있습니다.

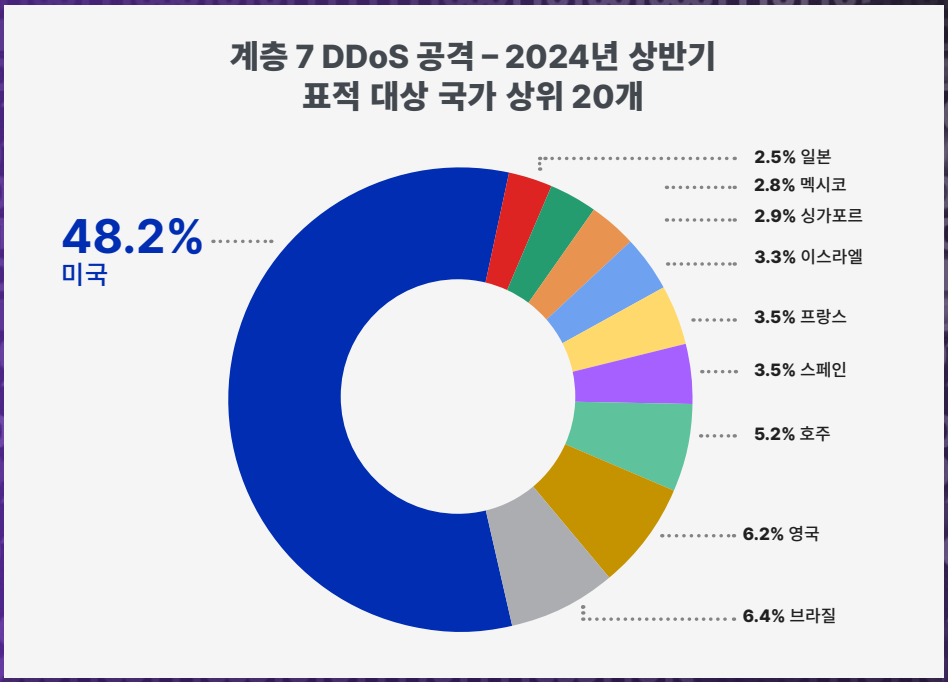


소매업에 대한 DDoS 공격 61% 증가

상위 10위에는 들지 않지만, 소매업에 대한 DDoS 공격은 작년에 비해 61% 정도 증가했으며, 이는 전자 상거래 플랫폼과 온라인 리테일 사이트를 표적으로 하는 사이버 범죄가 꾸준히 증가하고 있음을 시사합니다. 이러한 동향은 사이버 범죄자들이 영업을 방해하고 고객 데이터를 유출하려고 시도하면서 소매업계의 취약성이 커지고 있음을 나타냅니다.

주요 표적 국가

2024 상반기 전체 애플리케이션 계층 공격의 거의 절반이 미국을 표적으로 삼을 정도로 미국은 여전히 DDoS 공격의 주요 표적입니다. 브라질, 영국, 호주에서도 상당한 공격이 발생했지만, 미국에는 미치지 못했습니다.



이 기간 가장 적게 표적이 된 국가 및 지역은 슬로바키아, 세네갈, 몰디브입니다.

발견 및 해결된 새로운 공격 벡터

새로운 공격 벡터는 사이버 범죄자들이 무기를 추가하고 더 복잡하고 정교한 공격을 가능하게 해주기 때문에 항상 중요합니다.

올해에는 두 가지 새로운 주요 애플리케이션 계층 DDoS 공격 벡터가 발견되었습니다.

HTTP/2 신속한 재설정 공격

HTTP/2 신속한 재설정은 2023년에 처음 시도된 비교적 새로운 유형의 공격입니다. HTTP2 프로토콜에 영향을 미치는 CVE-2024-44487로 분류된 서비스 거부 취약점으로, http 클라이언트가 스트림을 열었다가 즉시 취소할 수 있는 취약점입니다. 이러한 열기/취소 작업이 반복적으로 수행되면 서버에 과부하가 걸릴 수 있습니다.

HTTP/2 연속 프레임 공격

최근에는 새로운 유형의 계층 7 DDoS 공격인 **HTTP/2 연속 프레임 공격**이 급증했습니다. 이 공격은 서버에 과부하를 주기 위해 작고 단편적인 요청 스트림을 계속 전송하여 HTTP/2 프로토콜의 취약점을 악용합니다. 이 방법을 사용하면 공격자는 기존의 방어를 우회하고 상대적으로 적은 트래픽으로 큰 혼란을 야기할 수 있습니다. 이러한 정교한 공격이 증가하면서 진화하는 위협 환경과 중요 인프라를 보호하기 위한 더욱 강력한 보안 조치의 필요성이 대두되고 있습니다.

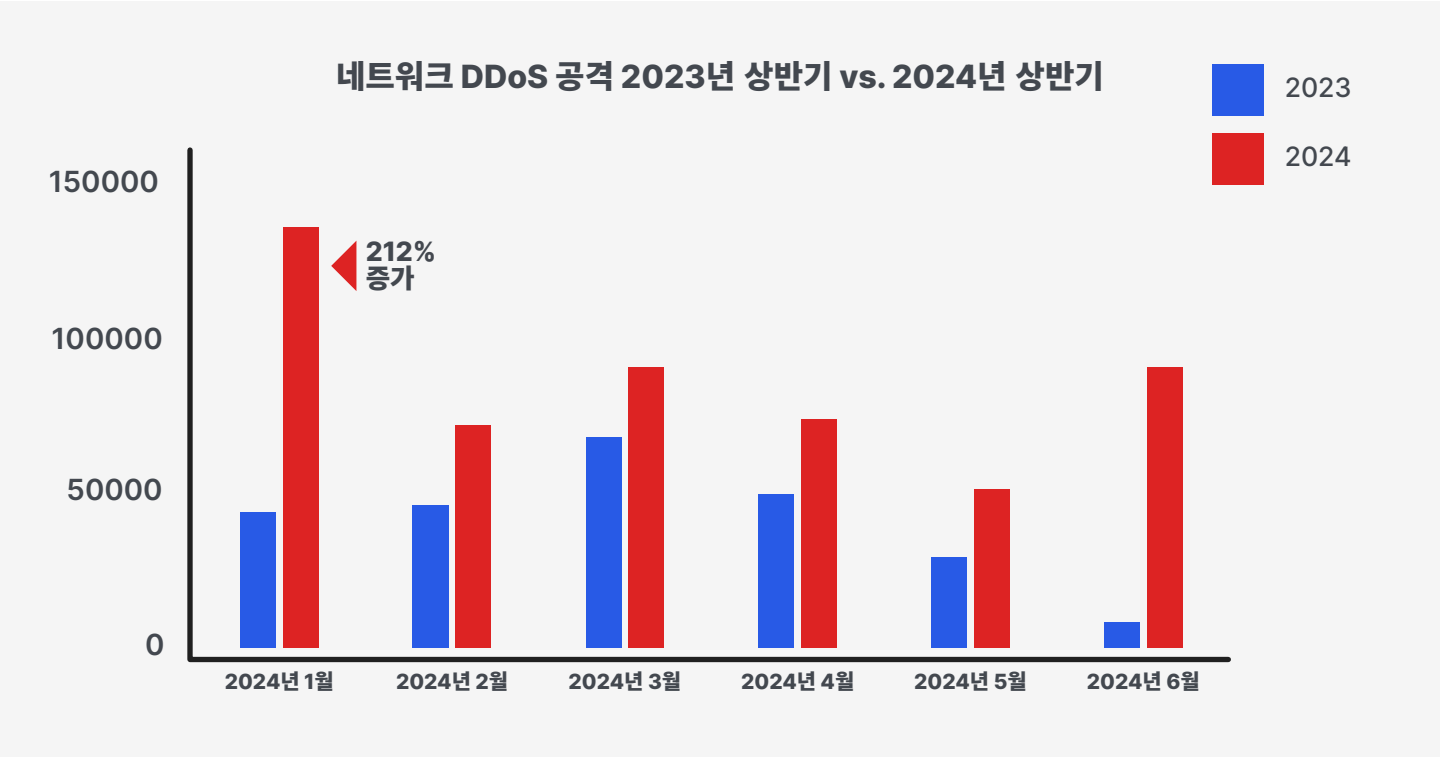
네트워크 계층 DDoS 공격 (계층 3 및 4)

11

전년 대비 네트워크 계층 DDoS 공격 증가

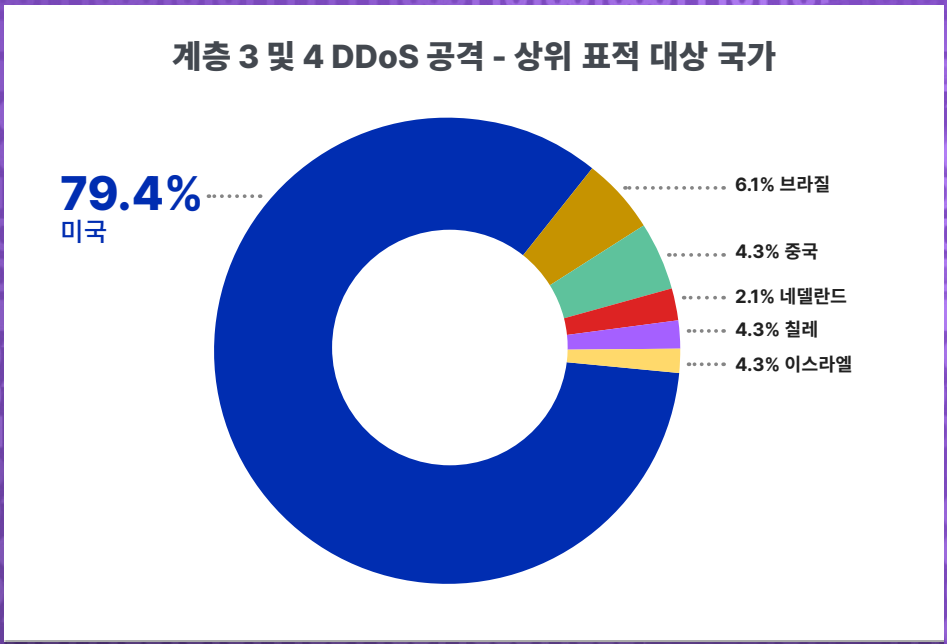
2024년 상반기에 계층 3과 4에 대한 DDoS 공격은 작년에 비해 111% 증가했으며, 2024년 3월에 발생한 4시간 이상 731Gbps에 달하는 공격이 지속된 것이 가장 주목할 만한 사례입니다.

계층 3 및 4 DDoS 공격이 가장 크게 증가한 시기는 2024년 1월로, 전년 동월 대비 212%의 증가율을 보였습니다.

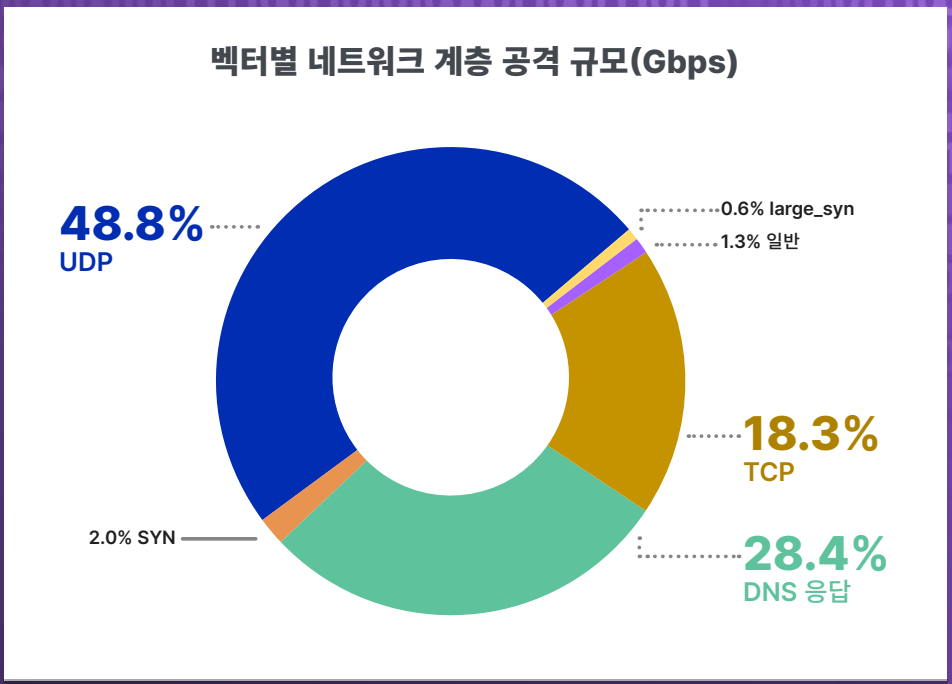


네트워크 계층 DDoS 공격의 주요 표적 국가

2024년 상반기 전체 공격의 약 80%가 미국 내 네트워크를 표적으로 삼았으며, 브라질, 중국, 네덜란드가 그 뒤를 이었습니다.



가장 적게 표적이 된 국가는 남아프리카공화국, 베네수엘라, 바레인입니다.

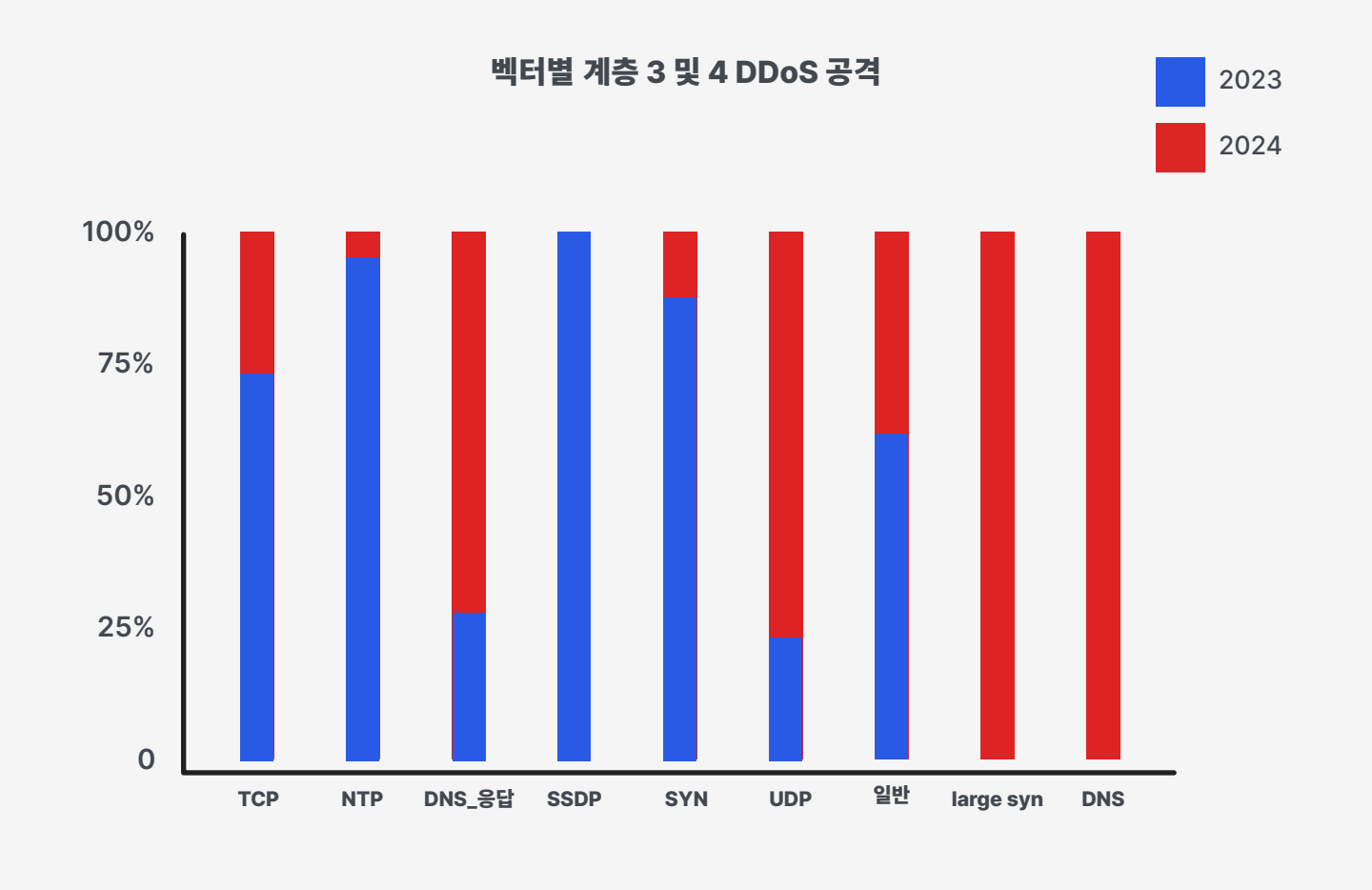


위 2024년 5월 도표를 보면 DNS 응답 공격과 UDP 공격이 네트워크 계층 공격의 대부분을 차지하고 있음을 알 수 있습니다. 두 벡터 모두 매년 큰 폭으로 증가했습니다.[3]

새로운 계층 3 및 4 공격 벡터

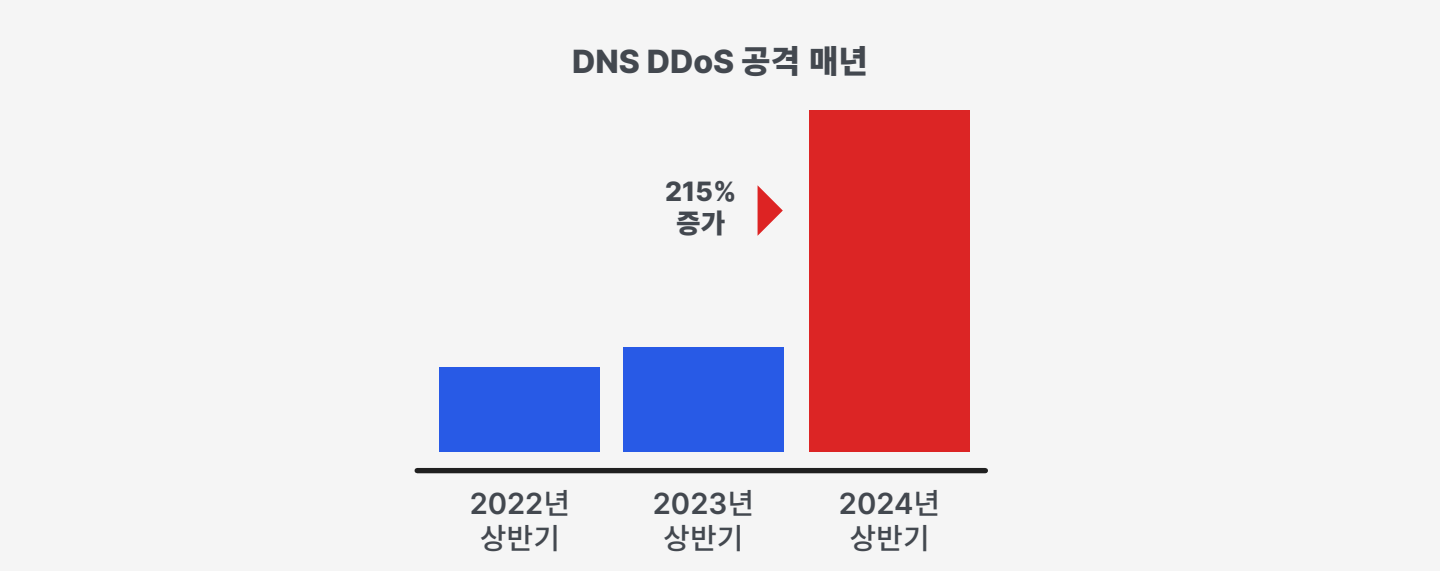
애플리케이션 계층 루프 DoS 공격

The Hacker News에 따르면, 새로 확인된 이 공격 벡터는 레거시(예: QOTD, Chargen, Echo)와 최신(예: DNS, NTP, TFTP)의 UDP 기반 프로토콜을 대상으로 하며 모두 서버가 무한정 통신하도록 만듭니다. CISPA Helmholtz-Center 연구진이 발견한 이 벡터는 약 30만 개의 인터넷 호스트에 영향을 미칠 수 있습니다. 올해 새로운 DDoS 벡터가 발견되었지만, 2024년 상반기에 Imperva각 확인한 바로는, 계층 3 및 4 DDoS 루프 공격은 없었습니다.



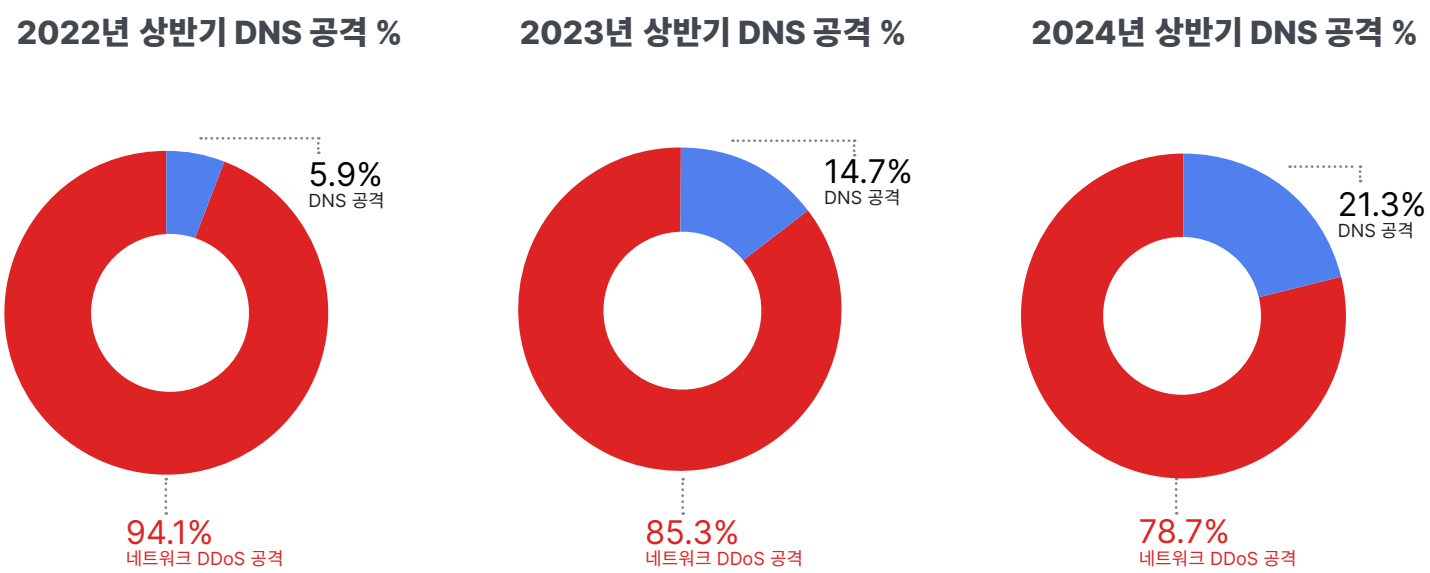
DNS 공격 215% 급증

DNS DDoS 공격이 크게 증가하고 있습니다. 2024년 상반기와 전년 동기를 비교하면 DNS DDoS 공격은 215% 증가했습니다.

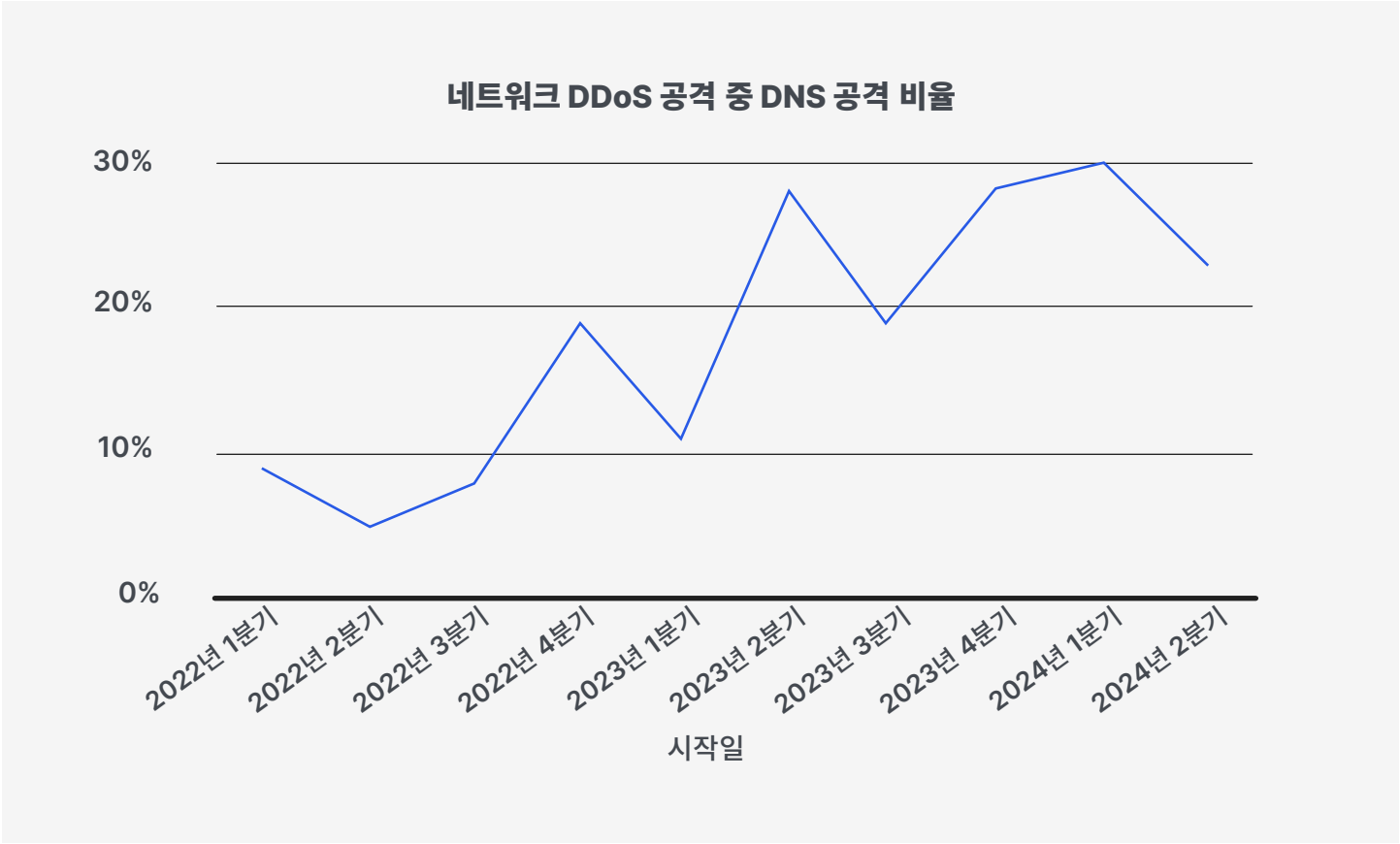


네트워크 DDoS 공격 환경에서 점유율을 높여가는 DNS 공격

벡터로서 DNS 공격은 전체 네트워크 DDoS 공격 환경에서 차지하는 비중이 해마다 증가하고 있습니다. 2022년 상반기 전체 네트워크 DDoS 공격의 6%에 불과했던 DNS DDoS 공격이 2024년 상반기에는 네트워크 DDoS 공격의 21% 이상을 차지했습니다.



아래 도표처럼, DNS 요청 및 DNS 응답 벡터 모두 전체 네트워크 DDoS 공격 건수에서 차지하는 비율이 증가하고 있습니다.

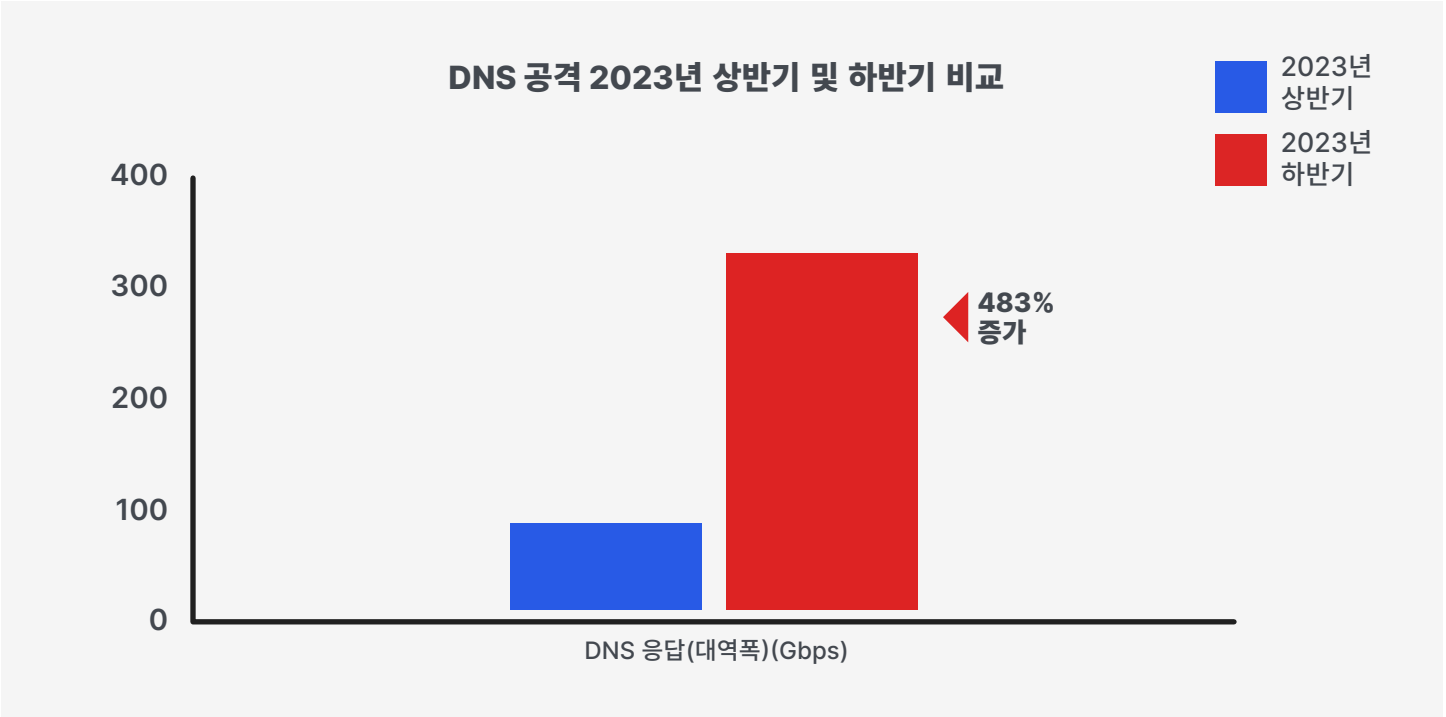


아래 도표처럼, DNS 요청 및 DNS 응답 벡터 모두 전체 네트워크 DDoS 공격 건수에서 차지하는 비율이 증가하고 있습니다.

DNS DDoS 공격 규모 확대

DNS 증폭 공격은 주로 봇넷에서 서버에 쿼리를 폭증시키는 방법으로 서버를 압도하여 공격받은 서버나 네트워크의 서비스 성능이 저하되거나 중단되는 서비스 거부를 일으킬 수 있습니다.

2023년 DNS 증폭 공격은 최대 대역폭 면에서 증가했는데, 2023년 상반기에는 59Gbps에 그쳤지만, 2023년 하반기에는 344Gbps에 달했습니다.



최대 대역폭은 2023년 상반기에는 59Gbps에 도달했으며, 2023년 하반기에는 344Gbps로 증가했습니다.

DNS 서버에 대한 공격의 빈도와 강도가 증가한 이유는 인터넷 기능에서의 핵심적인 역할, 봇넷의 확산, 진화하는 공격 기법, 보안 관리의 취약성 등 여러 요인에 기인합니다. 금융적, 정치적 동기와 보안이 취약한 IoT 기기의 급증 또한 이러한 공격을 촉발하여 DNS 보안을 중요한 문제로 만들고 있습니다.

2023년 상반기의 평균 DNS 증폭 공격 대역폭은 59Gbps였으나, 2023년 하반기에는 344Gbps로 증가하여 483% 상승했습니다.

핵티비즘과 표적 DDoS 공격

핵티비스트들은 중요한 인프라를 교란하기 위해 DDoS 공격을 자주 사용합니다. 최근, 지정학적 긴장과 관련된 러시아 핵티비스트 단체 NoName57(16)이 EU 선거 기간에 유럽 인터넷 인프라를 위협한 사례가 있었다고 **The Register**가 보도한 바 있습니다. 우크라이나 침공 이후 새롭게 등장한 공격자들이 선호하는 전술인 DDoS는 여전히 혼란을 야기하는 강력한 도구입니다.

Anonymous Sudan, NoName57(16)과 같은 집단은 사이버 환경에서 지속되는 위협으로서 계속 진화하고 있습니다. 2024년 초, Imperva는 국가 중요 인프라에 대한 수많은 DDoS 공격에 대응했습니다. 특히 2024년 3월, 유럽 주요 공항에 대한 초당 요청 건수(RPS) 100만 건에 육박하는 공격을 막아낸 바 있습니다. 공항은 국가 중요 허브라는 역할과 기능 중단 시 물류 혼란이 발생할 수 있다는 이유로 주요 공격 대상이 됩니다.

또한 Imperva는 아시아 지역의 통신 기관에 대한 반복적 DDoS 공격을 방어했습니다. 그중 한 사례는 최고 250만 RPS를 기록하기도 했으며, 또 다른 표적 기관은 150만 RPS 규모의 공격을 받았습니다. 지난 2월에는 일본의 한 관공서를 대상으로 발생한 78만 RPS 규모의 공격을 방어하기도 했습니다.

자주 DDoS 공격 표적이 되는 국가 주요 인프라

- 국가 통신 기관
- 방송
- 미디어 공항
- 병원
- 인터넷 서비스 사업자
- 관공서

주요 스포츠 행사에 대한 DDoS 공격

2024년 2월, Imperva는 470만 RPS에 달하는 당해년도 최대 규모의 DDoS 공격을 막아냈습니다. 당시 열리고 있던 AFC 컵 축구 토너먼트를 노린 것으로 보이는 인도네시아 게임 사이트에 대한 공격이었습니다. 핵티비스트들은 공격의 효과를 극대화하기 위해 주요 이벤트를 이용하는 경우가 많은데, 프랑스와 독일은 올해 각각 올림픽과 UEFA 유로 2024 개최국으로서 관련 산업에 대한 위협이 증가하고 있습니다. 일례로 **폴란드의 한 스포츠 채널도 네덜란드와 폴란드의 유로 2024 경기 중계 도중 DDoS 공격**을 받은 바 있습니다.

Imperva의 위협 조사에 따르면 유럽 지역의 여행, 스포츠, 엔터테인먼트, 도박 사이트에 대한 계층 7 DDoS 공격은 작년에 비해 89% 급증했으며, 최고 공격 강도는 150만 RPS에 달했습니다.

주요 스포츠 행사 기간 DDoS 공격이 중요 인프라에 미치는 영향에 대한 자세한 내용은 다음 블로그를 참조하십시오. **다가오는 유럽 하계 스포츠 시즌은 사이버 보안 산업에 어떤 의미를 갖는가?**

2024년 예상되는 DDoS 동향 및 전망

선거 관련 DDoS 공격: 2024년은 세계 각국에서 중요한 선거가 있는 해로, 전 세계 인구의 절반 가까이가 투표소로 향할 것입니다. 선거 기간에는 핵티비스트 활동과 정치적 불안으로 인한 DDoS 공격이 증가하는 경우가 많습니다. 예를 들어, 우크라이나 침공 이후 등장한 친러시아 핵티비스트 그룹 NoName57(16)은 EU 선거 기간에 유럽의 인터넷 인프라를 표적으로 삼았습니다. 이러한 사례는 지정학적 긴장이 어떻게 DDoS 공격의 증가로 이어질 수 있는지를 잘 보여줍니다.

Mirai 봇넷 변종: 2024년 초 당사의 연구에 따르면 웹 취약점을 통해 1,200개 이상의 사이트에 미라이 봇넷 멀웨어가 전달된 것으로 확인되었습니다. Mirai의 궁극적인 목표는 아직 명확하지 않지만, 기록으로 상세히 남아 있는 대규모 DDoS 공격의 전력으로 미루어 향후 잠재적인 위협을 예고하고 있습니다. 여기에서 블로그 전문을 읽어 보세요.

공격 장벽을 낮추는 AI: AI를 통해 숙련된 공격자가 아니어도 새로운 취약점을 신속하게 악용할 수 있습니다. 예를 들어, AI 도구는 정교한 DDoS 공격의 생성과 배포를 자동화하여 초보 해커도 강력한 공격을 실행할 수 있게 해줍니다. 이러한 추세는 Mirai의 잠재적인 새로운 변종 등의 AI 강화 봇넷으로 구동되는 중대한 DDoS 공격 가능성을 높입니다.

DDoS 해킹 그룹의 변화: 사이버 위협 환경도 변화를 거듭하고 있는데, 유명한 DDoS 해킹 그룹인 Anonymous Sudan이 사라진 사례에서도 이러한 변화를 실감할 수 있습니다. 특히 이스라엘 사이트에 대한 공격으로 유명한 이들이 갑작스럽게 사라짐으로써 눈에 띄는 공백을 남겼습니다. 이들은 2024년 2월, 지정학적 긴장 속에서 챗봇의 행동 변화 요구와 함께 수행된 OpenAI의 ChatGPT에 대한 DDoS 공격이 자신들의 소행임을 밝히기도 했습니다. 이들의 활동은 그 이후로 중단되었는데, 아마도 일련의 중요한 사건과 관련이 있어 보입니다.

핵심 요점

- **선거 보안**: 선거 기간에는 잠재적인 DDoS 공격에 대응하기 위해 경계를 강화하고 강력한 사이버 방어 체계를 구축해야 합니다.
- **Mirai 활동:** Mirai와 그 변종으로 인한 위협을 방어하려면 지속적인 모니터링과 보안 조치 업데이트가 반드시 필요합니다.
- **AI 및 사이버 보안:** AI가 사이버 공격자의 장벽을 낮추면서 AI 기반 방어 메커니즘에 대한 투자가 점점 더 중요해지고 있습니다.
- **위협 집단의 진화**: 주요 해커 집단의 활동 변화에 대한 정보를 지속적으로 파악하여 새로운 위협을 예측하고 대비해야 합니다.

DDoS 공격 시 대응 모범 사례

- 적극적으로 대응해야 합니다
- 상시 DDoS 방어 기능을 갖출 수 없다면, 최소한 온디맨드 방어 기능이라도 갖추어야 합니다
- 지금 바로 조사하고 DDoS 솔루션으로 보호합니다
- 만약 공격을 받게 되면, 신속하고 간단한 절차로 안 서비스를 이용할 수 있는 사업자를 선택합니다.
  이런 일이 발생할 경우, 페이지를 즐겨찾기에 추가하여 직접 저희에게 연락하실 수 있습니다.
- 보안팀과 네트워크 팀이 상시 소통해야 합니다
- 전 세계에 진출해 있고 대규모의 정교한 공격을 해결할 역량을 갖춘 평판이 좋은 DDoS 문제 해결 서비스 사업자를 선택합니다
- 빠르고 정확한 문제 해결 역량을 갖추고 최소한의 지연 시간으로 작동하는 솔루션을 선택해야 합니다

Imperva 소개

18

Imperva는 기업의 데이터와 해당 데이터로 연결되는 모든 경로를 보호하는 일을 사명으로 하는 사이버 보안 분야 최고의 기업입니다.

전 세계 고객들은 사이버 공격으로부터 애플리케이션, 데이터, 웹사이트 보호를 위한 보안 업체로 Imperva를 신뢰합니다. Imperva는 엣지, 애플리케이션 보안, 데이터 보안을 결합한 통합 접근 방식을 통해 디지털 여정의 모든 단계에서 기업을 보호합니다. Imperva 위협 연구팀과 글로벌 인텔리전스 커뮤니티를 통해 Imperva는 위협 환경에서 앞서 나가고 최신 보안, 개인정보 보호 및 규정 준수 전문 지식을 솔루션에 원활하게 통합할 수 있습니다.

Imperva DDoS 방어에 대한 자세한 내용은 당사 웹사이트를 참조하십시오.