CLOUDFLARE

Cloudflare 보안 인사이트:
2022년 1분기 DDoS 공격 동향

+82 70 4515 6893 | enterprise@cloudflare.com | www.cloudflare.com

색인

개요 **3**

개요 3

주요 특징 3-4

랜섬 DDoS 공격 5

분기별 랜섬 DDoS 공격 및 위협 5

월별 랜섬 DDoS 공격 및 위협 5

응용 프로그램 계층 DDoS 공격 6

월별 응용 프로그램 계층 DDoS 공격 6

산업별 응용 프로그램 계층 DDoS 공격 7

출발 국가별 응용 프로그램 계층 DDoS 공격 8

대상 국가별 응용 프로그램 계층 DDoS 공격 8

네트워크 계층 DDoS 공격 9

월별 네트워크 계층 DDoS 공격 10

산업별 네트워크 계층 DDoS 공격 11

대상 국가별 네트워크 계층 DDoS 공격 12

수신 국가별 네트워크 계층 DDoS 공격 12-14

공격 벡터 14

새롭게 떠오르는 위협 15

공격 비율별 네트워크 계층 DDoS 공격 16-18

지속 시간별 네트워크 계층 DDoS 공격 18-19

요약 20

개요

이 보고서에는 2022년 1월과 3월 사이에 Cloudflare 글로벌 전역 네트워크에서 관찰된 응용 프로그램 계층 및 네트워크 계층 모두에서의 새로운 데이터 포인트와 인사이트가 포함되어 있습니다.

2022년 1분기에는 응용 프로그램 계층 DDoS 공격이 급증했지만, 네트워크 계층 DDoS 공격의 총 횟수는 줄었습니다. 공격 횟수는 줄었지만, 볼류메트릭 DDoS 공격이 전분기 대비 최대 645% 급증한 것이 확인되었으며, 우리는 2,200억 퍼센트의 증폭 계수로 새로운 제로 데이 반사 공격을 방어 했습니다.

러시아와 우크라이나의 사이버 공간에서 가장 빈번히 목표가 되었던 업종은 온라인 미디어와 방송 미디어였습니다. 아제르바이잔과 팔레스타인 Cloudflare 데이터 센터에서는 DDoS 활동이 엄청나게 늘어나는 것이 목격되었습니다. 이는 봇넷이 내부에서 작동했다는 것을 의미합니다.

주요 특징

러시아와 우크라이나의 사이버 공간

- 1분기에 러시아 내에서 가장 자주 목표가 된 산업은 러시아 온라인 미디어 회사였습니다. 그 다음이 인터넷 산업이었고, 암호화폐와 소매업종이 그 뒤를 이었습니다. 러시아 암호화폐 회사를 대상으로 한 공격은 주로 우크라이나 또는 미국에서 시작됐지만, 또 하나의 주요 공격 출처는 바로 러시아 내부였습니다.
- 러시아 기업을 겨냥한 HTTP DDoS 공격은 대부분 독일, 미국, 싱가포르, 핀란드, 인도, 네덜란드, 우크라이나에서 시작 되었습니다. 여기서 유의할 점은, 사이버 공격 트래픽이 발원한 위치를 식별할 수 있다고 해도 공격자의 위치를 파악하는 것은 또 다른 문제라는 것입니다.
- 우크라이나에 대한 공격은 방송 미디어와 출판 웹 사이트를 대상으로 했으며 더 많은 국가에서 발원하여 더 넓게 분산되었던 것으로 보입니다. 따라서 글로벌 봇넷이 사용되었다고 추측해 볼 수 있습니다. 그렇지만 공격 트래픽의 출처는 대부분 미국, 러시아, 독일, 중국, 영국, 태국이었습니다.

본 리포트를 자세히 읽어보시면, Cloudflare가 러시아 내부에서 발생한 공격들이 외부로 유출되지 않고 즉시 차단하기 위해 어떤 일들을 했는지 확인하실 수 있습니다.

랜섬 DDoS 공격

- 2022년 1월, 공격을 받았던 설문 응답자의 17% 이상이 랜섬 DDoS 공격의 목표가 되었거나 사전에 위협을 받았다고 답했습니다.
- 이 수치는 2월에는 6%로 급격히 감소했고 3월에는 3%로 감소했습니다.
- 이전 몇 분기와 비교할 때 1분기에는 전체적으로 응답자의 10%만이 랜섬 DDoS 공격을 받았다고 답했음을 알 수 있습니다. 이는 전년 대비 28%, 전 분기 대비 52% 감소한 수치입니다.

주요 특징(계속)

응용 프로그램 계층 DDoS 공격

- 2022년 1분기는 지난 12개월 동안 응용 프로그램 계층 공격이 가장 많았던 분기였습니다. HTTP 계층 DDoS 공격이 전년 대비 164%, 전 분기 대비 135% 늘어났습니다.
- 분기를 자세히 살펴보면 2022년 3월에는 HTTP DDoS 공격이 4분기 전체 (1, 3분기도 동일)를 합친 것보다 많았습니다.
- 중국이 4분기 연속 HTTP DDoS 공격 출처로서 1위를 했었으나, 미국이 이번 분기에 선두로 올라섰습니다. 미국 발 HTTP DDoS 공격은 전 분기 대비 6,777%, 전년 대비 2,225% 폭증했습니다.

네트워크 계층 DDoS 공격

- 네트워크 계층 공격은 1분기에 전년 대비 71% 증가했지만, 전 분기 대비로는 58% 감소했습니다.
- 통신 산업이 네트워크 계층 DDoS 공격의 가장 큰 목표가 되었으며 게임 회사와 도박 회사, 정보 기술 산업과 서비스 산업이 그 뒤를 이었습니다.
- 볼류메트릭 공격이 1분기에 증가했습니다. 10Mpps(초당 백만 패킷) 이상의 공격은 전 분기 대비 300% 이상 증가했으며 100Gbps 이상의 공격은 전 분기 대비 645% 증가했습니다.

이 보고서는 Cloudflare의 DDoS 방어 시스템에서 자동으로 감지되어 완화된 DDoS 공격을 기반으로 한 것입니다. 이 시스템의 원리에 대해 자세히 알아보려면 다음을 참고하세요 심층 블로그 게시물.

당사의 네트워크에서 관찰된 DDoS 공격을 당사에서 측정하는 방식에 대한 기록

우리는 공격 동향을 분석하기 위해 “DDoS 활동” 비율을 측정합니다. 이는 우리의 전역 네트워크/특정 지역/특정 범주(예: 산업 또는 대금 청구 국가)에서 관찰된 총 트래픽(공격 트래픽 + 정상 트래픽) 중 공격 트래픽의 비율을 의미합니다. 이런 비율을 고려하여 분석하면 데이터 포인트를 정규화하면서, 예를 들어 더 많은 전체 트래픽을 수신하면서 자연스레 더 많은 공격을 받게 되는 Cloudflare 데이터 센터에 대한 절대 수치에 편향이 반영하지 않고 분석할 수 있게 됩니다.

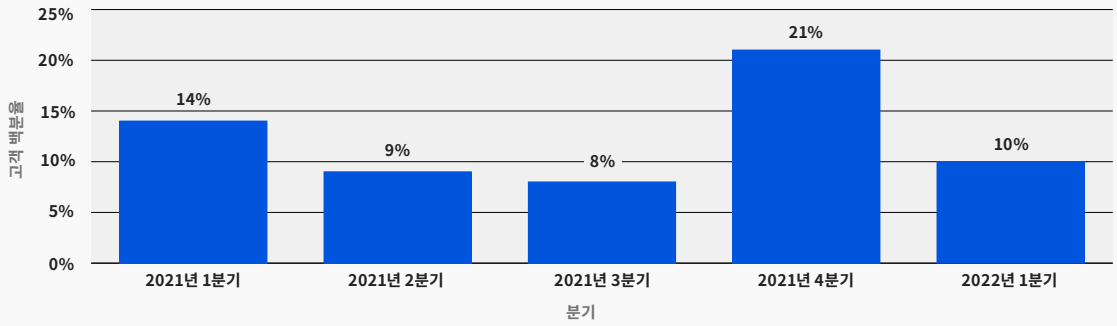
랜섬 공격

우리의 시스템은 지속해서 트래픽을 분석하면서, DDoS 공격이 감지되면 자동으로 완화 조치를 적용합니다. DDoS 공격을 당한 각 고객에게는 자동적으로 서베이가 요청되고, 이를 통해 분석된 내용은 당사에서 공격의 특성을 보다 자세히 파악하고 완화에 성공하는 데 도움이 됩니다.

현재 2년 여에 걸쳐 Cloudflare는 공격을 받은 고객들을 대상으로 설문을 진행하고 있으며, 질문 중 하나는 DDoS 공격을 멈추는 대가로 돈을 요구하는 위협이나 랜섬 노트를 받았는지 여부를 묻는 것입니다. 지난 분기인 2021년 4분기에 우리는 보고된 랜섬 DDoS 공격이 기록적인 수준으로 증가한 것을 목격했습니다(고객 5명 중 1명). 이번 분기에는 랜섬 DDoS 공격이 감소하는 것을 목격했으며 설문 응답자 10명 중 1명만이 랜섬 DDoS 공격을 받았다고 답했습니다. 이는 전년 대비 28%, 전 분기 대비 52% 감소한 수준입니다.

분기별 랜섬 DDoS 공격 및 위협[1]

랜섬 DDoS 공격을 받았다고 답한 응답자의 비율

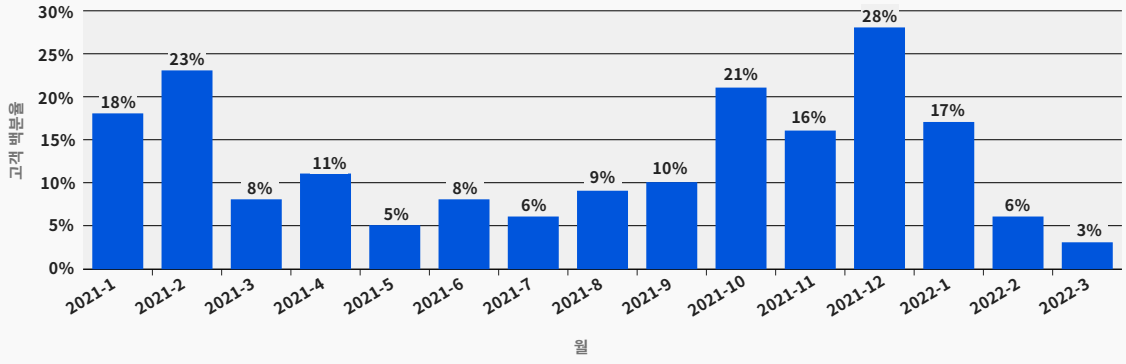


랜섬 DDoS 공격을 받았다고 답했거나
공격에 앞서 위협을 받았다고 답한 응답자의 비율.

이를 월 단위로 분석해 보면 2022년 1월에 1분기에 랜섬 노트를 받았다고 보고한 응답자가 가장 많았음을 알 수 있습니다. 설문 응답자 세 명 중 한 명 꼴로 랜섬 노트를 받은 셈입니다(17%).

월별 랜섬 DDoS 공격 및 위협[1]

랜섬 DDoS 공격에 대한 협박 또는 공격을 받았다고 답한 응답자의 비율

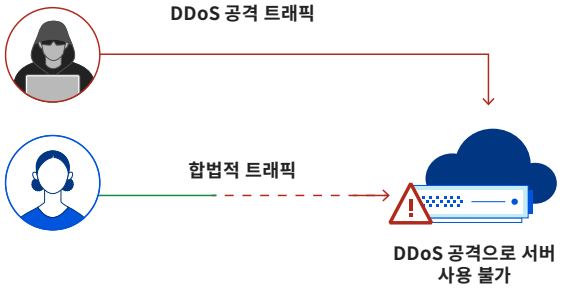


1. 출처: https://radar.cloudflare.com/notebooks/ddos-2022-q1

응용 프로그램 계층 DDoS 공격

응용 프로그램 계층 DDoS 공격 중 특히 HTTP DDoS 공격은 주로 웹 서버가 합법적인 사용자 요청을 처리할 수 없도록 하여 웹 서버를 다운시켜 사용할 수 없게 만드는 것을 목표로 합니다.

서버가 처리할 수 있는 양보다 많은 요청이 쏟아질 경우, 해당 서버는 합법적인 요청의 처리를 중단하게 되고, 경우에 따라서는 충돌을 일으켜 성능이 저하되거나 합법적인 사용자의 서비스도 거부하게 됩니다.



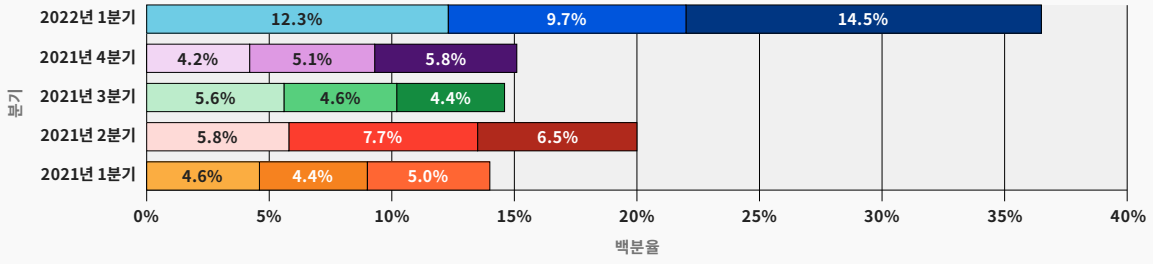
월별 응용 프로그램 계층 DDoS 공격

1분기에는 응용 프로그램 계층 DDoS 공격이 전년 대비 164%, 전 분기 대비 135% 급증했으며, 1분기는 지난 1년 동안 가장 공격이 잦았던 분기였습니다.

2022년 1분기에는 응용 프로그램 계층 DDoS 공격이 새로운 수준으로 증가했습니다. 3월에만 해도 HTTP DDoS 공격이 2021년 4분기 전체 (1,3 분기도 동일)를 합친 것보다 많았습니다.

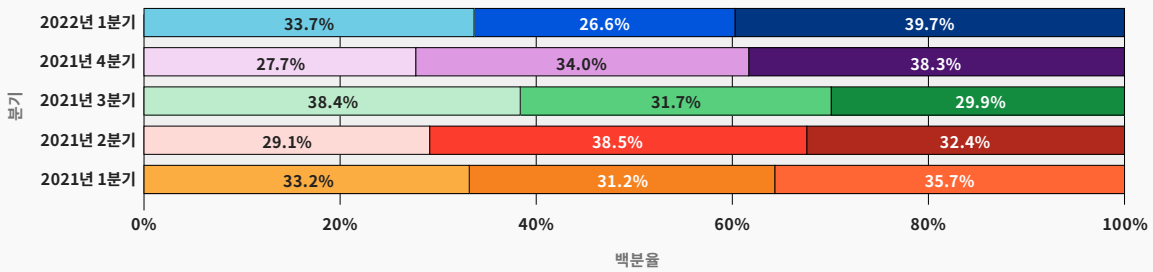
월별 연간 분포[1]

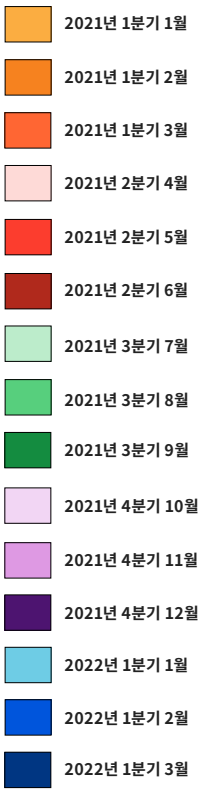
지난 15개월 동안의 월별 응용 프로그램 계층 DDoS 공격에 대한 분포 (연간)



월별 분기 분포[1]

지난 15개월 동안의 월별 응용 프로그램 계층 DDoS 공격에 대한 분포 (분기)





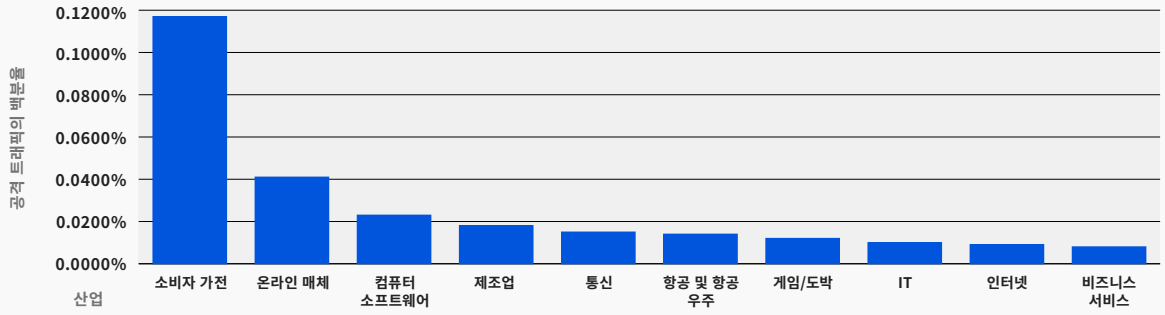
1. 출처: https://radar.cloudflare.com/notebooks/ddos-2022-q1

산업별 응용 프로그램 계층 DDoS 공격

소비자 가전 산업 1분기에 가장 자주 목표가 되었던 산업입니다.

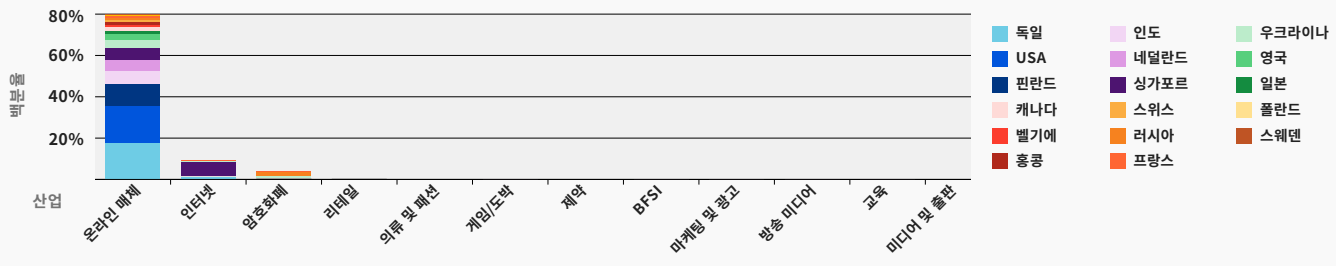
전 세계적으로 소비자 가전 산업은 전 분기 대비 5,086% 증가하여 가장 많은 공격을 받았습니다. 2위는 전 분기 대비 2,131% 증가한 온라인 미디어 산업이었습니다. 3위는 컴퓨터 소프트웨어 기업으로 전 분기 대비 76%, 전년 대비 1,472% 증가했습니다.

산업별 분포[1]
2022년 1분기의 산업별 HTTP DDoS 공격 분포

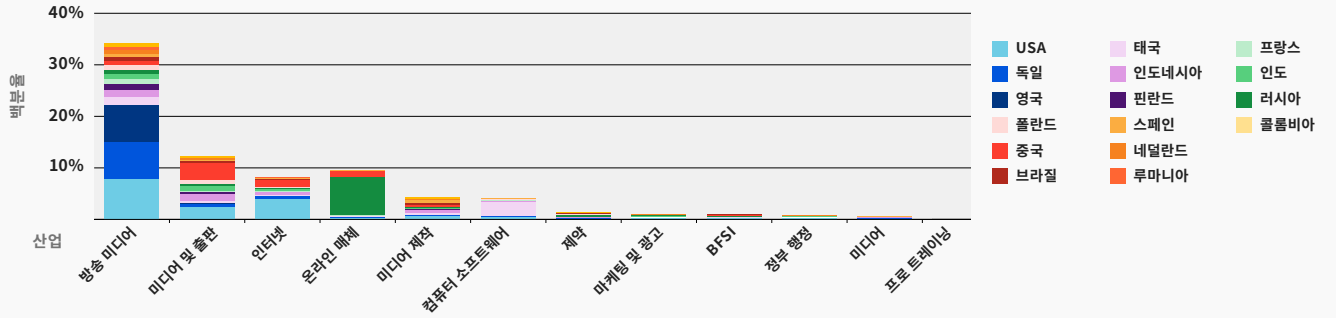


그렇지만 우크라이나와 러시아만 집중해서 보면 방송 미디어, 온라인미디어 기업, 인터넷 기업이 가장 자주 목표가 되었음을 알 수 있습니다. 러시아로 유입되는 개방형 인터넷을 유지하고 공격이 외부로 유출되는 것을 차단하기 위해 Cloudflare에서 어떠한 일을 하고 있는지 자세히 읽어보세요.

산업별 및 출발 국가별 러시아에 대한 공격[1]
2022년 1분기 러시아 산업에 대한 출발 국가별 HTTP DDoS 공격 분포



산업별 및 출발 국가별 우크라이나에 대한 공격[1]
2022년 1분기 우크라이나 산업에 대한 출발 국가별 HTTP DDoS 공격 분포



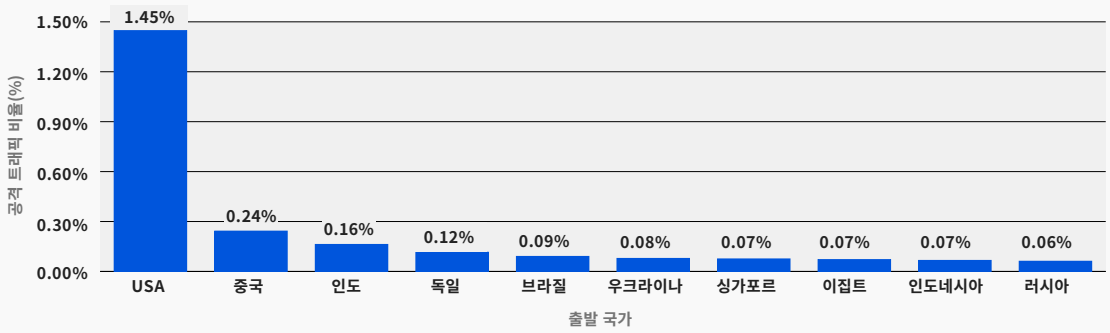
1. 출처: https://radar.cloudflare.com/notebooks/ddos-2022-q1

공격 출처 국가별 응용 프로그램 계층 DDoS 공격

HTTP 공격의 출발 지점을 이해하려면 먼저 공격 HTTP 요청을 생성한 클라이언트가 가진 소스 IP 주소의 지리적 위치부터 살펴봐야 합니다. 소스 IP는 네트워크 계층 공격에서와는 달리 HTTP 공격 시 스푸핑이 불가능합니다. 특정 국가에서 DDoS 활동 비율이 높다는 것은 대개 해당 국가 내에서 봇넷이 작동 중임을 의미합니다.

중국이 4분기 연속으로 HTTP DDoS 공격이 가장 많이 발생한 출발 국가로 밝혀진 이후, 이번 분기에는 미국이 선두에 올라섰습니다. 미국에서 출발한 HTTP DDoS 공격은 전 분기 대비 6,777%, 전년 대비 2,225% 폭증했습니다. 중국이 2위이고, 인도, 독일, 브라질, 우크라이나가 그 뒤를 이었습니다.

출발 국가별 분포[1]
2022년 1분기의 출발 국가별 HTTP DDoS 공격 분포

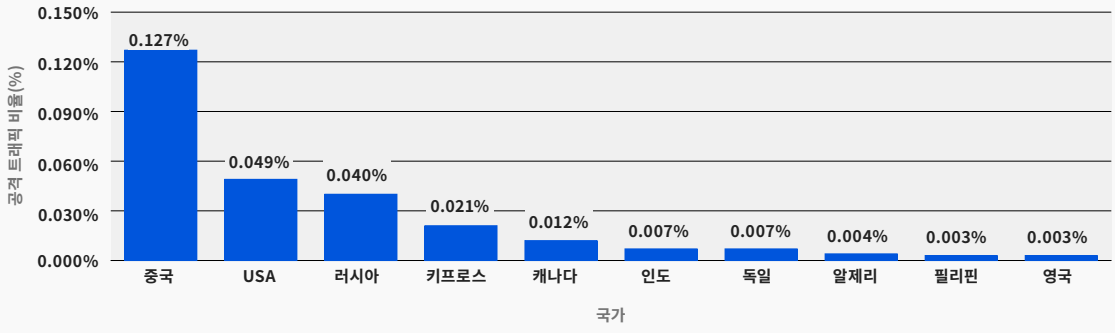


대상 국가별 응용 프로그램 계층 DDoS 공격

어느 국가가 가장 많은 HTTP DDoS 공격을 받았는지 파악하기 위해 우리는 고객의 청구 국가별로 DDoS 공격을 분류해, 이를 모든 DDoS 공격 대비 비율로 분석합니다.

3분기 연속으로 1위를 차지했던 미국이 이번에는 2위로 내려갔습니다. 중국의 기관들이 HTTP DDoS 공격을 가장 많이 받았고 미국, 러시아, 키프로스가 그 뒤를 이었습니다.

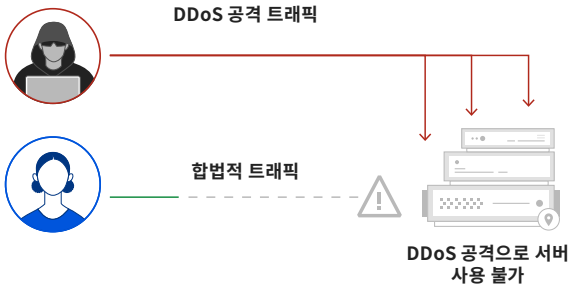
대상 국가별 분포[1]
2022년 1분기 대상 국가별 HTTP DDoS 공격 분포



1. 출처: https://radar.cloudflare.com/notebooks/ddos-2022-q1

네트워크 계층 DDoS 공격

응용 프로그램 계층 공격이 최종 사용자가 액세스하려는 서비스(우리의 경우 HTTP/S)를 구동하는 응용 프로그램(OSI 모델의 계층 7)를 대상으로 하는 반면, 네트워크 계층 공격은 네트워크 인프라(예: 인라인 라우터 및 서버)와 인터넷 링크 자체를 마비시키는 것을 목표로 합니다.



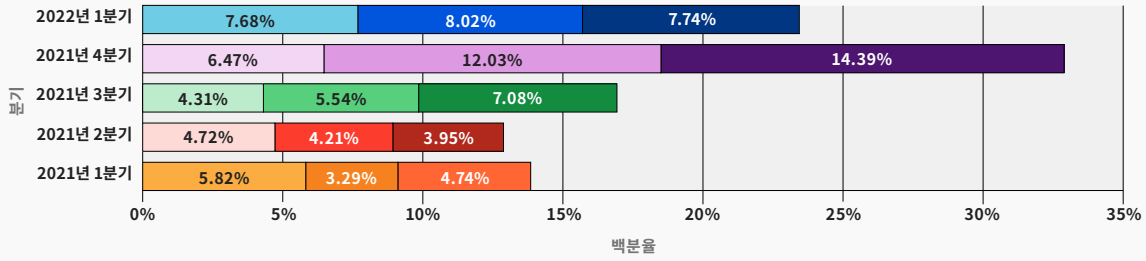
월별 네트워크 계층 DDoS 공격

HTTP DDoS 공격은 1분기에 급증한 반면, 네트워크 계층 DDoS 공격은 실제로 전 분기 대비 58% 감소했지만, 전년 대비로는 여전히 71% 증가했습니다.

1분기를 자세히 살펴보면 네트워크 계층 DDoS 공격의 양이 분기 내내 거의 일관되게 유지되었으며 공격의 약 1/3이 매달 발생한다는 것을 알 수 있습니다.

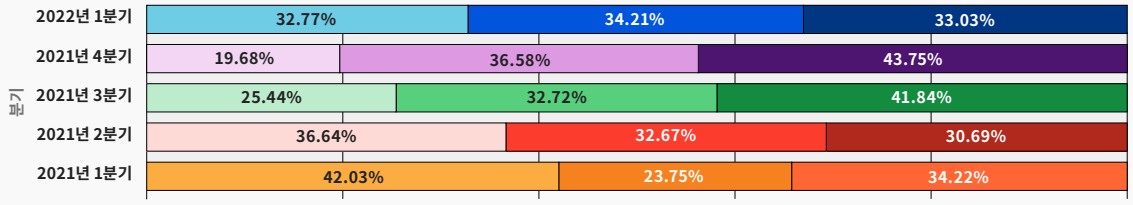
월별 연간 분포[1]

지난 15개월 동안의 월별 네트워크 계층 DDoS 공격에 대한 연간 분포



월별 분기 분포[1]

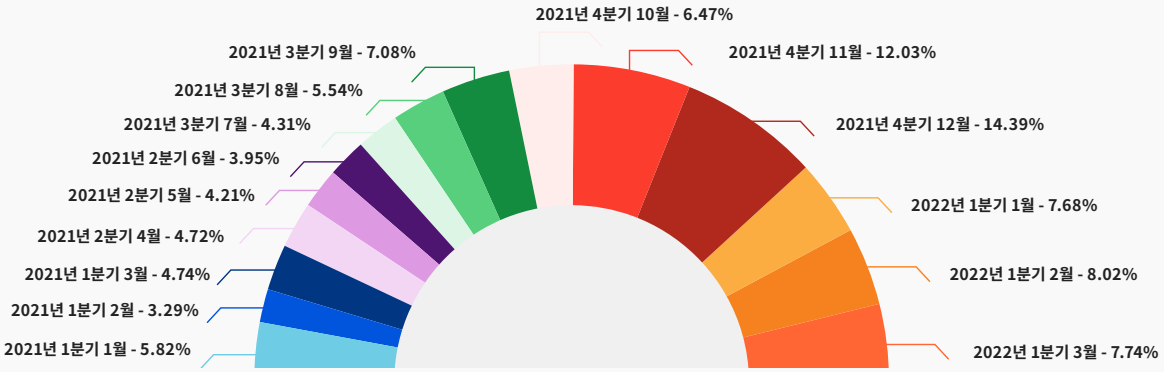
지난 15개월 동안의 월별 네트워크 계층 DDoS 공격에 대한 분기 분포



1. 출처: https://radar.cloudflare.com/notebooks/ddos-2022-q1

월별 네트워크 계층 DDoS 공격(계속)

지난 15개월[1]
지난 15개월 동안의 네트워크 계층 DDoS 공격에 대한 분포



Cloudflare의 제로 데이 증폭 DDoS 공격 완화

이러한 네트워크 계층 DDoS 공격 중에는 Cloudflare에서 자동으로 감지하고 완화하는 제로 데이 DDoS 공격도 있습니다.

3월 초에 Cloudflare의 연구원들은 Mitel 비즈니스 전화 시스템의 제로 데이 취약점을 조사하고 파악하는 데 도움을 주었습니다. 이 취약점은 여러 가지로 악용될 수 있지만, 무엇보다도 공격자가 증폭 DDoS 공격을 시작할 수 있게 해줍니다. 이 유형의 공격을 받은 취약한 Mitel 서버에서는 트래픽이 반사되며, 이러한 특정 경우에는 그 과정에서 전송된 트래픽의 양을 **2200억 퍼센트의 증폭 계수**로 증폭시킵니다. 이에 대한 자세한 내용은 우리의 최근 블로그 게시물에서 확인하세요.

우리는 우리의 네트워크에서 이러한 공격 중 몇 가지를 확인했습니다. 그 중 하나는 Cloudflare Magic Transit 서비스를 이용하는 북미 클라우드 공급자를 목표로 삼았습니다. 공격은 주로 미국, 영국, 캐나다, 네덜란드, 호주와 기타 약 20개국의 100개 소스 IP에서 출발했습니다. 그 공격은 최고 50Mpps(~22Gbps)를 넘어섰으며, Cloudflare 시스템에서 자동으로 감지하고 완화했습니다.

1. 출처: https://radar.cloudflare.com/notebooks/ddos-2022-q1

산업별 네트워크 계층 DDoS 공격

많은 네트워크 계층 DDoS 공격은 Cloudflare의 IP 범위를 직접 대상으로 합니다. 이러한 IP 범위는 우리의 WAF/CDN 고객, Cloudflare 권한 DNS, Cloudflare 공용 DNS 리졸버 1.1.1.1, Cloudflare Zero Trust제품, 본사 사무실 등에 서비스를 제공합니다. 또한 우리의 Spectrum 제품을 통해 고객에게 전용 IP 주소를 할당하고 L3/4 DDoS 방어용 Magic Transit, Magic WAN 및 Magic Firewall 제품을 통해 외부에 Prefixed IP를 노출합니다.

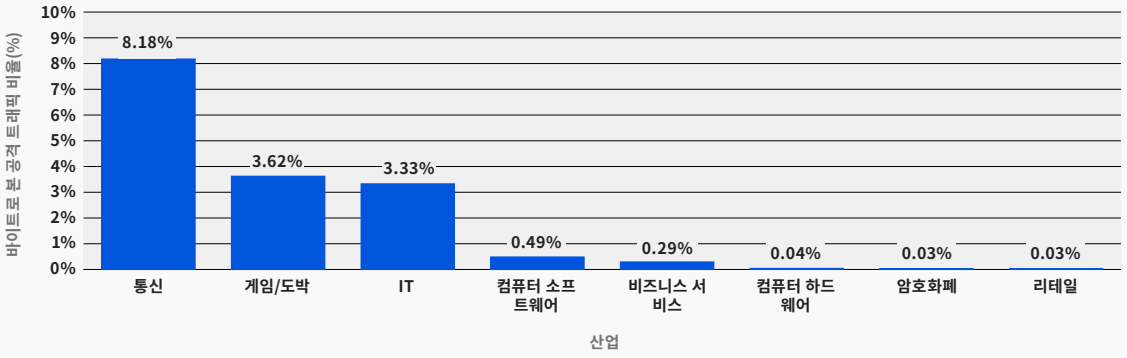
이 보고서에서 우리는 처음으로 Spectrum 및 Magic 제품을 사용하는 고객의 산업에 따라 네트워크 계층 DDoS 공격을 분류하기 시작했습니다. 이 분류를 통해 우리는 네트워크 계층 DDoS 공격을 가장 많이 받는 산업을 파악할 수 있습니다.

1분기 통계를 살펴보면 Cloudflare 고객을 대상으로 실행된 공격 패킷 및 공격 바이트 측면에서 통신 산업이 가장 많이 목표가 되었음을 알 수 있습니다. Cloudflare에서 완화한 모든 공격 바이트의 8% 이상, 그리고 모든 공격 패킷의 10% 이상이 통신 회사를 표적으로 삼았습니다.

그 뒤를 바짝 따르며 게임/도박, 정보 기술 및 서비스 산업이 2위와 3위를 기록했습니다.

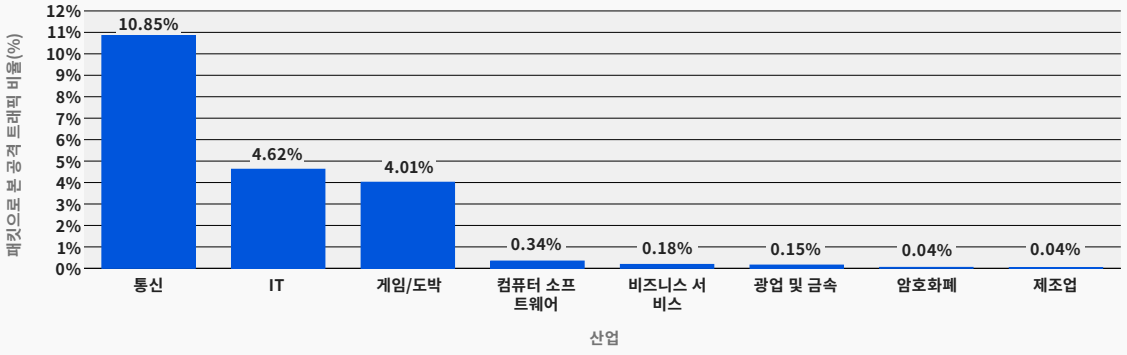
산업별 바이트 분포[1]

산업별 네트워크 계층 DDoS 공격 바이트 분포



산업별 패킷 분포[1]

산업별 네트워크 계층 DDoS 공격 패킷 분포



1. 출처: https://radar.cloudflare.com/notebooks/ddos-2022-q1

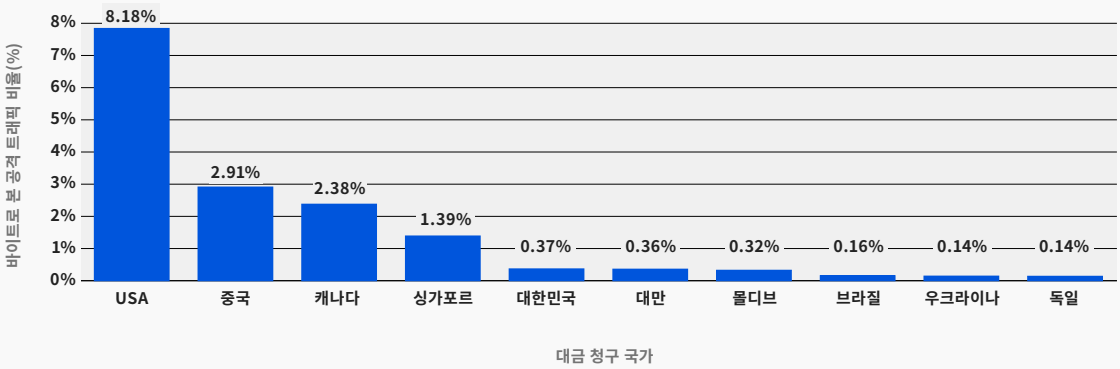
대상 국가별 네트워크 계층 DDoS 공격

고객 업종별 분류와 유사하게, 응용 프로그램 계층 DDoS 공격의 경우와 마찬가지로 고객 청구서 발행 국가별 공격을 버킷팅하여 가장 많이 공격받는 국가를 식별할 수도 있습니다.

1분기 수치를 보면 미국이 가장 높은 비율로 DDoS 공격 트래픽의 표적이 되었음을 알 수 있습니다. 미국은 모든 공격 패킷의 10% 이상, 그리고 전체 공격 바이트의 거의 8%를 차지했습니다. 중국, 캐나다, 싱가포르 순으로 미국의 뒤를 이었습니다.

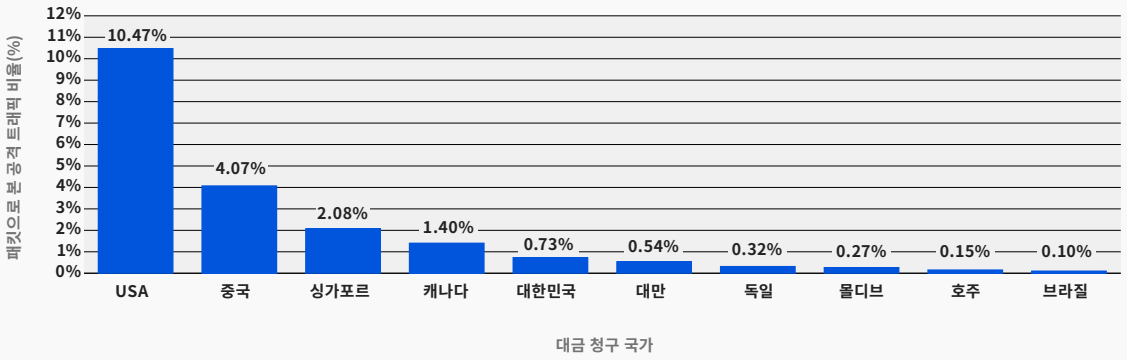
국가별 공격 바이트 분포[1]

대상 국가별 네트워크 계층 DDoS 공격 바이트 분포



국가별 공격 패킷 분포[1]

대상 국가별 네트워크 계층 DDoS 공격 패킷 분포



수신 국가별 네트워크 계층 DDoS 공격

네트워크 계층 DDoS 공격이 어디에서 발생했는지 파악하려고 할 때 응용 프로그램 계층 공격 분석에 사용하는 방법과 같은 방법을 사용할 수는 없습니다. 응용 프로그램 계층 DDoS 공격을 시작하려면 HTTP/S 연결을 설정하기 위해 클라이언트와 서버 간에 성공적인 핸드셰이크가 발생해야 합니다. 성공적인 핸드셰이크를 발생시키려면 공격은 소스 IP 주소를 스푸핑할 수 없습니다. 공격자는 봇넷, 프록시 등의 방법을 사용하여 ID를 난독화할 수 있지만, 공격하는 클라이언트의 소스 IP 위치는 응용 프로그램 계층 DDoS 공격의 소스를 충분히 나타냅니다.

1. 출처: https://radar.cloudflare.com/notebooks/ddos-2022-q1

수신 국가별 네트워크 계층 DDoS 공격(계속)

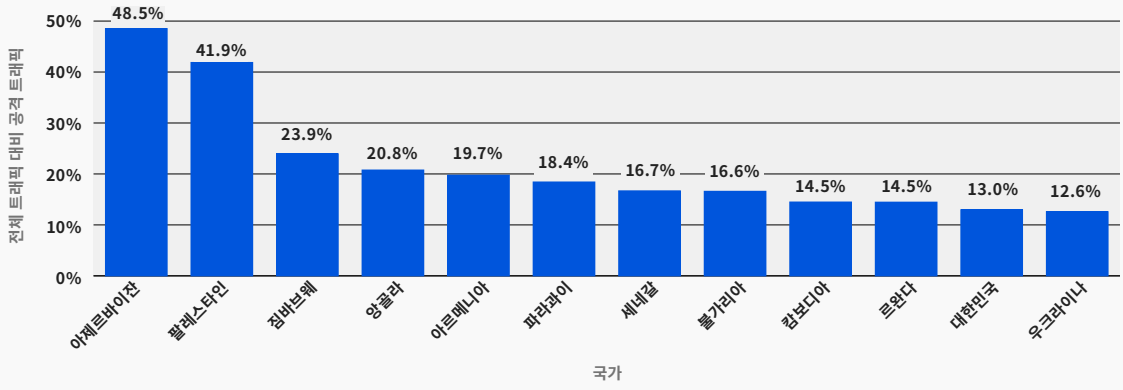
반면에 네트워크 계층 DDoS 공격을 시작하려면 대부분의 경우 핸드셰이크가 필요하지 않습니다. 공격자는 공격 소스를 난독화하고 공격 속성에 임의성을 도입하기 위해 소스 IP 주소를 스푸핑할 수 있습니다. 그럴 경우 단순한 DDoS 방어 시스템으로는 공격을 차단하기가 더 어려워질 수 있습니다. 따라서 스푸핑된 소스 IP를 기반으로 소스 국가를 파생시키면 '스푸핑된 국가'가 됩니다.

이러한 이유 때문에 네트워크 계층 DDoS 공격 소스를 분석할 때는 (잠재적으로) 스푸핑된 소스 IP가 아니라 트래픽이 수집된 Cloudflare 에지 데이터 센터 위치별로 트래픽을 버킷팅하여 공격이 어디에서 발생했는지 파악합니다. 전 세계 270여 개 도시에 우리 데이터 센터가 있기 때문에 보고서에 지리적 위치를 정확하게 나타낼 수 있습니다. 그러나 이 방법도 100% 정확하지는 않습니다. 비용 절감, 혼잡 및 장애 관리 등 다양한 이유로 트래픽이 백홀되고 다양한 인터넷 서비스 공급자 및 국가를 통해 라우팅될 수 있기 때문입니다.

1분기에 아제르바이잔의 Cloudflare 데이터 센터에서 탐지된 공격의 비율은 전 분기 대비 16,624%, 전년 대비 96,900% 증가하여 아제르바이잔이 네트워크 계층 DDoS 활동 비율이 가장 높은 국가가 되었습니다(48.5%).

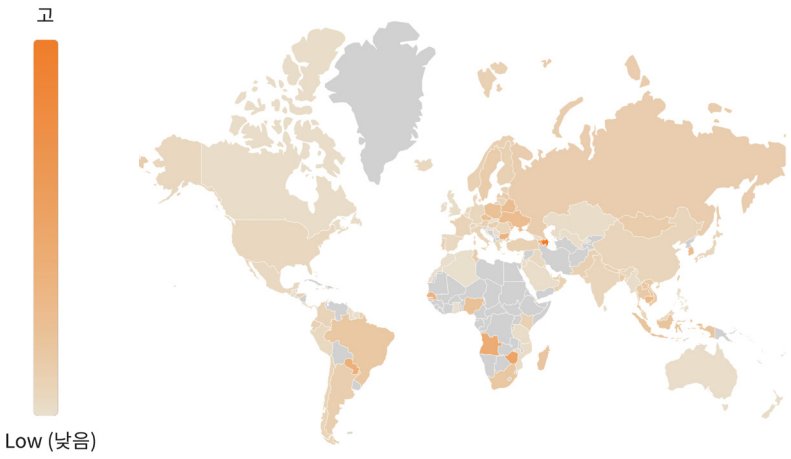
아제르바이잔 데이터 센터 다음은 팔레스타인 데이터 센터였으며, 전체 트래픽의 41.9%가 DDoS 트래픽이었습니다. 이는 전 분기 대비 10,120%, 전년 대비 46,456% 증가한 수치입니다.

공격이 탐지된 국가별 공격 바이트 분포[1]
2022년 1분기 출발 국가별 네트워크 계층 DDoS 공격 분포



1. 출처: https://radar.cloudflare.com/notebooks/ddos-2022-q1

수신 국가별 네트워크 계층 DDoS 공격(계속)



모든 지역 및 국가를 보려면 인터랙티브 지도를 이용하시기 바랍니다.

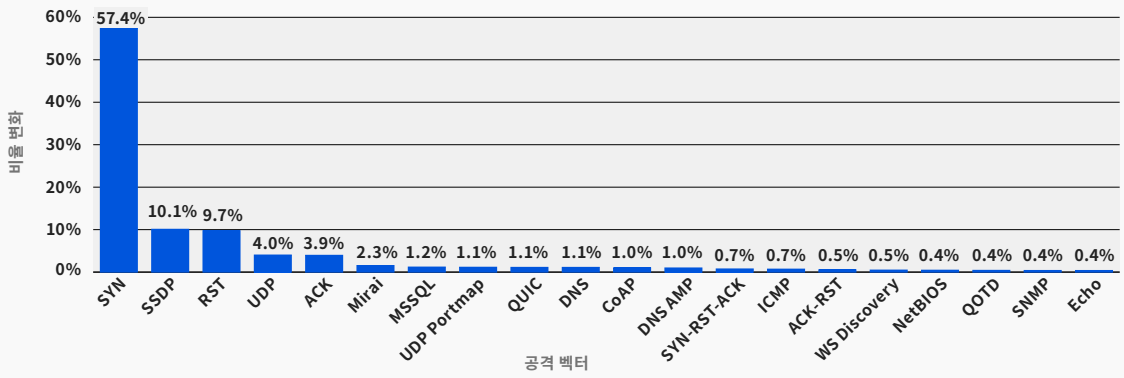
공격 벡터

SYN Flood는 여전히 가장 인기 있는 DDoS 공격 벡터인 반면, 일반 UDP Flood의 사용은 1분기에 크게 감소했습니다.

공격 벡터는 공격자가 DDoS 공격을 실행하기 위해 사용하는 방법, 즉 IP 프로토콜, TCP 플래그 같은 패킷 속성, 폭주 등의 방법을 설명하는 용어입니다.

1분기에 SYN Flood는 전체 네트워크 계층 DDoS 공격의 57%를 차지했으며, 이는 전 분기 대비 69%, 전년 대비 13%의 수준입니다. 2위를 차지한 SSDP 공격은 전 분기 대비 1,100% 이상 급증했습니다. UDP를 통한 RST Flood 및 공격이 그 뒤를 이었습니다. 지난 분기에는 일반 UDP Flood가 2위를 차지했지만, 이번 분기에는 일반 UDP DDoS 공격이 32%에서 3.9%로 전 분기 대비 87% 급감했습니다.

주요 공격 벡터별 분포[1]
2022년 1분기 주요 네트워크 계층 DDoS 공격 벡터



1. 출처: https://radar.cloudflare.com/notebooks/ddos-2022-q1

새롭게 떠오르는 위협

주요 공격 벡터를 식별하면 조직에서 위협 환경을 파악하는 데 도움이 됩니다. 그에 따라 이러한 위협으로부터 보호하기 위해 조직의 보안 상태를 개선하는 데 도움이 될 수 있습니다. 마찬가지로, 아직 공격의 상당 부분을 차지하지 않는 새로운 위협에 대해 학습할 경우 해당 공격이 상당한 위력을 발휘하기 전에 공격을 완화하는 데 도움이 될 수 있습니다.

1분기에 새롭게 떠오른 공격 벡터를 살펴보면 Lantronix 서비스(전 분기 대비 +971%) 및 SSDP 반사 공격(전 분기 대비 +724%)을 반영하는 DDoS 공격의 증가가 두드러집니다. 또한 SYN-ACK 공격은 전 분기 대비 437%, 그리고 Mirai 봇넷 공격은 321% 증가했습니다.

Lantronix Discovery Service의 트래픽을 반사하는 공격자

Lantronix는 폭넓은 제품군을 보유하고 있지만, 특히 사물 인터넷(IoT) 관리용 솔루션을 제공하는 미국 기반 소프트웨어 및 하드웨어 회사로 유명합니다. 이 회사에서 IoT 구성 요소를 관리하기 위해 제공하는 도구 중 하나가 Lantronix Discovery Protocol입니다. 이는 Lantronix 장치를 검색하고 찾는 데 도움이 되는 명령 라인 도구입니다. 이 검색 도구는 UDP 기반이므로 핸드셰이크가 필요하지 않습니다.

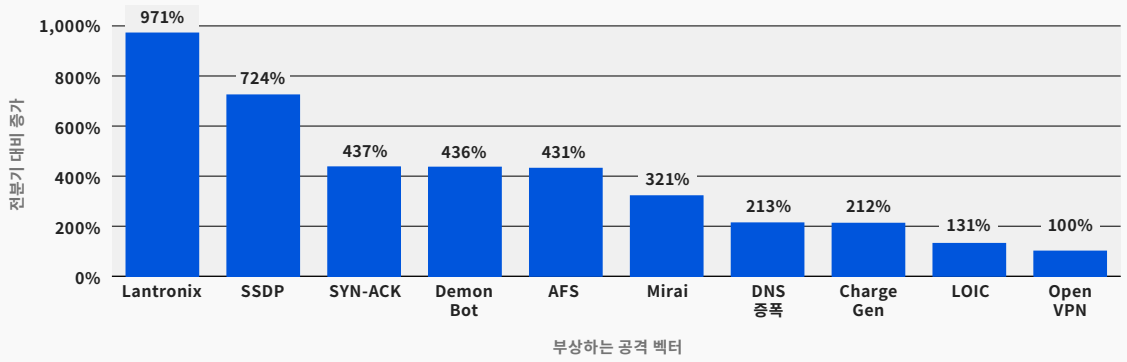
소스 IP는 스푸핑될 수 있습니다. 따라서 공격자는 이 도구를 사용하여 4바이트 요청을 사용해서 공개적으로 노출된 Lantronix 장치를 검색할 수 있으며, 이 요청에 대해서는 차례로 포트 30718에서 30바이트 응답으로 응답됩니다. 모든 Lantronix 장치에서는 피해자의 소스 IP를 스푸핑함으로써 피해자에 대한 응답을 목표로 삼게 되므로 반사/증폭 공격이 발생합니다.

반사 DDoS 공격에 사용되는 Simple Service Discovery Protocol

SSDP(Simple Service Discovery Protocol) 프로토콜은 Lantronix Discovery 프로토콜과 작동 방식은 유사하지만, 네트워크 연결 프린터와 같은 UPnP(Universal Plug and Play) 장치용입니다. 공격자는 SSDP 프로토콜을 남용함으로써 공격 대상의 인프라를 압도하고 인터넷 자산을 오프라인으로 전환하는 반사 기반 DDoS 공격을 생성할 수 있습니다. 여기에서 SSDP 기반 DDoS 공격에 대해 자세히 알아보세요.

부상하는 주요 위협 분포[1]

2022년 1분기의 부상하는 주요 네트워크 계층 DDoS 공격 위협



1. 출처: https://radar.cloudflare.com/notebooks/ddos-2022-q1

공격 비율별 네트워크 계층 DDoS 공격

1분기에는 패킷 전송률과 비트 전송률 측면에서 볼류메트릭 DDoS 공격이 크게 증가하는 것이 확인되었습니다. 10Mpps 이상의 공격은 전 분기 대비 300% 이상, 그리고 100Gbps 이상의 공격은 전 분기 대비 645% 증가했습니다.

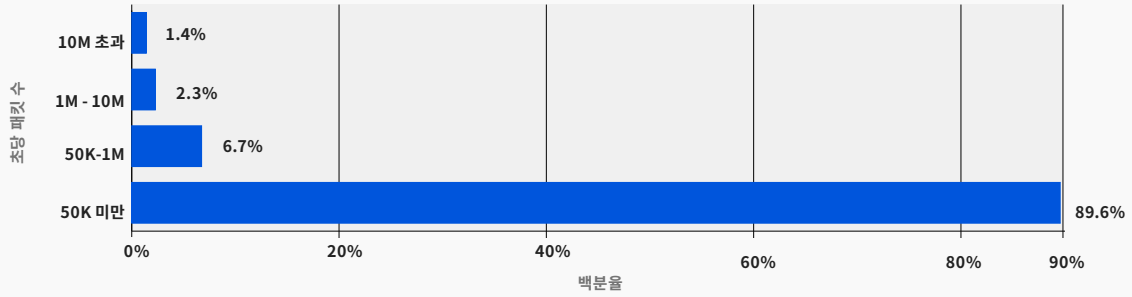
L3/4 DDoS 공격의 규모를 측정하는 방법은 여러 가지입니다. 하나는 공격 트래픽의 양을 비트 전송률(초당 테라비트 또는 초당 기가비트 수)로 측정하는 방법입니다. 또 다른 방법은 총 패킷의 개수를 패킷 전송률(수백만 단위의 초당 패킷 수)로 측정하는 것입니다.

비트 전송률이 높은 공격은 인터넷 링크를 포화시킴으로써 서비스 거부 이벤트를 발생시키려는 시도이며, 패킷 전송률이 높은 공격은 서버, 라우터, 기타 인라인 장비를 마비시키려는 시도입니다. 이러한 장비는 각각의 패킷을 처리하기 위해 일정량의 메모리와 연산 능력을 할당합니다. 따라서 장비에 많은 패킷을 퍼부으면 처리를 위한 리소스를 완전히 고갈시킬 수 있습니다. 이러한 경우에는 패킷의 "드롭(drop)", 즉 해당 장비가 패킷을 처리할 수 없는 상황이 발생합니다. 그 결과 사용자는 서비스 중단 및 서비스 거부를 경험하게 됩니다.

패킷 전송률별 분포

네트워크 계층 DDoS 공격은 대부분 초당 50,000패킷 미만으로 유지됩니다. 50kpps는 Cloudflare의 규모에서는 스펙트럼의 아래쪽에 위치하지만, 여전히 보호되지 않는 인터넷 자산을 손쉽게 중단시키고 표준 기가비트 이더넷 연결까지도 혼잡하게 만들 수 있습니다.

패킷 전송률별 분포[1]
2022년 1분기 패킷 전송률별 네트워크 계층 DDoS 공격 분포

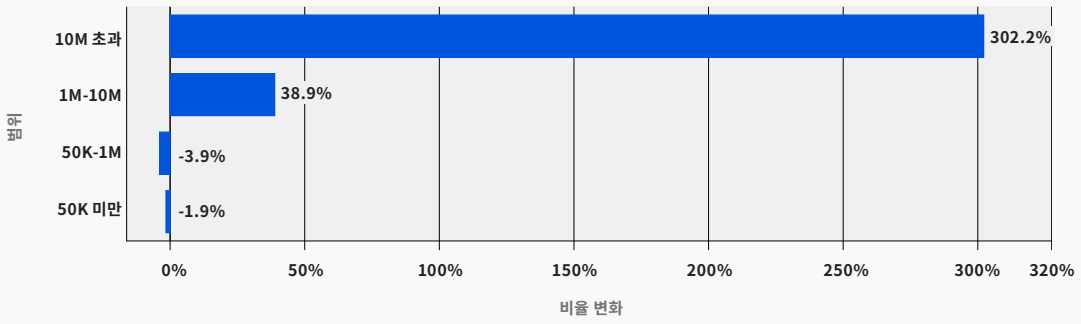


공격 규모의 변화를 살펴보면 10Mpps 이상의 공격이 전 분기 대비 300% 이상 증가한 것이 눈에 띕니다. 유사하게, 1~10Mpps의 공격은 전 분기 대비 거의 40% 증가했습니다.

1. 출처: https://radar.cloudflare.com/notebooks/ddos-2022-q1

공격 비율별 네트워크 계층 DDoS 공격(계속)

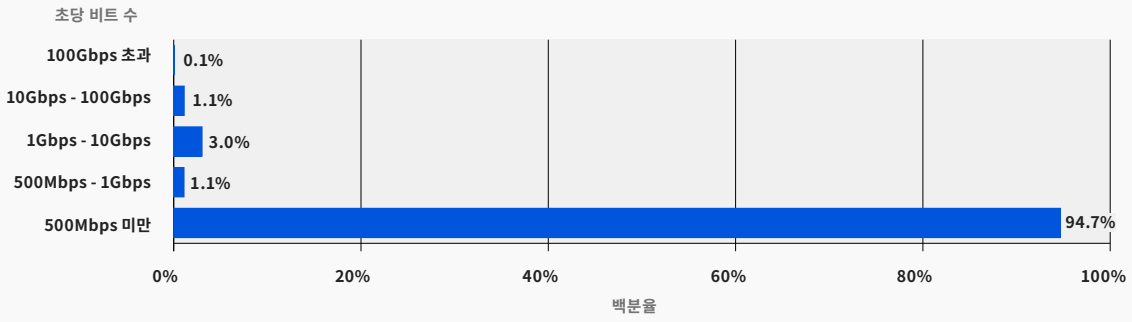
분기별 패킷 전송률 변화[1]
분기에 따른 패킷 전송률별 네트워크 계층 DDoS 공격 분포의 변화



비트 전송률별 분포

1분기에는 네트워크 계층 DDoS 공격이 대부분 500Mbps 미만으로 유지되었습니다. 이 또한 Cloudflare의 규모에서 보면 아주 작은 티끌에 지나지 않지만, 사실 이것만으로도 표준 기가비트 이더넷 연결을 포함하여 용량이 적거나 최소한의 혼잡으로 보호되지 않는 인터넷 자산을 아주 빨리 종료시킬 수 있습니다.

비트 전송률별 분포[1]
2022년 1분기 비트 전송률별 네트워크 계층 DDoS 공격 분포

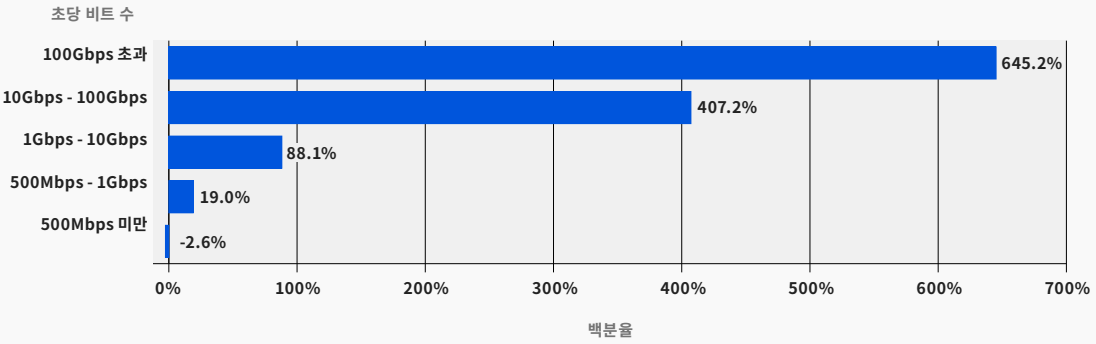


초당 패킷 부문에서 확인된 추세와 유사하게 여기에서도 큰 증가를 볼 수 있습니다. 100Gbps를 초과하여 정점에 이른 DDoS 공격의 양은 전 분기 대비 645% 증가했습니다. 10Gbps~100Gbps에서 정점에 이른 공격은 407% 증가했습니다. 1Gbps~10Gbps에서 정점에 이른 공격은 88% 증가했습니다. 500Mbps~1Gbps에서 정점에 이른 공격까지도 전 분기 대비 거의 20% 증가했습니다.

1. 출처: https://radar.cloudflare.com/notebooks/ddos-2022-q1

공격 비율별 네트워크 계층 DDoS 공격(계속)

분기별 비트 전송률 변화[1]
2022년 1분기 비트 전송률별 네트워크 계층 DDoS 공격 분포



지속 시간별 네트워크 계층 DDoS 공격

대부분의 공격은 지속 시간이 1시간 미만이므로, 자동화된 상시 가동 DDoS 완화 솔루션의 필요성이 다시 한번 강조됩니다.

Cloudflare에서는 시스템에서 공격이 처음으로 감지 및 확인된 시점과 해당 공격 서명이 관찰된 마지막 패킷 사이의 간격을 기록하여 특정 타겟을 노리는 공격의 지속 시간을 측정합니다.

우리는 이전 보고서에서 '1시간 미만의 공격'을 분석하고 더 긴 기간을 다루었습니다. 그렇지만 90% 이상의 경우 공격 기간이 1시간을 넘지 않습니다. 따라서 이 보고서를 시작으로, 우리는 짧은 공격을 세분화하고 세분화 결과를 개선하기 위해 더 짧은 시간 범위로 분류했습니다.

한 가지 유의할 점은 공격이 몇 분 동안만 지속되더라도 공격이 성공하면 그 영향이 초기 공격 지속 시간보다 훨씬 더 오래 지속될 수 있다는 것입니다. 공격이 성공리에 끝나면 IT팀은 서비스를 복구하는 데 몇 시간, 심지어 며칠까지 작업을 해야 할 수도 있습니다.

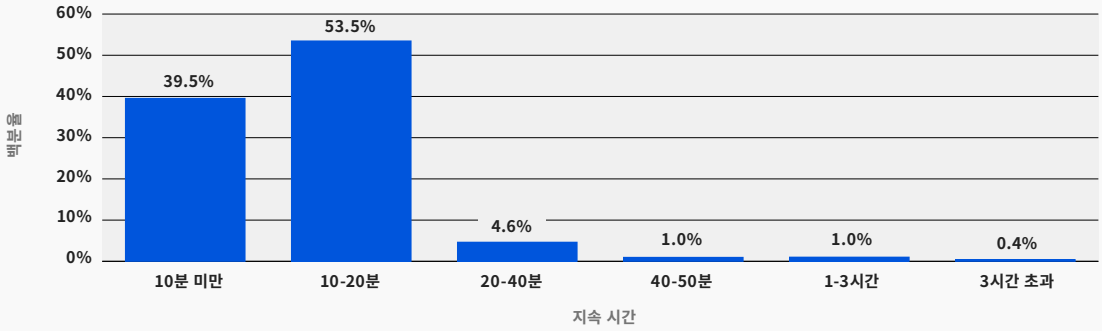
1. 출처: https://radar.cloudflare.com/notebooks/ddos-2022-q1

지속 시간별 네트워크 계층 DDoS 공격(계속)

2022년 1분기의 경우 공격의 절반 이상이 10~20분간 지속되었고, 약 40%는 10분 이내에 종료되었으며, 또 다른 5% 이하는 20~40분간 지속되었고, 나머지 공격은 40분 이상 지속되었습니다.

지속 시간별 분포[1]

2022년 1분기 지속 시간별 네트워크 계층 DDoS 공격 분포



짧은 공격은 감지되지 않을 수 있으며, 막대한 수의 패킷, 바이트 또는 요청을 몇 초 안에 집중시켜 대상을 공격하는 버스트 공격은 특히 감지가 어렵습니다. 이 경우, 보안 분석을 통한 수동 완화에 의존하는 DDoS 방어 서비스로는 적시에 공격을 완화할 기회가 없습니다. 단지 공격 후 분석에서 이를 확인한 다음 해당 공격 지문을 필터링하는 새로운 규칙을 배포하고 다음을 기약할 수 있을 뿐입니다. 마찬가지로, 보안팀이 공격 진행 도중에 트래픽을 DDoS 공급자에게 리디렉션하는 "주문형" 서비스도 해당 트래픽이 주문형 DDoS 공급자에게 라우팅되기 전에 이미 공격이 끝나버리기 때문에 비효율적입니다.

기업들에게는 트래픽을 분석하여 실시간 핑거프린팅을 빠르게 적용함으로써 단기 공격을 차단할 수 있는 자동화된 상시 가동 DDoS 방어 서비스를 사용하는 것을 권장합니다.

1. 출처: https://radar.cloudflare.com/notebooks/ddos-2022-q1

요약

Cloudflare의 사명은 더 나은 인터넷 환경을 구축하는 데 힘을 보태는 것입니다. 더 나은 인터넷이란 더 안전하고 빠르며 믿을 수 있는 인터넷입니다. DDoS 공격이 발생하더라도 말입니다. 이 사명의 일환으로 2017년부터 우리는 모든 고객에게 무제한으로DDoS 방어 기능을 무료 제공하고 있습니다. 여러 해가 지나면서 공격자들이 DDoS 공격을 실행하기가 점점 더 쉬워지고 있습니다. 그렇지만 공격 실행이 더 쉬워졌을지라도, 우리는 모든 조직 역시 그 규모와 상관없이 모든 종류의 DDoS 공격에 맞서 스스로를 더 쉽게 무료로 보호할 수 있도록 하려 합니다.

아직 Cloudflare를 사용하지 않으시나요? 지금 우리의 Free 및 Pro 요금제에 가입해서 귀사의 웹 사이트를 보호하거나 당사에 문의하여 네트워크 전체에 대한 포괄적인 DDoS 방어를 제공하는 Magic Transit을 이용해 보세요.