WHITEPAPER

CLOUDFLARE

Cloudflare-Sicherheitsreport: Entwicklung der DDoS-Bedrohungslandschaft im vierten Quartal 2021

+49 89 2555 2276 | enterprise@cloudflare.com | www.cloudflare.com/de-de/

CLOUDFLARE-SICHERHEITSREPORT: ENTWICKLUNG DER DDOS-BEDROHUNGSLANDSCHAFT IM VIERTEN QUARTAL 2021

Im ersten Halbjahr 2021 haben Ransomware- und Ransom-DDoS (Distributed Denial of Service)-Großangriffe Störungen kritischer Infrastrukturen auf der ganzen Welt (unter anderem bei einem der größten Betreiber von Erdölpipelinesystemen der Vereinigten Staaten) verursacht. Außerdem trat eine Sicherheitslücke in IT-Verwaltungssoftware auf, von der unter anderem Schulen, der öffentliche Sektor, Reiseanbieter und Kreditgenossenschaften betroffen waren.

In der zweiten Jahreshälfte wurden ein wachsender Schwarm eines der leistungsfähigsten Botnetze (Meris) sowie rekordverdächtige HTTP-DDoS-Angriffe und Angriffe auf Netzwerkschicht über das Cloudflare-Netzwerk beobachtet. Hinzu kommt die im Dezember entdeckte Sicherheitslücke Log4j2 (CVE-2021-44228), die es einem Angreifer ermöglicht, Code auf einem entfernten Server auszuführen – wohl eine der schwerwiegendsten Sicherheitslücken im Internet seit Heartbleed und Shellshock.

Aufsehenerregende Angriffe wie die oben genannten sind nur einige Beispiele, die einen allgemeinen Trend zur Intensivierung der Cybersicherheit verdeutlichen. Davon sind alle Arten von Organisationen betroffen, von Technologieunternehmen und Behörden bis hin zu Weinkellereien und Fleischverarbeitungsbetrieben.

Hier sind einige DDoS-Angriff-Trends und Highlights aus dem Jahr 2021 und speziell aus vierten Quartal:

Ransom-DDoS-Angriffe

- Im vierten Quartal nahmen die Ransom-DDoS-Angriffe um 29 % im Jahres- und 175 % im Quartalsvergleich zu.
- Allein im Dezember gab einer von drei Befragten an, Ziel eines DDoS-Angriffs mit Lösegeldforderung gewesen zu sein oder von einem Angreifer bedroht worden zu sein.

DDoS-Angriffe auf Anwendungsschicht

- Das verarbeitende Gewerbe wurde im vierten Quartal 2021 am häufigsten angegriffen und verzeichnete einen Anstieg der Zahl der Angriffe um satte 641 % im Vergleich zum Vorjahr. Die Branchen Unternehmensdienstleistungen und Gaming/Glücksspiel waren die am zweit- und drittstärksten von DDoS-Angriffen auf Anwendungsschicht betroffenen Branchen.
- Zum vierten Mal in Folge führte China in diesem Jahr die Rangliste mit dem höchsten Prozentsatz des von seinen Netzen ausgehenden Angriffs-Traffics an.
- Ein neues Botnetz, Meris, trat Mitte 2021 in Erscheinung und bombardierte beständig Unternehmen auf der ganzen Welt mit einigen der größten HTTP-Angriffen, die jemals verzeichnet wurden – einschließlich eines Angriffs mit 17,2 Mio. Anfragen pro Sekunde, der von Cloudflare automatisch abgewehrt wurde.

DDoS-Angriffe auf Netzwerkschicht

- Im den letzten drei Monaten 2021 waren die Angreifer am aktivsten. Allein im Dezember wurden mehr Attacken verzeichnet als im ersten und im zweiten Quartal des Jahres.
- Anfangs waren die meisten Angriffe klein, aber im zweiten Halbjahr wurden Angriffe im Terabit-Bereich zur Norm. Cloudflare wehrte Dutzende von Attacken mit Spitzenwerten von über 1 Tbit/s automatisch ab. Der größte erreichte knapp 2 Tbit/s und stellte damit alle bisherigen in den Schatten.
- Im vierten Quartal und insbesondere im November wurde eine anhaltende Ransom-DDoS-Angriffskampagne gegen VoIP-Anbieter auf der ganzen Welt verzeichnet.
- Die Angriffe aus Moldawien vervierfachten sich im vierten Quartal 2021 im Vergleich zum Vorquartal und machten Moldawien zum Land mit dem höchsten Anteil an DDoS-Aktivitäten auf Netzwerkschicht.
- SYN-Floods und UDP-Floods waren die häufigsten Angriffsvektoren, wobei neue Bedrohungen wie SNMP-Angriffe gegenüber den vorangegangenen drei Monaten um fast 5.800 % anstiegen.

Dieser Bericht basiert auf DDoS-Angriffen, die von den DDoS-Schutzsystemen von Cloudflare automatisch erkannt und abgewehrt wurden. Mehr über die Funktionsweise erfahren Sie in diesem ausführlichen Blog-Beitrag.

Hinweis zur Messung von über unser Netzwerk beobachteten DDoS-Angriffen

Um Angriffstrends zu analysieren, berechnen wir die „DDoS-Aktivitätsrate“, d. h. den prozentualen Anteil des Angriffs-Traffics am gesamten Datenverkehr, der in unserem globalen Netzwerk registriert wurde. Dieser Messwert ermöglicht es uns, die Datenpunkte zu normalisieren und Verzerrungen zu vermeiden, die sich in den absoluten Zahlen widerspiegeln, z. B. in Bezug auf ein Cloudflare-Rechenzentrum, das insgesamt mehr Traffic verarbeitet und daher wahrscheinlich auch häufiger Ziel von Angriffen wird.

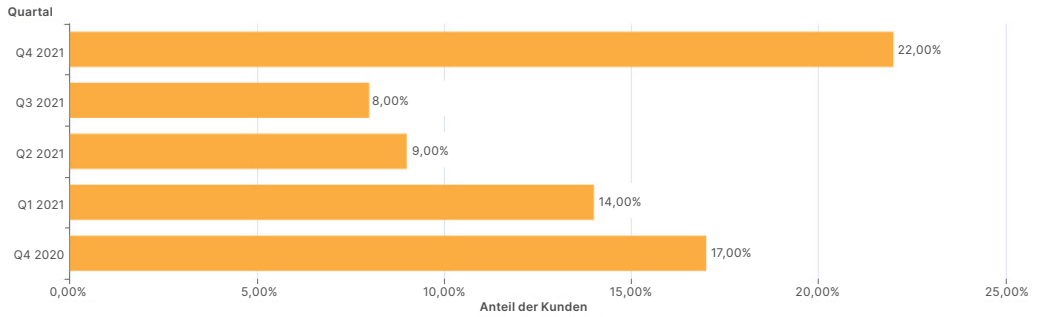
Eine interaktive Version dieses Berichts ist bei Cloudflare Radar verfügbar.

Ransom-Angriffe

Unsere Systeme analysieren ständig den Datenverkehr und wenden automatisch Schutzmaßnahmen an, wenn DDoS-Angriffe entdeckt werden. Jeder von einer DDoS-Attacke betroffene Kunde wird automatisch zur Teilnahme an einer Umfrage aufgefordert, anhand derer wir besser verstehen wollen, wie ein Angriff geartet war und welchen Erfolg die ergriffenen Abwehrmaßnahmen hatten.

Seit über zwei Jahren befragt Cloudflare angegriffene Kunden unter anderem dazu, ob ihnen von Kriminellen angeboten wurde, einen DDoS-Angriff gegen Zahlung eines Lösegelds zu stoppen. Im Zeitraum Oktober bis Dezember 2021 gingen die meisten Meldungen von angedrohten Ransom-Angriffen ein. Diese Attacken erhöhten sich um 29 % im Jahres- und 175 % im Quartalsvergleich zu. Genauer gesagt gab einer von 4,5 Befragten (22 %) an, eine Lösegeldforderung von Angreifern erhalten zu haben.

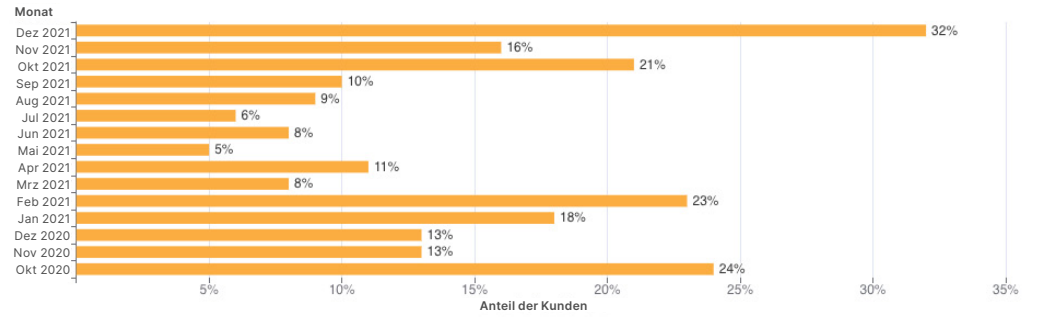
Angedrohte und durchgeführte Ransom-DDoS-Angriffe



Der Prozentsatz der Befragten, die angaben, von einem Ransom-DDoS-Angriff betroffen zu sein oder Drohungen im Vorfeld eines solchen Angriffs erhalten zu haben.

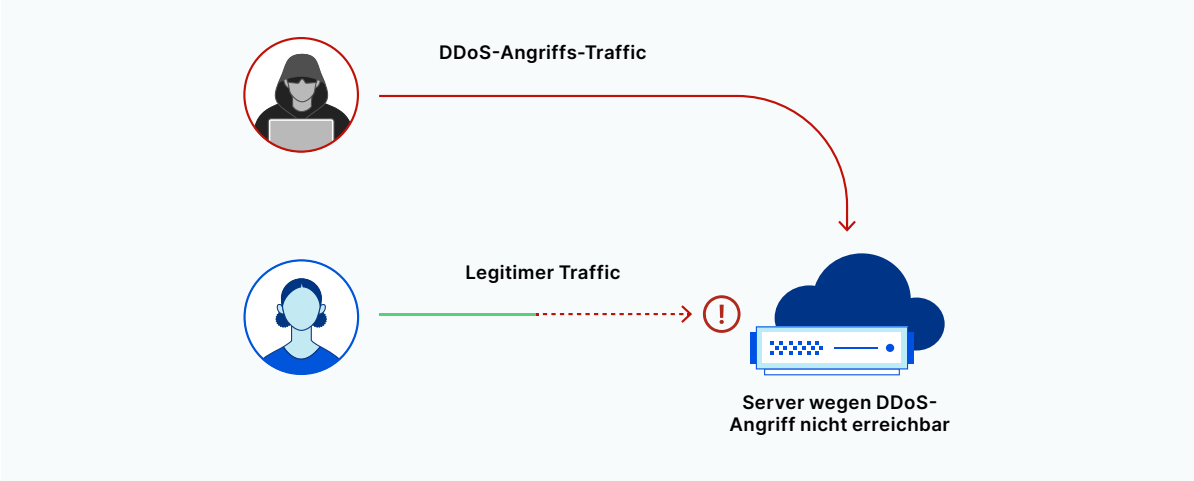
Bei einer Aufschlüsselung nach Monaten zeigt sich, dass der Dezember 2021 mit 32 % der Befragten, die eine Lösegeldforderung erhalten haben, an der Spitze steht – das ist fast einer von drei Befragten.

Angedrohte und durchgeführte Ransom-DDoS-Angriffe aufgeschlüsselt nach Monat



DDoS-Angriffe auf Anwendungsschicht

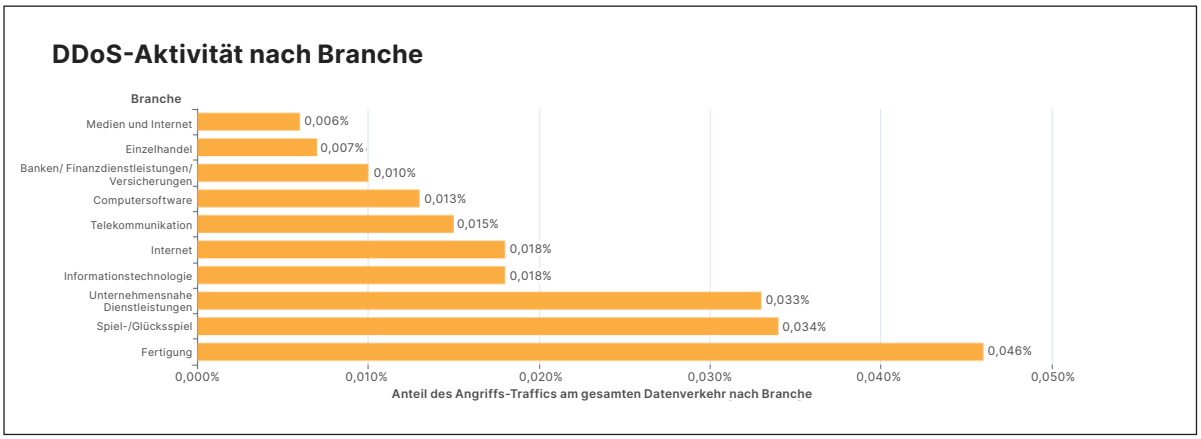
DDoS-Angriffe auf Anwendungsschicht – genauer gesagt HTTP-DDoS-Attacken – sind normalerweise Versuche, einen Webserver zu stören, sodass er keine legitimen Nutzeranfragen mehr verarbeiten kann: Wenn ein Server eine Flut von Anfragen erhält und nicht alle bearbeiten kann, verwirft er legitime Anfragen und stürzt in manchen Fällen sogar ab. Für die User hat das eine schlechtere Performance oder einen Ausfall zur Folge.



DDoS-Angriffe auf Anwendungsschicht aufgeschlüsselt nach Branche

Im letzten Jahresviertel 2021 legten die DDoS-Angriffe auf Unternehmen des verarbeitenden Gewerbes im Vergleich zum Vorquartal um 641 % und die DDoS-Angriffe auf Unternehmen der Dienstleistungsbranche um 97 % zu.

Den meisten Angriffen auf Anwendungsschicht waren in diesem Zeitraum die Fertigungsindustrie, der Bereich unternehmensnahe Dienstleistungen und der Spiel- und Glücksspielsektor ausgesetzt.

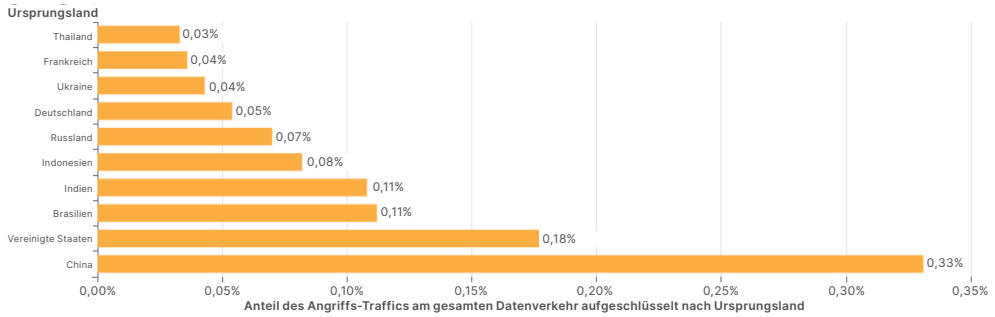


DDoS-Angriffe auf Anwendungsschicht aufgeschlüsselt nach Ursprungsland

Um den Ausgangspunkt der HTTP-Attacken in Erfahrung zu bringen, nutzen wir die Geolokalisierungsinformationen der Ursprungs-IP-Adresse des Clients, von dem die für den Angriff eingesetzten HTTP-Anfragen ausgegangen sind. Anders als bei Angriffen auf Netzwerkschicht können Ursprungs-IP-Adressen bei HTTP-Angriffen nicht gefälscht werden. Wird in einem bestimmten Land ein hoher Anteil an DDoS-Aktivität registriert, zeigt das normalerweise an, dass dort Botnetze aktiv sind.

Das vierte Quartal in Folge verzeichnete China den höchsten Anteil an DDoS-Angriffen inländischen Ursprungs. Von tausend HTTP-Anfragen, die von chinesischen IP-Adressen ausgingen, waren mehr als drei Teil eines HTTP-DDoS-Angriffs. Die USA blieben an zweiter Stelle, gefolgt von Brasilien und Indien.

Aufschlüsselung der DDoS-Angriffe nach Ursprungsland

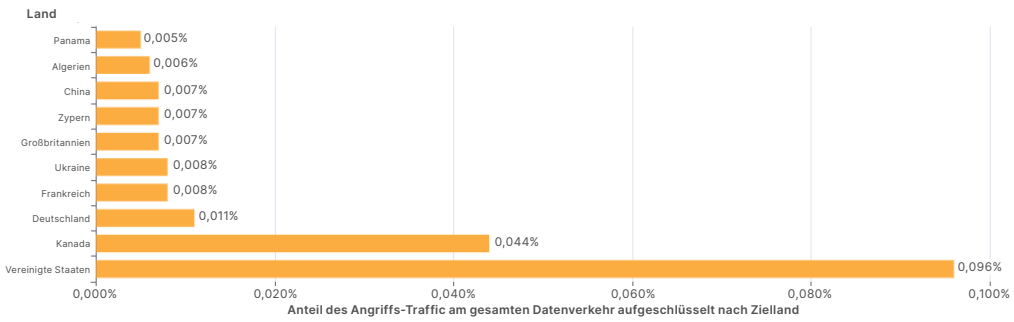


DDoS-Angriffe auf Anwendungsschicht aufgeschlüsselt nach Zielland

Um herauszufinden, auf welche Länder die meisten HTTP-DDoS-Angriffe abzielen, haben wir die Attacken nach den Ländern der Rechnungsadressen unserer Kunden gebündelt und als prozentualen Anteil an allen DDoS-Angriffen dargestellt.

Zum dritten Mal in Folge waren 2021 Unternehmen in den Vereinigten Staaten am stärksten von HTTP-DDoS-Angriffen betroffen, gefolgt von Kanada und Deutschland.

Aufschlüsselung der DDoS-Angriffe nach Zielland



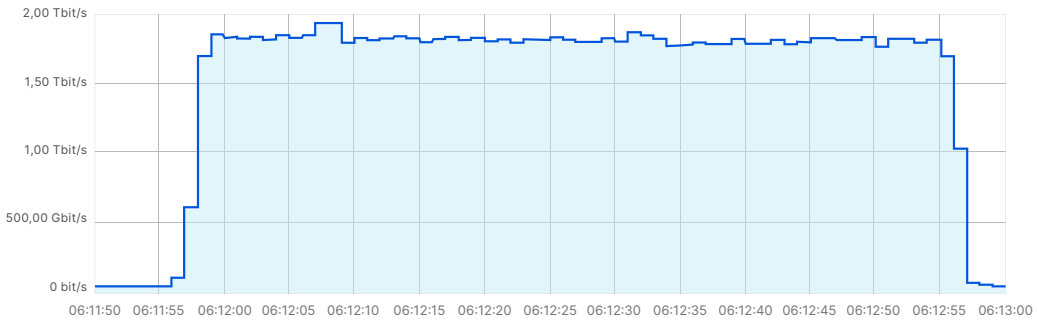
DDoS-Angriffe auf Netzwerkschicht

Bei Angriffen auf Anwendungsschicht (Layer 7 im OSI-Modell) sind die Dienste betroffen, auf die Endnutzer zugreifen wollen. Demgegenüber zielen Attacken auf Netzwerkschicht auf eine Überlastung der Netzwerkinfrastruktur (wie Router und Server innerhalb des Netzwerkpfads) und der Internetverbindung selbst ab.

Cloudflare vereitelt einen Angriff von fast 2 Tbit/s

Im November erkannten unsere Systeme einen DDoS-Angriff mit fast 2 Tbit/s und wehrten diesen automatisch ab. Dabei handelte es sich um einen Multi-Vektor-Angriff, bei dem DNS-Amplification und UDP-Floods kombiniert wurden. Die gesamte Attacke dauerte nur eine Minute. Sie wurde von etwa 15.000 Bots gestartet, die eine Variante des ursprünglichen Mirai-Codes auf IoT-Geräten und ungepatchten GitLab-Instanzen ausführten.

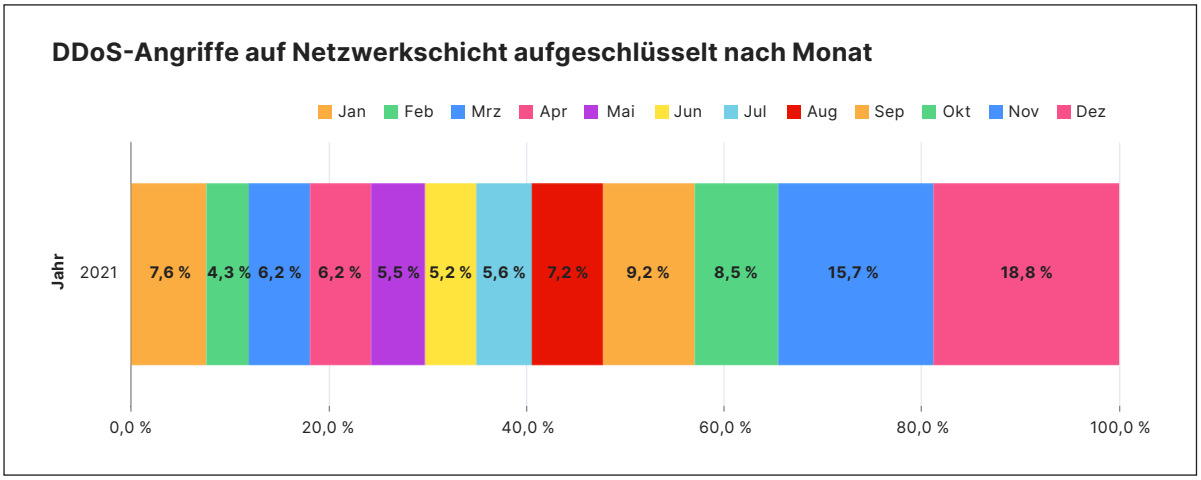
Variante des Mirai-Botnetzes startet DDoS-Angriff



DDoS-Angriffe auf Netzwerkschicht aufgeschlüsselt nach Monat

Der Dezember war der Monat, in dem die Angreifer 2021 am aktivsten waren.

Im vierten Quartal waren die Angreifer 2021 am aktivsten. Über 43 % aller DDoS-Angriffe auf Netzwerkschicht des Jahres erfolgten in diesem Zeitraum. Während es im Oktober vergleichsweise ruhig war, hat sich im November – dem Monat des chinesischen Singles' Day, des amerikanischen Thanksgiving-Feiertags, des Black Friday und des Cyber Monday – die Zahl der DDoS-Angriffe auf Netzwerkschicht fast verdoppelt. Die Zahl der registrierten Angriffe nahm in den letzten Tagen des Dezembers 2021 zu, als sich die Welt auf den Jahreswechsel vorbereitete. Tatsächlich wurden allein im Dezember mehr Attacken verbucht als im gesamten zweiten Quartal und fast genau so viele wie im ersten.



DDoS-Angriffe auf Netzwerkschicht aufgeschlüsselt nach Angriffsrate

Die meisten Angriffe sind zwar noch relativ „klein“, doch Attacken im Terabit-Bereich werden immer mehr zur Norm.

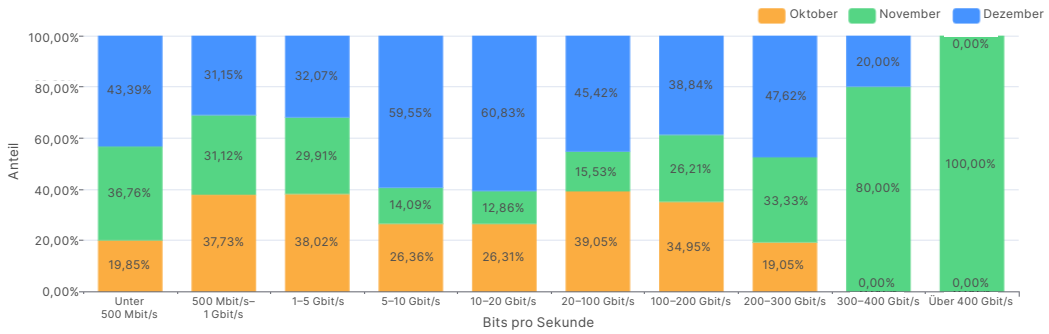
Es gibt verschiedene Möglichkeiten, die Größe eines L3/4-DDoS-Angriffs zu messen. Man kann sich das reine Volumen des Angriffs-Traffics ansehen, das als Bitrate (in Gigabits pro Sekunde, Gbit/s) ausgedrückt wird, oder man stellt auf die Paketrate (die Zahl der pro Sekunde gelieferten Datenpakete in Millionen) ab.

Angriffe mit hohen Bitraten zielen darauf ab, die Internetverbindung zu belegen, sodass es zu einer Denial of Service (Nichtverfügbarkeit) kommt. Mit hohen Paketraten dagegen wird versucht, die Server, Router oder andere Hardwaregeräte innerhalb des Netzwerkpfads durch Überlastung lahmzulegen. Diese Geräte wenden eine bestimmte Speicher- und Rechenleistung zur Verarbeitung eines Datenpakets auf. Werden sie daher mit Paketen regelrecht bombardiert, sind ihre Verarbeitungskapazitäten unter Umständen irgendwann erschöpft. In einem solchen Fall

werden Pakete „verworfen“ – mit anderen Worten: Die Appliance ist nicht in der Lage, sie zu verarbeiten. Für Nutzer hat das zur Folge, dass die von ihnen angesteuerten Dienste nicht richtig funktionieren oder nicht mehr verfügbar sind.

Unten sind die Angriffe nach Größe (angegeben als Bitrate) und Monat dargestellt. Wie das obige Schaubild zeigt, fanden die meisten Angriffe im Dezember statt. Aus der nachstehenden Abbildung geht aber hervor, dass im November größere Angriffe mit über 300 Gbit/s erfolgten. Die meisten Angriffe mit 5–20 Gbit/s wurden im Dezember ausgeführt.

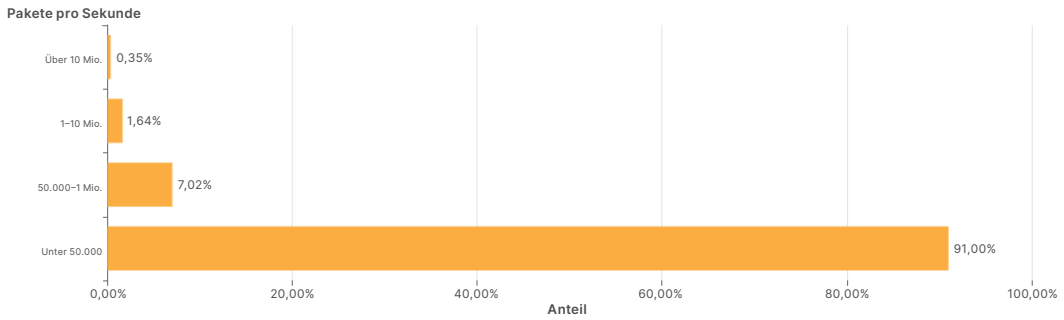
DDoS-Angriffe auf Netzwerkschicht aufgeschlüsselt nach Größe je Monat



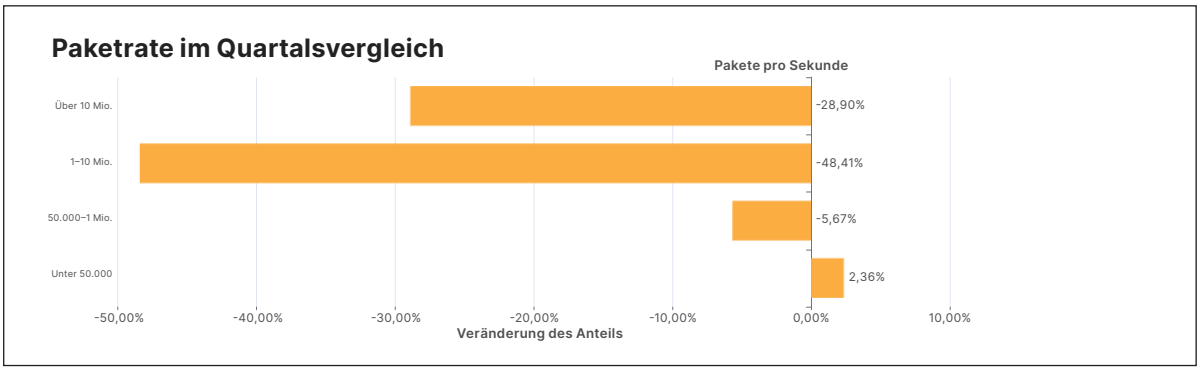
Verteilung nach Paketrate

Eine interessante Korrelation, die Cloudflare beobachtet hat, ist, dass mit zunehmender Anzahl der Angriffe deren Größe und Dauer abnehmen. In den ersten zwei Dritteln des Jahres 2021 war die Zahl der Angriffe relativ gering, und dementsprechend stiegen die Angriffsraten, z. B. im dritten Quartal 2021 um 196 % bei Angriffen mit 1 bis 10 Millionen Paketen pro Sekunde (million packets per second –mpps). Im vierten Quartal 2021 stieg die Zahl der Angriffe und Cloudflare beobachtete einen Rückgang der Größe der Angriffe. 91 % aller Angriffe erreichten einen Spitzenwert von weniger als 50.000 Paketen pro Sekunde (pps), was leicht ausreicht, um ungeschützte Internet-Seiten lahm zu legen.

DDoS-Angriffe auf Netzwerkschicht aufgeschlüsselt nach Paketrate

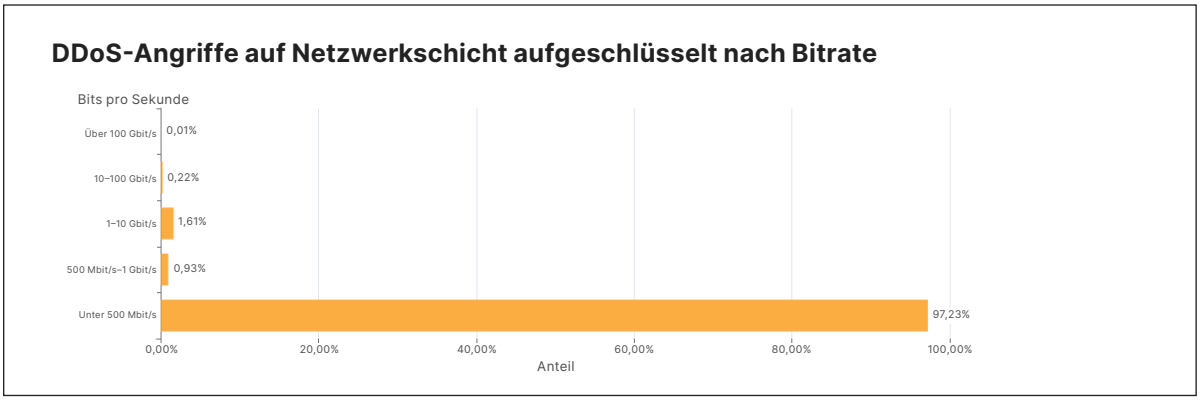


Größere Angriffe mit mehr als 1 Mio. pps gingen um 48 % auf 28 % im Quartalsvergleich zurück, während Angriffe mit weniger als 50.000 pps um 2,36 % im Quartalsvergleich zunahmen.

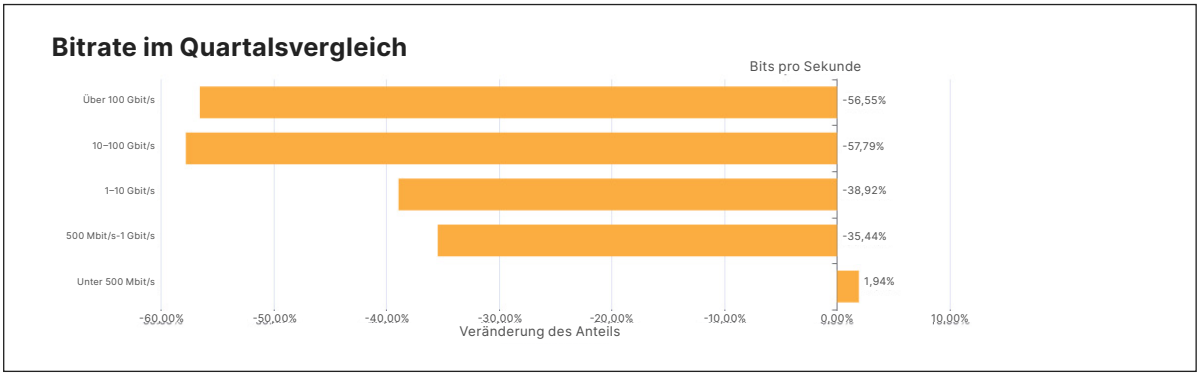


Verteilung nach Bitrate

Ähnlich wie bei den paketintensiven Angriffen ist auch der Anteil der bitintensiven Angriffe zurückgegangen. Während Angriffe mit mehr als 1 Tbit/s zur Norm werden und der größte Angriff, den wir je gesehen haben, knapp unter 2 Tbit/s lag, sind die meisten Angriffe immer noch klein und erreichten einen Spitzenwert von unter 500 Mbit/s (97,2 %).



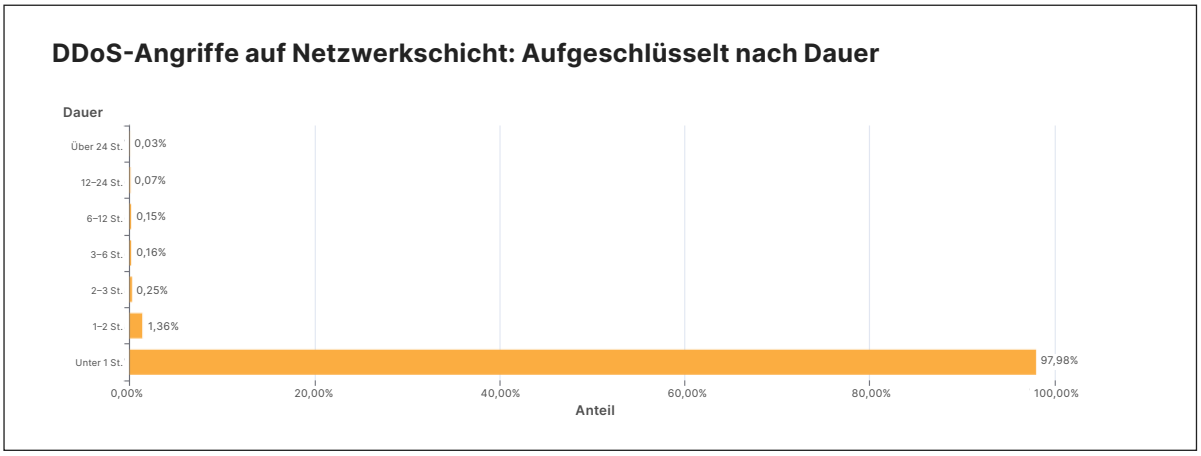
In vierten Quartal 2021 gab es bei größeren Angriffen in allen Bereichen über 500 Mbit/s einen massiven Rückgang von 35 % bis 57 % bei den größeren Angriffen mit 100+ Gbit/s.



DDoS-Angriffe auf Netzwerkschicht aufgeschlüsselt nach Dauer

Die meisten Attacken sind nach weniger als einer Stunde vorüber, was wieder einmal die Notwendigkeit automatisch handelnder und ständig aktiver DDoS-Abwehrlösungen unterstreicht.

Zur Ermittlung der Dauer eines Angriffs wird die Zeit zwischen dem Moment, in dem er von unseren Systemen erstmals als solcher erkannt wird, und dem Augenblick, in dem wir das letzte Paket mit der Signatur dieser Attacke auf dieses konkrete Ziel registrieren, gemessen. Im Schlussquartal 2021 dauerten 98 % aller Angriffe auf Netzwerkschicht weniger als eine Stunde. Dies ist sehr häufig der Fall, da die meisten Angriffe nur von kurzer Dauer sind. Mehr noch: Wir konnten unter anderem den Trend beobachten, dass bei einer Zunahme der Angriffszahl, wie sie in dem betreffenden Quartal zu verzeichnen war, die Dauer der Attacken abnimmt.



Kurze Angriffe bleiben leicht unbemerkt – insbesondere, wenn sie ein Ziel für wenige Sekunden mit einer großen Menge an Paketen, Bytes oder Anfragen bombardieren. In diesen Fällen haben Abwehrlösungen, die auf einer manuellen Bekämpfung mittels Sicherheitsanalyse beruhen, keine Chance, den Angriff rechtzeitig zu unterbinden. Es bleibt dann nur die Möglichkeit, ihn im Nachhinein zu untersuchen und auf Grundlage der dabei gewonnenen Erkenntnisse eine neue Regel zu erstellen, anhand derer der Traffic anschließend auf das Angriffsprofil hin gefiltert werden kann. Dann besteht zumindest eine gewisse Hoffnung, dass die nächste Attacke erkannt wird. Ebenso wenig zielführend ist der Einsatz eines „On Demand"-Services, bei dem das Sicherheitsteam den Traffic während eines Angriffs zu einem DDoS-Dienst umleitet, weil die Attacke vorüber ist, bevor der Datenverkehr dort ankommt.

Unternehmen wird daher empfohlen, automatisch arbeitende und ständig aktive DDoS-Schutzdienste zur Analyse des Datenverkehrs und zum Einsatz von Fingerprints in Echtzeit zu verwenden, die schnell genug sind, um auch kurze Angriffe zu blockieren.

Angriffsvektoren

SYN-Flood-Angriffe erfreuen sich nach wie vor der größten Beliebtheit, aber auch Attacken per SNMP sind im Quartalsvergleich um beachtliche 5.800 % gestiegen.

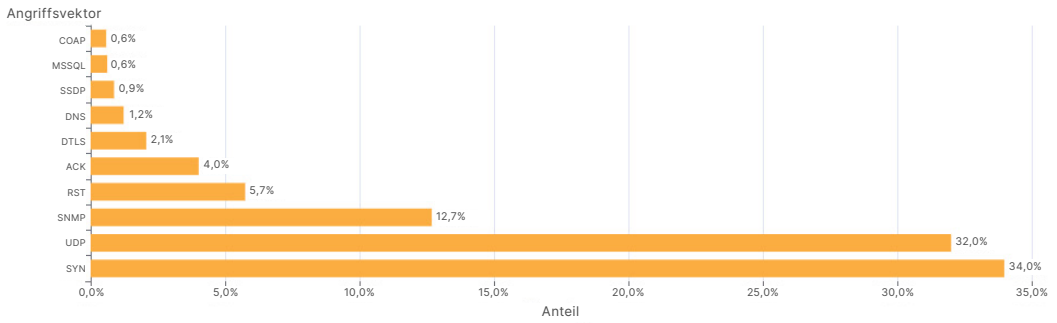
Mit dem Begriff „Angriffsvektor" bezeichnet man den Weg und die Methode, die bei einer Attacke verfolgt werden, d. h. das IP-Protokoll, Paketattribute wie TCP-Flags, die Flooding-Methode und andere Kriterien.

2021 ist der Anteil der SYN-Flood-Angriffe erstmals deutlich zurückgegangen. Im gesamten Jahr machten diese im Durchschnitt 54 % aller Attacken auf Netzwerkschicht aus. Obwohl sie immer noch der häufigste Angriffsvektor waren, sank ihr Anteil um 38 % im Quartalsvergleich auf 34 %.

Es war jedoch ein knappes Rennen zwischen SYN-Angriffen und UDP-Angriffen. Ein UDP-Flood ist eine Art von Denial-of-Service-Angriff, bei dem eine große Anzahl von User Datagram Protocol (UDP)-Paketen an einen Zielserver gesendet wird, um die Verarbeitungs- und Reaktionsfähigkeit des Geräts zu überfordern. Oft erreicht auch die Firewall, die den Zielserver schützt, infolge des UDP-Floodings ihre Grenzen, was zu einem Denial of Service für den legitimen Datenverkehr führt. Angriffe per UDP kletterten vom vierten Platz im dritten Quartal auf den zweiten Platz im vierten Quartal 2021, mit einem Anteil von 32 % aller Angriffe auf Netzwerkschicht – ein Zuwachs um 1.198 % im Quartalsvergleich.

An dritter Stelle steht der Außenseiter SNMP, der mit seinem erstmaligen Auftauchen in den Top-Angriffsvektoren 2021 einen gewaltigen Sprung gemacht hat.

DDoS-Angriffe auf Netzwerkschicht aufgeschlüsselt nach den wichtigsten Angriffsvektoren



Neue Bedrohungen

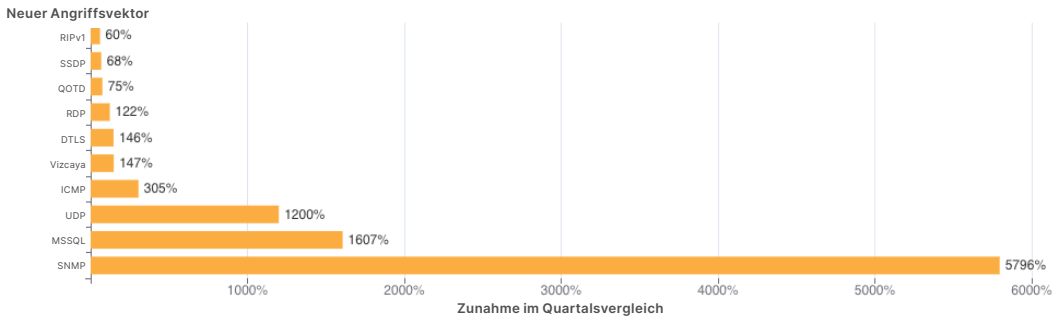
Wenn wir uns neue Angriffsvektoren ansehen, ist ein massiver Anstieg von SNMP-, MSSQL- und generischen UDP-basierten DDoS-Attacken zu beobachten.

Sowohl SNMP- als auch MSSQL-Angriffe werden eingesetzt, um den an das Ziel gerichtete Datenverkehr zu spiegeln und zu verstärken, indem in den zur Auslösung des Angriffs verwendeten Paketen die IP-Adresse des Ziels so gefälscht wird, dass sie als Quell-IP-Adresse erscheint.

Das Simple Network Management Protocol (SNMP) ist ein UDP-basiertes Protokoll, das häufig zur Erkennung und Verwaltung von Netzwerkgeräten wie Druckern, Switches, Routern und Firewalls eines Heim- oder Unternehmensnetzwerks über den bekannten UDP-Port 161 verwendet wird. Bei einem SNMP-Reflection-Angriff sendet der Angreifer eine große Anzahl von SNMP-Abfragen, wobei sich die Quell-IP-Adresse in den Paketen als Zielgeräte im Netzwerk ausgibt, die ihrerseits an die Adresse des Zielgeräts antworten. Eine große Anzahl von Antworten von den Geräten im Netz führt dazu, dass das Zielnetz einen DDoS-Angriff erlebt.

Ähnlich wie der SNMP-Amplification-Angriff basiert der Microsoft SQL (MSSQL)-Angriff auf einer Technik, die das Microsoft SQL Server Resolution Protocol missbraucht, um einen Reflection-basierten DDoS-Angriff zu starten. Der Angriff erfolgt, wenn ein Microsoft SQL Server auf eine Client-Abfrage oder -Anfrage antwortet und versucht, das Microsoft SQL Server Resolution Protocol (MC-SQLR) auszunutzen, das den UDP-Port 1434 für den Empfang nutzt.

DDoS-Angriffe auf Netzwerkschicht: die wichtigsten neuen Angriffsvektoren



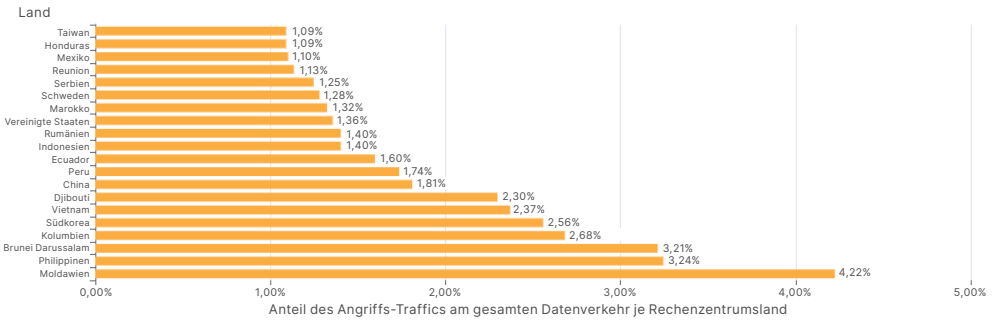
DDoS-Angriffe auf Netzwerkschicht aufgeschlüsselt nach Land

Die Angriffe aus Moldawien vervierfachten sich und machten Moldawien zum Land mit dem höchsten Anteil an DDoS-Aktivitäten auf Netzwerkschicht.

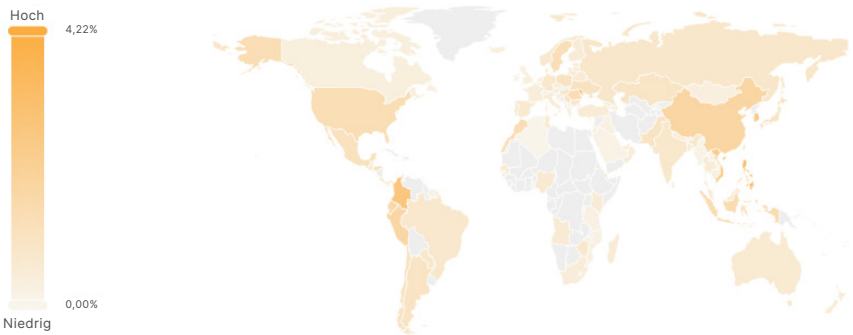
Bei der Analyse von DDoS-Angriffen gruppieren wir den Traffic auf Netzwerkschicht nicht nach der Quell-IP ein, sondern nach den Standorten der Cloudflare-Edge-Rechenzentren, an denen er eingegangen ist. Der Grund dafür ist, dass bei Angriffen auf Netzwerkschicht die Quell-IP-Adresse gefälscht werden kann, um die Angriffsquelle zu verschleiern und Zufälligkeit in die Angriffseigenschaften zu bringen. Für einfache DDoS-Schutzsysteme wird es dadurch schwieriger, den Angriff zu blockieren.

Würde das Land auf Grundlage einer gefälschten Quell-IP abgeleitet, hätte das eine Verfälschung der Ergebnisse zur Folge. Das Problem der gefälschten IPs wird dadurch gelöst, dass die Angriffsdaten nach dem Standort des Cloudflare-Rechenzentrums angezeigt werden, in dem der Angriff beobachtet wurde. In unserem Bericht bieten wir geografisch genaue Angaben, weil wir Rechenzentren in über 250 Städten auf der ganzen Welt unterhalten.

Aufschlüsselung der DDoS-Angriffe nach Standort der Cloudflare-Rechenzentren



DDoS-Angriffe auf Netzwerkschicht – wichtigste Länder (weltweit)



Die interaktive Karte ermöglicht einen Überblick über alle Regionen und Länder.

Zusammenfassung

Cloudflare hat es sich zur Aufgabe gemacht, ein besseres Internet zu schaffen. Damit ist ein sicheres, schnelleres und zuverlässigeres Web für alle gemeint – auch angesichts von DDoS-Angriffen. Als Teil unserer Mission bieten wir seit 2017 zeitlich unbeschränkten und unbegrenzten DDoS-Schutz kostenlos für alle unsere Kunden. Im Lauf der Jahre ist es immer leichter geworden, DDoS-Angriffe auszuführen. Um dem Vorteil der Angreifer entgegenzuwirken, wollen wir dafür sorgen, dass sich auch Unternehmen jeder Größe problem- und kostenlos vor DDoS-Angriffen aller Art schützen können.

Sie sind noch kein Cloudflare-Nutzer? Dann werden Sie es jetzt.