CLOUDFLARE

Cloudflare-Bericht zu DDoS-Angriffstrends

Inhalt

Q4 2023

Kurzfassung

Willkommen zum sechzehnten DDoS-Bedrohungsbericht von Cloudflare. Distributed Denial-of-Service (DDoS)-Attacken sind Cyberangriffe, die darauf abzielen, Websites (und andere Arten von Internetpräsenzen) für legitime Nutzer unerreichbar zu machen. Dafür werden sie mit großen Mengen Traffic bombardiert, bis sie unter der Last zusammenbrechen. Der Effekt ist vergleichbar mit einem Autofahrer, der wegen zu hohen Verkehrsaufkommens im Stau steht.

Unser Netzwerk zählt zu den größten der Welt und umfasst über 300 Städte in mehr als 120 Ländern. Wir sind in der Lage, riesige Mengen Internettraffic zu bewältigen, bearbeiten zu Spitzenzeiten gut 70 Mio. Webanfragen in der Sekunde und 2,6 Mrd. DNS-Abfragen am Tag. Im Durchschnitt neutralisieren wir täglich 170 Mrd. Cyberbedrohungen. Dank dieses riesigen Datenvolumens können wir den Rest der Cybersicherheitsbranche über wertvolle Erkenntnisse und aktuelle Trends informieren.

Vor dem Hintergrund der vor Kurzem in Taiwan durchgeführten Wahlen und von Berichten über Spannungen in China haben wir in den letzten Wochen einen sprunghaften Anstieg von DDoS-Attacken und anderen Cyberangriffen beobachtet. Und seit Beginn des bewaffneten Konflikts zwischen Israel und der Hamas haben sich die DDoS-Angriffe auf palästinensische und israelische Websites stark intensiviert.

Die DDoS-Attacken auf Anwendungsschicht sind von 2022 auf 2023 um 20 % gesunken. Doch paradoxerweise wurden im vergangenen Jahr auch die größten Angriffskampagnen in diesem Segment verzeichnet, bei denen in mehreren Fällen die Zahl von 100 Mio. Anfragen pro Sekunde überschritten wurde. Dazu zählte die HTTP/2 Rapid Reset-Angriffskampagne zu Jahresbeginn. Bei DDoS-Attacken auf Netzwerkschicht zeigte sich ein völlig anderes Bild, denn diese schnellten 2023 im Jahresvergleich um 85 % nach oben.

Auffallend war, dass Umweltorganisationen den höchsten HTTP-DDoS-Angriffstraffic registrierten, wobei diese Entwicklung zeitlich mit der 28. UN-Klimakonferenz (COP 28) zusammenfiel.

Eine interaktive Version dieses Berichts ist auch bei Cloudflare Radar verfügbar.

Wichtigste Erkenntnisse

DDoS-Trends im Jahr 2023

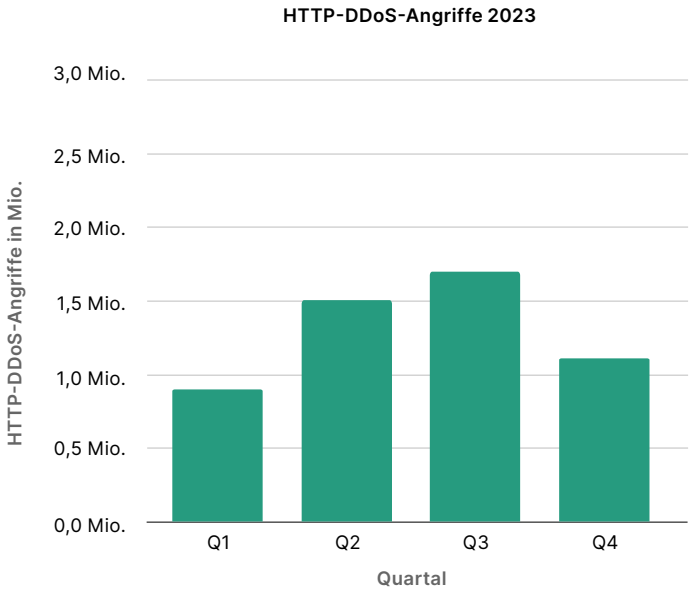
Nach Ende der hypervolumetrischen Kampagne haben wir 2023 insgesamt einen unerwarteten Rückgang der HTTP-DDoS-Angriffe um 20 % gegenüber 2022 verzeichnet. Insgesamt wurden im vergangenen Jahr durch unsere automatischen Schutzmaßnahmen über 5,2 Mio. solcher Attacken abgewehrt, die zusammen mehr als 26 Bio. Anfragen umfassten. Obwohl die Attacken also alles in allem rückläufig waren, ergab sich immer noch ein ausgesprochen hoher Durchschnittswert, denn pro Stunde wurden im vergangenen Jahr 3 Mrd. Anfragen im Rahmen von 594 HTTP-DDoS-Angriffen abgewehrt.

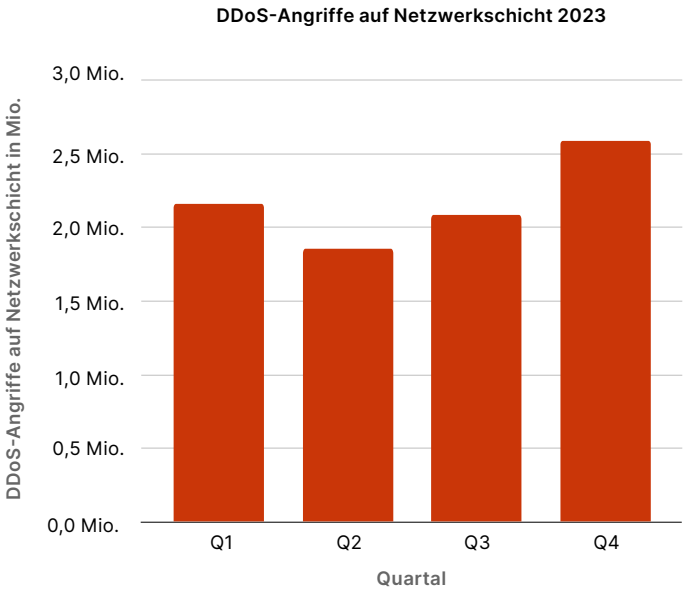
Was DDoS-Attacken auf Netzwerkschicht betrifft, zeigte sich dort ein ganz anderer Trend. Mit unseren automatischen Schutzmaßnahmen wurden letztes Jahr 8,7 Mio. solcher Angriffe abgefangen. Gegenüber 2022 stellt das eine Zunahme von 85 % dar. Pro Stunde haben unsere Systeme damit durchschnittlich 996 DDoS-Attacken in einem Gesamtumfang von 27 Terabyte neutralisiert.

DDoS-Angriffe des Jahres 2023 in Zahlen

↓ **HTTP-DDoS-Angriffe**
5,2 Mio. Angriffe
wurden 2023 abgewehrt
-20 % im Jahresvergleich

↑ **DDoS-Angriffe auf Netzwerkschicht**
8,7 Mio. Angriffe
wurden 2023 abgewehrt
+85 % im Jahresvergleich





Konkrete Konfliktzonen und DDoS-Angriffe: Wahlen in Taiwan, Krieg zwischen Israel und Hamas

Die sprunghafte Zunahme von Angriffen auf bestimmte Weltregionen (Taiwan, Israel und die palästinensischen Autonomiegebiete) macht deutlich, dass DDoS-Angriffe als Instrument der Kriegsführung eingesetzt werden, um mittels Cyberkapazitäten entweder politischen Druck auszuüben oder kritische digitale Infrastruktur zu stören.

Wahlen in Taiwan

Wir haben einen Anstieg der HTTP-DDoS-Angriffe auf Websites in Taiwan um 3.370 % im Vergleich zum Vorjahr festgestellt. Die überwiegende Mehrheit (82 %) ging von China aus, was mit dem spannungsgeladenen politischen Verhältnis zwischen China und Taiwan zusammenhängt. Überraschenderweise standen Websites mit pornografischen Inhalten stärker unter Beschuss als die von Branchen, die stärker im Alltag verwurzelt sind, etwa Finanzdienstleistungen, das Gesundheitswesen oder der Sektor Verkehr und Transport.

Krieg zwischen Israel und der Hamas

DDoS-Angriffe sind inzwischen ein gern genutztes Instrument der Kriegsführung und Störung. Dementsprechend haben wir eine Zunahme solcher Attacken während des Konflikts zwischen Russland und der Ukraine ebenso beobachtet wie bei der Auseinandersetzung zwischen Israel und der Hamas. Zum ersten Mal über diese jüngsten Aktivitäten berichtet haben wir in unserem Blog-Beitrag „Israel und Hamas tragen Konflikt auch im Cyberspace aus“. Seitdem behalten wir die Entwicklung weiter im Blick.

Die palästinensischen Autonomiegebiete waren im vierten Quartal die Weltregion, die am zweithäufigsten von HTTP-DDoS-Angriffen und DDoS-Attacken auf Netzwerkschicht betroffen war. Über 68 % des gesamten Layer-3- und Layer-4-Traffics in palästinensischen Netzwerken und mehr als 10 % aller HTTP-Anfragen an palästinensische Websites gingen auf DDoS-Angriffe zurück. In neun von zehn Fällen richteten sich diese HTTP-DDoS-Attacken gegen Websites palästinensischer Banken.

Auch israelische Websites verzeichneten einen hohen HTTP-DDoS-Datenverkehr, auch wenn dieser im Quartalsvergleich nur um 27 % anstieg. Fast 65 % aller HTTP-DDoS-Angriffe auf israelische Websites galten der Zeitungs- und Medienbranche sowie auf dem Bereich Computersoftware.

Unsere Daten lassen auf konzertierte Bemühungen auf beiden Seiten schließen, Branchen zu schädigen, die im Alltag eine wichtige Rolle spielen.

Internationale politische Zwischenfälle zunehmend Auslöser für Cyberangriffe

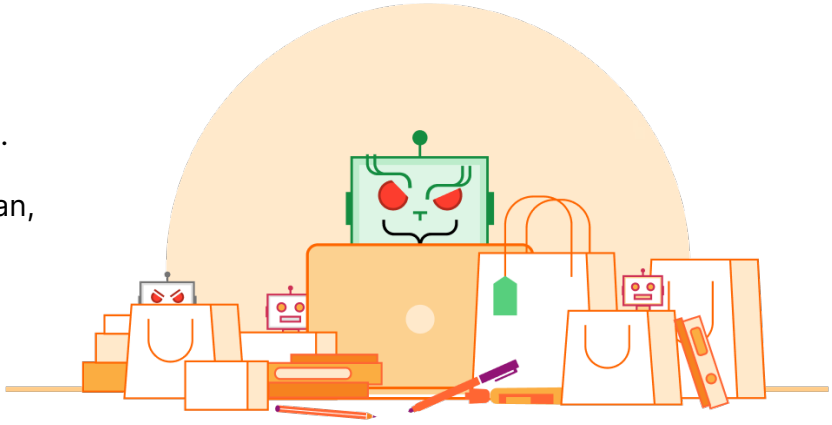
Wir beobachten, dass internationale Ereignisse zunehmend zu Auslösern von Cyberangriffen werden. Die 28. UN-Klimakonferenz (auch COP 28 genannt) endete am 13. Dezember 2023. Im Schlussquartal 2023 wurde ein atemberaubender Anstieg (um mehr als 61.000 %) im Jahresvergleich bei HTTP-DDoS-Angriffen auf Umweltorganisation verzeichnet. Es handelte sich aber keineswegs um einen Einzelfall.

Ähnliche Muster wurden schon früher – insbesondere während der COP 26, der COP 27 und anlässlich anderer umweltbezogener UN-Resolutionen oder Ankündigungen – registriert: Jedes Mal kam es zu einer entsprechenden Zunahme von Cyberangriffen auf die Websites von Umweltdienstleistern.

DDoS-Angriffe trüben im vierten Quartal die Feiertagslaune

Zwischen dem Black Friday, Weihnachten und Neujahr wurden vermehrt HTTP-DDoS-Angriffe auf Websites von Einzelhändlern, Versanddienstleistern und Public Relations-Firmen verzeichnet. Setzt man die Angriffe auf Anwendungsschicht mit dem gesamten HTTP-Traffic einer Branche ins Verhältnis, war (nach den Umweltdienstleistern) die Verpackungs- und Frachtversandindustrie am zweitstärksten von solchen Attacken betroffen. Dieser Wirtschaftszweig hat einen nicht unerheblichen Einfluss auf das Käufererlebnis am Black Friday und während der Winterfeiertage, womit er für den Geschäftserfolg in dieser Zeit eine Rolle spielt. Denn schließlich müssen die gekauften Geschenke und Waren irgendwie an ihren Bestimmungsort gelangen. Womöglich haben Angreifer versucht, dies zu verhindern. Ähnliches war bei den Einzelhandelsunternehmen zu beobachten, wo DDoS-Angriffe auf Anwendungsschicht im Jahresvergleich um 23 % zugenommen haben.

Auf Netzwerkschicht war die Branchen Public Relations und Kommunikation am stärksten betroffen: 36 % des Traffics waren hier bösartig. Werden die Betriebs- und Geschäftsabläufe gestört, kann das dem Image einer Firma unmittelbar und weitreichend schaden.
Im vierten Quartal werden aufgrund von Feiertagen, Jahresabschlüssen und der Vorbereitungen für das neue Jahr PR- und Kommunikationsaktivitäten häufig verstärkt. In dieser geschäftlich kritischen Zeit haben Angreifer möglicherweise ein Interesse daran, Störungen zu verursachen.

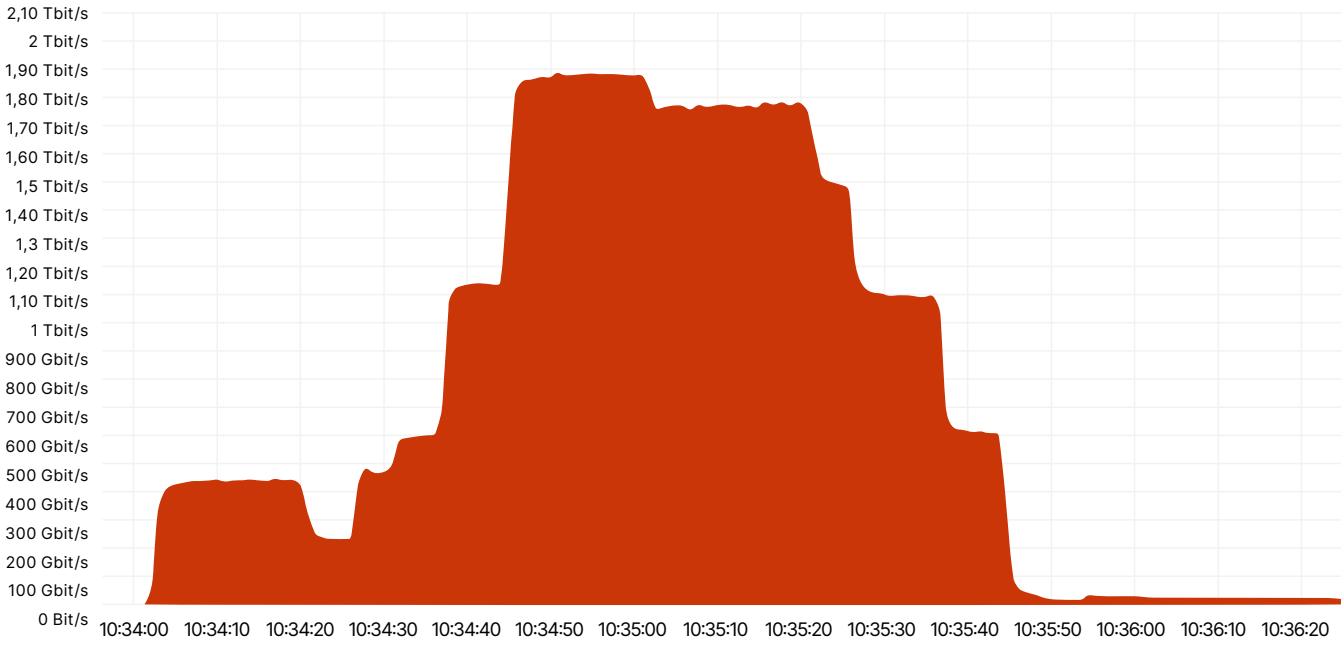


Neue Vektoren für Angriffe auf Netzwerkschicht

Um besser zu verstehen, wie sich die Bedrohungslandschaft bei DDoS-Angriffen auf Netzwerkschicht wandelt, wollen wir uns einen konkreten Fall genauer ansehen.

Eine der größten Attacken, die zwischen Oktober und Dezember stattgefunden hat, wurde durch ein Mirai-Botnetz auf einen bekannten europäischen Cloud-Dienstleister ausgeführt. Sie dauerte keine zehn Minuten, ging von über 18.000 (vermutlich gefälschten) Einzel-IP-Adressen aus und wurde von der Cloudflare-Abwehr automatisch erkannt und gestoppt.

Großer Mirai-Botnetz-Angriff auf europäischen Cloud-Dienstleister

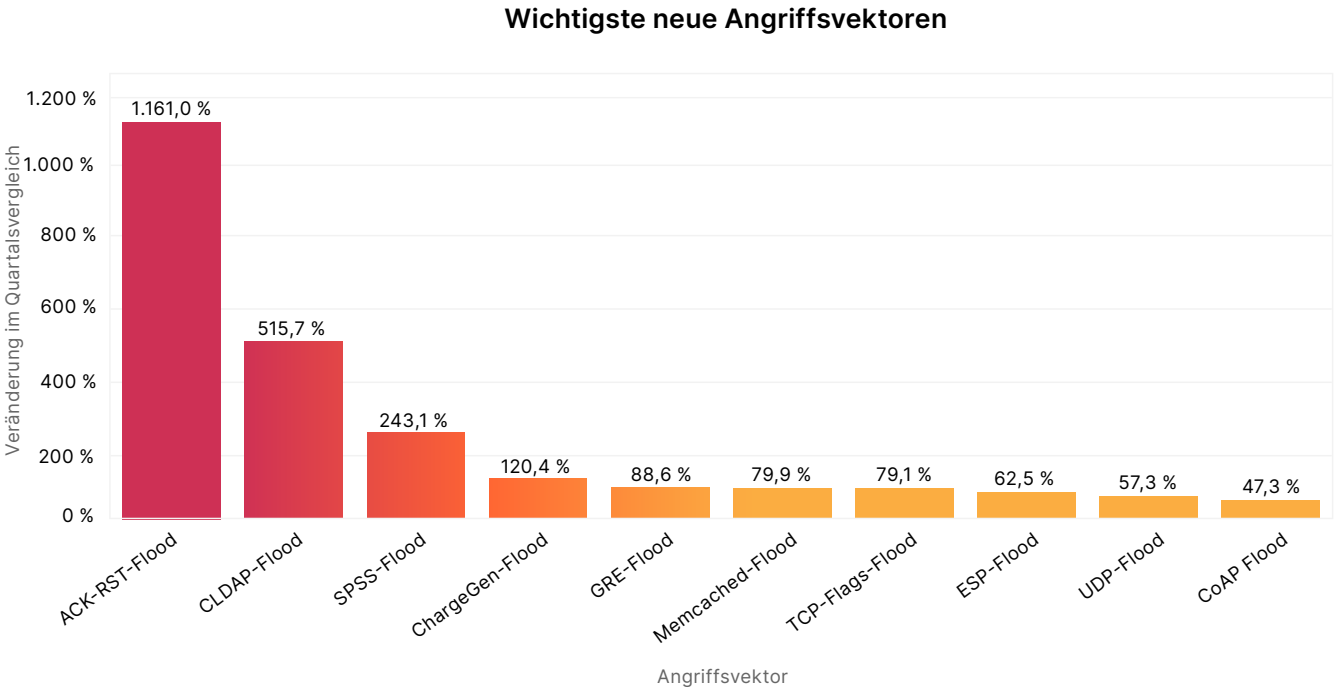


Dieser Angriff stach aufgrund seiner hohen Bitrate pro Sekunde und der Tatsache, dass mehrere Vektoren genutzt wurden, zwar heraus, war aber dennoch nur von kurzer Dauer. Er erreichte einen Spitzenwert von 1,9 Tbit/s und kombinierte mehrere Angriffsmethoden, darunter UDP-Fragment-Flood, UDP/Echo-Flood, SYN-Flood, ACK-Flood und TCP-Malformed-Flags. Attacken mit einer derart hohen Bitrate pro Sekunde sind selten. Noch raffinierter sind Angriffe, bei denen mehrere Methoden zusammen eingesetzt werden.

Die Rate von 160 Mio. Paketen pro Sekunde war allerdings nicht die höchste jemals von uns verzeichnete, denn im Jahr 2020 haben wir einen Wert von 754 Mio. Paketen pro Sekunde registriert.

Aber selbst, wenn man von diesem Angriff mit seinen einzigartigen Merkmalen absieht: Unternehmen können es sich einfach nicht erlauben, manuelle Scrubbing-Center für ihre DDoS-Abwehr einzusetzen. Vielmehr benötigen sie automatisierte interne Verteidigungssysteme.

Bei den von uns beobachteten neuen Bedrohungen haben wir im Quartalsvergleich einen Anstieg der ACK-RST Floods um 1.161 %, eine Zunahme der CLDAP-Floods um 515 % und eine Steigerung der SPSS-Floods um 243 % verzeichnet. Schauen wir uns jetzt einige dieser Attacken genauer an, um herauszufinden, auf welche Weise sie Schaden anrichten können.



ACK-RST-Floods

Bei einem Angriff per ACK-RST-Flood wird das Transmission Control Protocol (TCP) ausgenutzt, indem zahlreiche ACK- und RST-Pakete an das Opfer gesendet werden. Dieses ist irgendwann nicht mehr in die Lage, die Flut an Paketen zu verarbeiten und darauf zu reagieren, was Störungen oder einen Ausfall verursacht. Der Angriff hat Erfolg, weil jedes ACK- oder RST-Paket eine Antwort vom System des Opfers anfordert und dessen Ressourcen beansprucht. Traffic von ACK-RST-Floods lässt sich oft schwer herausfiltern, weil er legitimen Datenverkehr nachahmt, was die Erkennung und Abwehr schwierig macht.

CLDAP-Floods

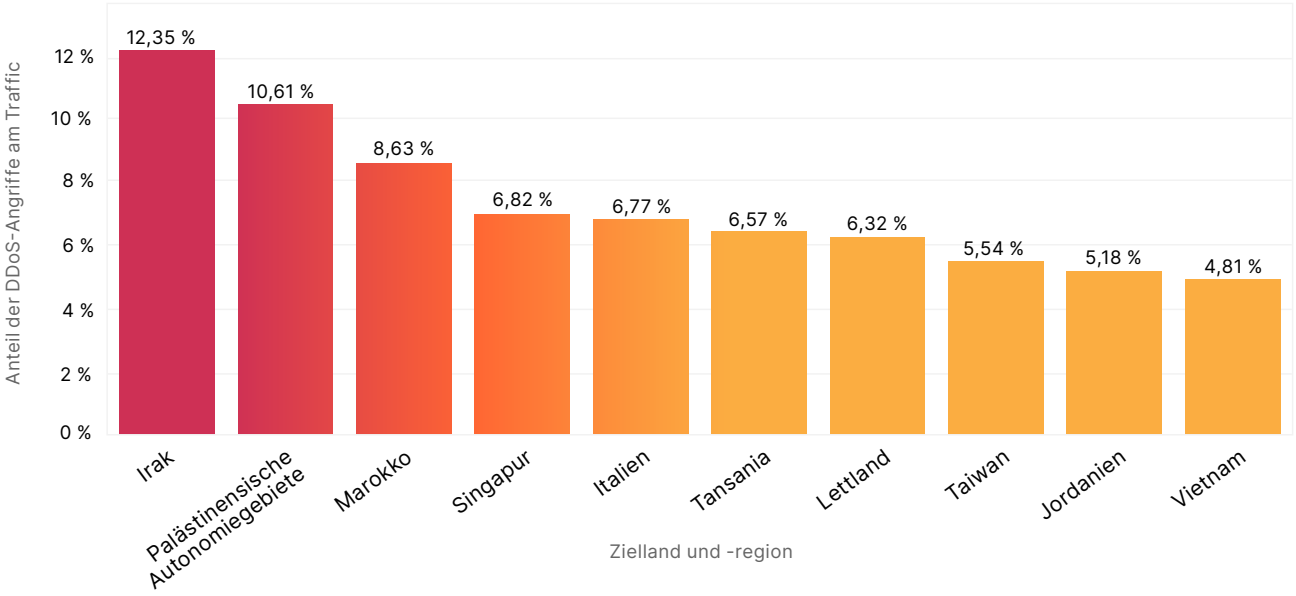
CLDAP (Connectionless Lightweight Directory Access Protocol) ist eine Variante von LDAP (Lightweight Directory Access Protocol). Dieses Protokoll wird für die Abfrage und Änderung von Verzeichnisdiensten verwendet, die über IP-Netzwerke laufen. CLDAP ist verbindungslos und verwendet UDP anstelle von TCP, wodurch es zwar schneller, aber auch weniger zuverlässig ist. Da UDP genutzt wird, ist kein Handshake erforderlich. Das gibt Angreifern die Möglichkeit, die IP-Adresse zu fälschen und als Reflection-Vektor zu nutzen. Bei solchen Attacken werden kleine Abfragen mit einer gefälschten Quell-IP-Adresse (der IP-Adresse des Opfers) gesendet, was dazu führt, dass die Server große Antworten an das Opfer senden und so eine Überlastung verursachen. Zur Abwehr dieser Angriffe gehört das Filtern und Überwachen von ungewöhnlichem CLDAP-Traffic.

SPSS-Floods

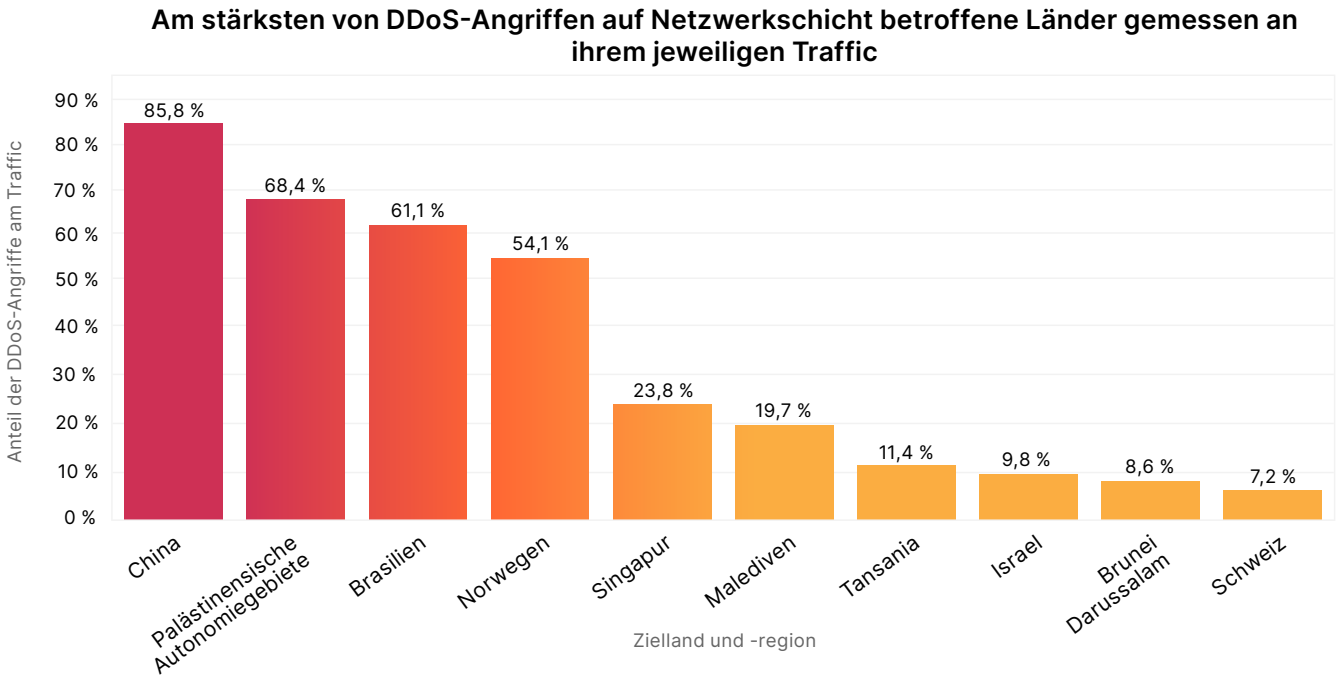
Floods, die das SPSS (Source Port Service Sweep)-Protokoll missbrauchen, sind eine Art von Netzwerkangriff. Dabei werden Pakete von zahlreichen zufälligen oder gefälschten Quellports an verschiedene Zielports eines Zielsystems oder -netzwerks gesendet. Es werden zwei Ziele verfolgt. Erstens geht es um die Überlastung der Rechenkapazitäten des Opfers, was zu Störungen oder Netzwerkausfällen führt. Zweitens lassen sich auf diese Weise offene Ports und anfällige Dienste aufspüren. Das Flooding wird durch das Versenden einer großen Anzahl von Paketen erreicht, die die Netzwerkressourcen des Opfers voll beanspruchen und die Kapazitäten seiner Firewalls und Intrusion Detection-Systeme erschöpfen können. Um solche Angriffe abzuwehren sollten unbedingt automatische systeminterne Erkennungsfunktionen eingesetzt werden.

Am stärksten angegriffene Regionen

Am stärksten von HTTP-DDoS-Angriffen betroffene Länder gemessen an ihrem jeweiligen Traffic



Der Irak, die palästinensischen Autonomiegebiete und Marokko stehen an der Spitze der am stärksten angegriffenen Weltregionen, wenn man den gesamten an sie gerichteten Datenverkehr betrachtet. Interessant ist, dass Singapur an vierter Stelle kommt. Das Land war nicht nur mit dem meisten HTTP-DDoS-Angriffstraffic konfrontiert (4 % des weltweiten DDoS-Datenverkehrs), sondern dieser hat auch einen beträchtlichen Teil des gesamten für Singapur bestimmten Datenverkehrs ausgemacht. Die USA wurden im Gegensatz dazu gemessen am Volumen des DDoS-Datenverkehrs (3,8 % des weltweiten DDoS-Traffics) am zweithäufigsten angegriffen. Setzt man dies aber ins Verhältnis zum gesamten für die Vereinigten Staaten bestimmten Traffic, erreichten sie nur den fünfzigsten Platz.



Die regionalen Trends sind auf Netzwerkschicht noch deutlicher als auf Anwendungsschicht.

China war auch 2023 das Land mit den meisten Angriffen auf Netzwerkschicht. Noch einschneidender als die HTTP-DDoS-Trends für Singapur ist die Tatsache, dass China sowohl im Hinblick auf den DDoS-Angriffstraffic auf Netzwerkschicht als auch in Bezug auf den gesamten an das Land gerichteten Datenverkehr am stärksten unter Beschuss stand. Fast 86 % des für die Volksrepublik bestimmten Datenverkehrs wurde von Cloudflare als DDoS-Angriff auf Netzwerkschicht eingestuft und abgewehrt. Bei drei anderen Weltregionen – den palästinensischen Autonomiegebieten, Brasilien und Norwegen – war mehr als eines von zwei aller für sie bestimmte Bytes Teil einer DDoS-Attacke.

Empfehlungen und Schlussfolgerungen

Best Practices	Cloudflare-Nutzung optimieren
Aktualisieren oder erstellen Sie einen Denial-of-Service-Reaktionsplan.	Stellen Sie sicher, dass Ihr IT-Sicherheitsdienstleister über eine rund um die Uhr besetzte Notfall-Hotline verfügt. Die „Cloudflare Under Attack“-Hotline bietet Expertise, Methoden und Technologie, um Angriffe in Echtzeit abzuwehren. Prüfen Sie den Incident Response-Prozess und die Service Level Agreements (SLA) Ihres Sicherheitsdienstleisters vor einem echten DDoS-Angriff auf Herz und Nieren. Schulen Sie ausgewählte Mitarbeitende für Ihren dokumentierten DDoS-Reaktionsplan und vergewissern Sie sich, dass diese den DDoS-Lernpfad von Cloudflare gelesen haben, damit die von Cloudflare bereitgestellten Kontrollen bestmöglich funktionieren.
Setzen Sie zur DDoS-Abwehr Bedrohungsdaten und integrierte, automatische Lösungen ein. Scrubbing-Center mit manueller Bereinigung sind den kurzen und intensiven Angriffen der heutigen Zeit nicht gewachsen.	Nutzen Sie mehrere Erkennungstechniken, um Ihre Sicherheitsvorkehrungen im Kontext einer sich ständig weiterentwickelnden Bedrohungslandschaft zu optimieren: 1. Dynamisches zustandsloses Fingerprinting 2. Auf maschinellem Lernen basierende Klassifizierung 3. Erkennung von irregulärem Datenverkehr 4. Erstellung von Trafficprofilen und zustandsabhängige Abwehrmaßnahmen 5. Einsatz von Bedrohungsdaten zu aktuellen DDoS-Aktivitäten und -Trends
Bringen Sie Ihre Infrastruktur auf den neuesten Stand, um sie entsprechend Ihres Datenverkehrsprofils widerstandsfähiger zu machen.	Stellen Sie sicher, dass die Kapazität Ihrer DDoS-Abwehrlösung Angriffen gewachsen ist, die doppelt so umfangreich sind wie größten bislang verzeichneten und deren Paketraten zweimal so hoch sind wie die Ihres legitimen Traffics zu Spitzenzeiten. Vergewissern Sie sich, dass Ihr IT-Sicherheitsdienstleister die neuesten Schwachstellen in Netzwerk- und Anwendungsprotokollen beseitigen kann. Verlagern Sie den DNS-Traffic auf regelkonforme und sichere Cloud-Plattformen, bei denen der Datenverkehr über Edge-Netzwerke geleitet wird, die dem Nutzer am nächsten sind.
Verbessern Sie die Netzwerk- und Anwendungsperformance zur Vermeidung von Engpässen.	Nutzen Sie einen digitalen Warteraum, um sicherzustellen, dass echte Nutzer und Besucher serös über die Wartezeit informiert werden und es nicht zu einer Überlastung der Anwendungsserver kommt. Optimieren Sie die Zwischenspeicherung und die Verwaltung von Arbeitslasten mit einem Content Delivery Network (CDN) und cloudbasierten Lösungen zur Lastverteilung.
Wenden Sie ein positives Sicherheitsmodell an: Stellen Sie sicher, dass der von Ihnen erwünschte Datenverkehr zuverlässig ankommt.	Halten Sie geschäftskritische Protokolle, IP, ASN, Ports und Nutzer-Agenten für bereinigten Datenverkehr offen. Verwenden Sie Schemavalidierung und ein API-Gateway für API-Datenverkehr.
Nutzen Sie künstliche Intelligenz, um neuen Bedrohungen einen Schritt voraus zu sein.	Greifen Sie auf Bot-Scores zurück, die für Firewall- und Durchsatzbegrenzungsregeln herangezogen werden können. Lassen Sie Ihre öffentlich zugänglichen API automatisch aufspüren und vor DDoS-Angriffen schützen.

Bei Cloudflare möchten wir es Unternehmen und Organisationen jeder Größe noch einfacher machen, sich selbst vor den umfangreichsten und komplexesten DDoS-Angriffen zu schützen – und zwar gratis. Wir bieten allen unseren Kunden seit 2017 – als Pionier des Konzepts – kostenlosen und uneingeschränkten DDoS-Schutz ohne Volumenbegrenzung.

Erfahren Sie mehr darüber, wie Sie sich mit Cloudflare vor den neuesten DDoS-Bedrohungen schützen können.

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

REV:BDES-5497.2024FEB08