CLOUDFLARE

Cloudflare-Bericht zur DDoS-Bedrohungslandschaft

Q2 2023

Inhalt

Kurzfassung

Willkommen beim vierteljährlichen Cloudflare-Bericht zu Distributed-Denial-of-Service (DDoS)-Angriffen für die Monate April bis Juni 2023.Dieser Report gibt Einblicke in die während des zweiten Quartals 2023 im globalen Netzwerk von Cloudflare beobachteten DDoS-Aktivitäten und zeigt die damit in Verbindung stehenden Trends auf.

Das zweite Quartal 2023 war geprägt von gut durchdachten, individuell zugeschnittenen und kontinuierlichen Wellen von DDoS-Angriffen an verschiedenen Fronten.

Auf HTTP-Ebene war ein sehr aktives Vorgehen der pro-russischen Hacktivistengruppen REvil, Killnet und Anonymous Sudan gegen westliche Websites und eine Zunahme von DDoS-Attacken mit geringem Umfang und hohem Zufallsgrad zu beobachten. DNS-basierte DDoS-Attacken haben sich im Berichtsquartal zur beliebtesten Angriffsmethode entwickelt: 32 % aller DDoS-Attacken zielten auf das DNS-Protokoll ab. Auf UDP-Ebene haben wir Angriffe beobachtet, die eine von uns im März 2022 veröffentlichte Zero-Day-Schwachstelle (CVE-2022-26143, TP240PhoneHome) ausgenutzt haben.

Angriffstrends auf Anwendungs- und Netzwerkschicht werden nicht nur nach bestimmten Angriffskampagnen, sondern auch nach branchen- und regionsspezifischen Unterschieden aufgeschlüsselt. Schließlich geben wir Hinweise, wie Sie Ihre Sicherheitsvorkehrungen proaktiv steigern können, um die Verfügbarkeit Ihrer Dienste in einer sich ständig weiterentwickelnden DDoS-Bedrohungslandschaft zu gewährleisten.

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

Die wichtigsten Erkenntnisse

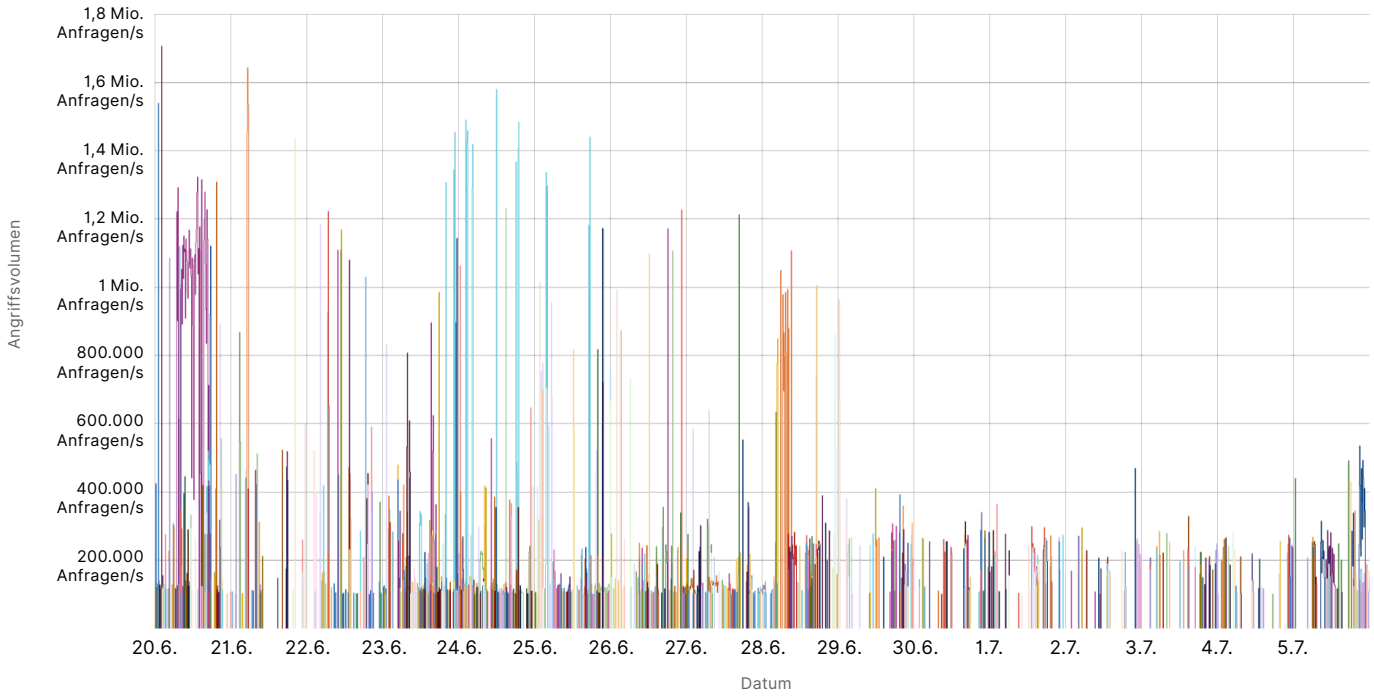
Hacktivisten-Allianz „Darknet Parliament“ in Aktion

Am 14. Juni haben mehrere prorussische Hacktivistengruppen – darunter Killnet, eine Wiederauferstehung von REvil und Anonymous Sudan – bekannt gegeben, dass sie sich unter dem Namen „Darknet Parliament“ zusammengeschlossen haben.

Ihr erklärtes Ziel ist die Durchführung „massiver“ Cyberangriffe auf das westliche Finanzsystem, einschließlich westlicher Banken, des US Federal Reserve System und des SWIFT (Society for Worldwide Interbank Financial Telecommunication)-Netzwerks.

Im Berichtsquartal hat Darknet Parliament bis zu 10.000 DDoS-Angriffe auf Websites ausgeführt, die von Cloudflare geschützt werden. Websites im Bereich Banken und Finanzdienstleistungen standen unter den am häufigsten angegriffenen Branchen allerdings nur an neunter Stelle – gemessen an den von uns im Rahmen dieser Kampagne registrierten Attacken auf unsere Kunden. Unsere Systeme haben die mit dieser Kampagne verbundenen Angriffe automatisch erkannt und abgewehrt.

Branchenübergreifend 10.000 Attacken von Killnet, REvil und Anonymous Sudan im zweiten Quartal 2023



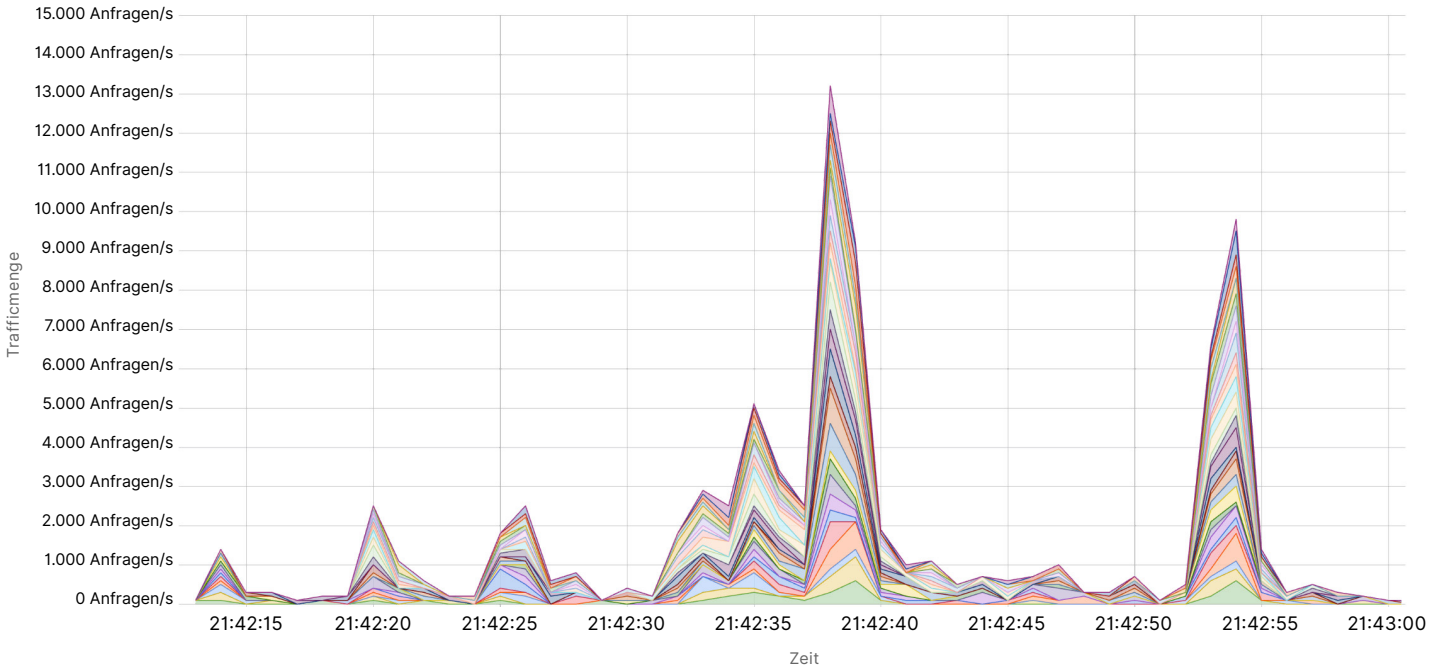
HTTP-DDoS-Angriffe mit geringem Volumen und hohem Zufallsgrad

Bei einem HTTP-DDoS-Angriff wird das Hypertext Transfer Protocol (HTTP) genutzt.Er zielt auf HTTP-Internetpräsenzen wie Websites und API-Gateways ab. In den letzten Monaten haben wir eine Zunahme von HTTP-DDoS-Angriffen mit geringem Volumen und hohem Zufallsgrad verzeichnet. Bisher ist diese Taktik hauptsächlich von gut finanzierten, staatlich geförderten Akteuren angewandt worden.

Es hat den Anschein, als ob die Angriffe absichtlich so gestaltet wurden, dass sie das Browserverhalten von Nutzern sehr genau imitieren und auf diese Weise Abwehrsysteme überwinden. In einigen Fällen wurde bei verschiedenen Präsenzen wie Nutzer-Agenten und JA3-Fingerprints ein hoher Grad an Randomisierung angewandt.

Ein Beispiel für einen solchen Angriff sehen Sie unten. Hier wurde jedem Randomisierungsmerkmal eine eigene Farbe zugewiesen.

HTTP-Datenverkehrsvolumen bei einem HTTP-DDoS-Angriff mit geringer Trafficmenge und hohem Zufallsgrad



DDoS-Angriffe per DNS-Laundering

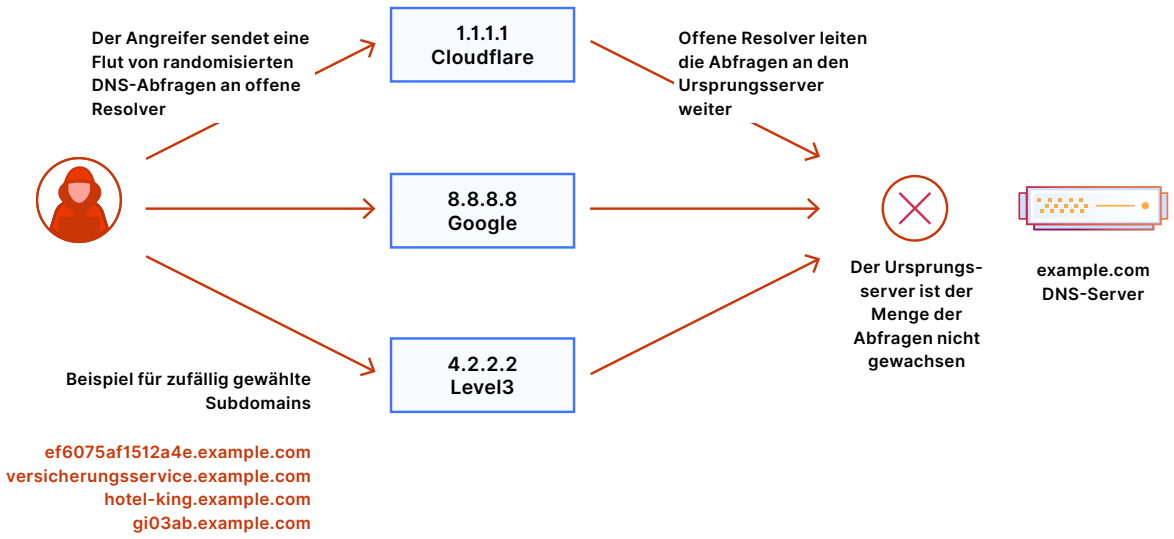
Im Berichtsquartal haben sich DNS-basierte DDoS-Angriffe zum häufigsten DDoS-Angriffsvektor entwickelt: 32 % aller DDoS-Angriffe zielen auf das DNS-Protokoll ab. Das Domain Name System, kurz DNS, ist das Telefonbuch des Internets. DNS hilft bei der Übersetzung der menschenfreundlichen Website-Adresse (z. B. www.cloudflare.com) in eine maschinenfreundliche IP-Adresse (z. B. 104.16.124.96). Durch die Störung von DNS-Servern beeinträchtigen Angreifer die Fähigkeit der Rechner, eine Verbindung zu einer Website herzustellen, wodurch diese für die Nutzer nicht mehr erreichbar ist.

Eine besorgniserregende und sich gerade schnell verbreitende Angriffsform ist das DNS Laundering. Solche Attacken können Unternehmen, die ihre eigenen autoritativen DNS-Server betreiben, vor große Herausforderungen stellen. Bei einem DNS-Laundering-Angriff wird bösartiger Datenverkehr über seriöse rekursive DNS-Resolver geleitet und auf diese Weise „gewaschen“, sodass er als gutartiger, legitimer Traffic erscheint. Das lässt sich mit Geldwäsche vergleichen, bei der „schmutziges Geld“ gewaschen wird, um den Anschein zu erwecken, dass es aus legalen Quellen stammt.

Bei einem DNS-Laundering-Angriff fragt der Bedrohungsakteur Subdomains einer Domain ab, die vom DNS-Server des Opfers verwaltet wird. Das Präfix, das die Subdomain definiert, ist zufällig und wird bei einem solchen Angriff nie mehr als ein- oder zweimal verwendet. Rekursive DNS-Server haben aufgrund der Randomisierung nie eine Antwort im Cache und müssen die Anfrage an den autoritativen DNS-Server des Opfers weiterleiten. Der autoritative DNS-Server wird dann mit so vielen Anfragen bombardiert, dass er legitime Anfragen irgendwann nicht mehr bearbeiten kann oder sogar ganz zusammenbricht.

Zu den jüngsten Opfern solcher Angriffe gehören ein großes asiatisches Finanzinstitut und ein nordamerikanischer DNS-Anbieter. Die Quellen umfassen seriöse rekursive DNS-Server wie 8.8.8.8 von Google und 1.1.1.1 von Clouflare. Die angegriffene Domain ist gültig und muss legitime Abfragen bearbeiten. Daher können DNS-Administratoren weder die Angriffsquelle noch alle Abfragen an die angegriffene Domain blockieren. Es ist schwierig, legitime Abfragen von bösartigen zu unterscheiden.

Abfolge eines DDoS-Angriffs per DNS-Laundering

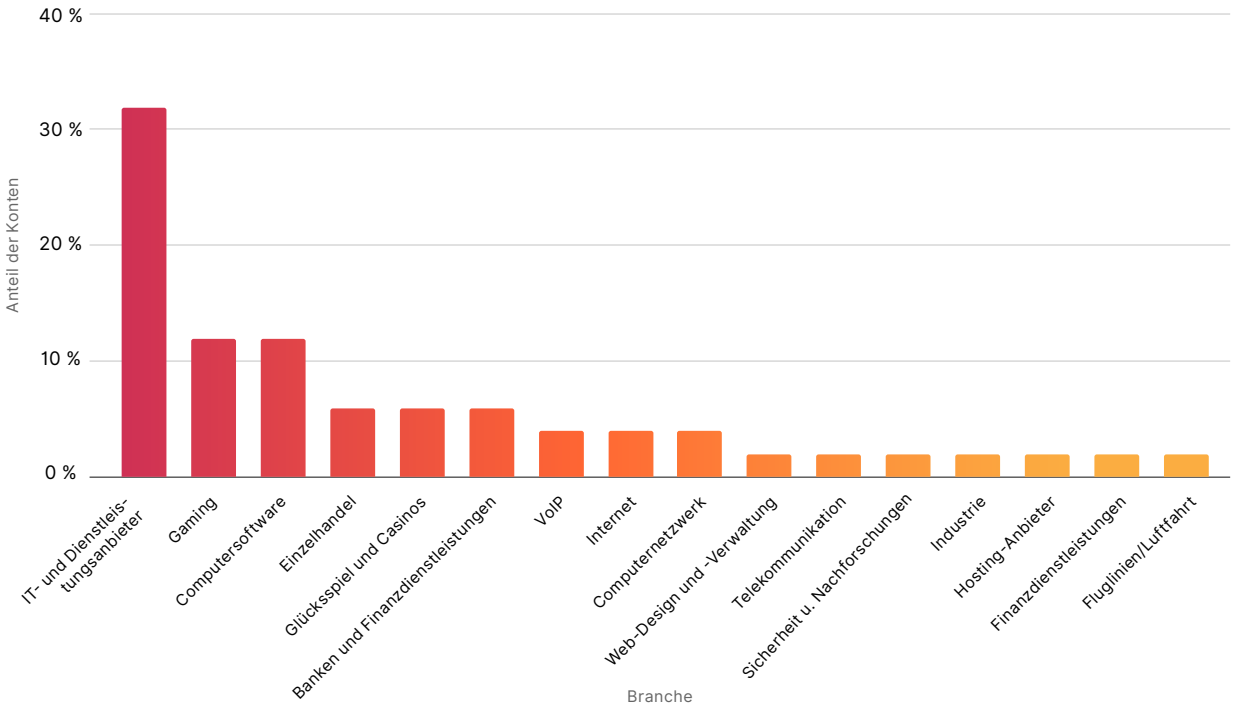


„Startblast“: Ausnutzung von Mitel-Exploits für DDoS-Angriffe

Auf UDP-Ebene haben wir Angriffe beobachtet, die eine von uns im März 2022 veröffentlichte Zero-Day-Schwachstelle (CVE-2022-26143, TP240PhoneHome) ausgenutzt haben. Zusammen mit anderen Mitgliedern der Informationssicherheitsbranche haben wir im Geschäftstelefonsystem Mitel MiCollab diese Sicherheitslücke ausfindig gemacht, die das System für DDoS-Angriffe per UDP-Amplification anfällig macht.

Der Kampagnenname „Startblast“ stammt von dem gleichnamigen Debugging-Befehl, der für die Ausnutzung dieser Schwachstelle entscheidend ist. Unserer Beobachtung nach waren von dieser Angriffsart allen voran IT- und Service-Provider betroffen, mehr als die Glückspiel- und Gamingbranche. Unter den DDoS-Angriffen auf Netzwerkschicht hat dieser Typ von Attacke im Berichtsquartal am schnellsten zugenommen.

Starblast-Angriffskampagnen nach Branchen im zweiten Quartal 2023



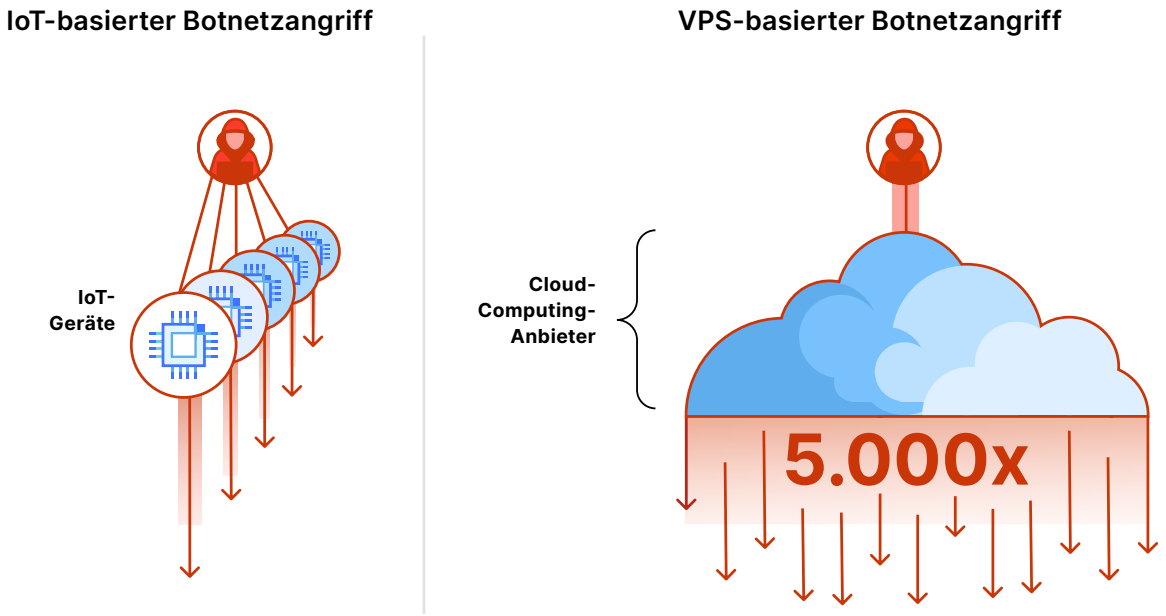
Schlagkräftige Botnetze weiter auf dem Vormarsch

Wie bereits im Cloudflare-Bericht zu DDoS-Trends für das erste Quartal 2023 beschrieben, ist nach wie vor eine Weiterentwicklung der Botnetz-DNA zu beobachten. Die Ära der VM-basierten DDoS-Botnetze ist angebrochen und mit ihr treten hypervolumetrische DDoS-Angriffe auf den Plan. Diese Botnetze bestehen nicht aus Geräten des Internet of Things (IoT), sondern aus virtuellen Maschinen (VMs oder Virtual Private Servers [VPS]). Das macht sie sehr viel – bis zu 5.000 Mal – schlagkräftiger.

Im Kampf gegen diese neuen Botnetze arbeitet Cloudflare mit führenden Cloud-Computing-Anbietern zusammen. Das hat bereits erste Ergebnisse gezeitigt: Wesentliche Teile dieser Botnetze konnten neutralisiert werden. Im zweiten Quartal 2023 haben wir seitdem keine weiteren hypervolumetrischen Angriffe (in der Größenordnung des ersten Quartals 2023 und der Zeit davor) mehr registriert.

Wir haben das Ziel, diese Zusammenarbeit zu automatisieren und weiter auszubauen. Wir bitten Cloud-Computing- und Hosting-Anbieter sowie andere allgemeine Service-Provider, sich an dem Botnet Threat Feed von Cloudflare zu beteiligen.

Für die Anbieter ist das kostenlos und wir verkaufen keine Daten an Dritte. Auf diese Weise erhalten wir Einblick in Angriffe, die von den eigenen Netzwerken der Dienstanbieter ausgehen. Das trägt zu unseren gemeinsamen Bemühungen bei, Botnetze zu zerschlagen.



Die wichtigsten DDoS-Trends im zweiten Quartal 2023

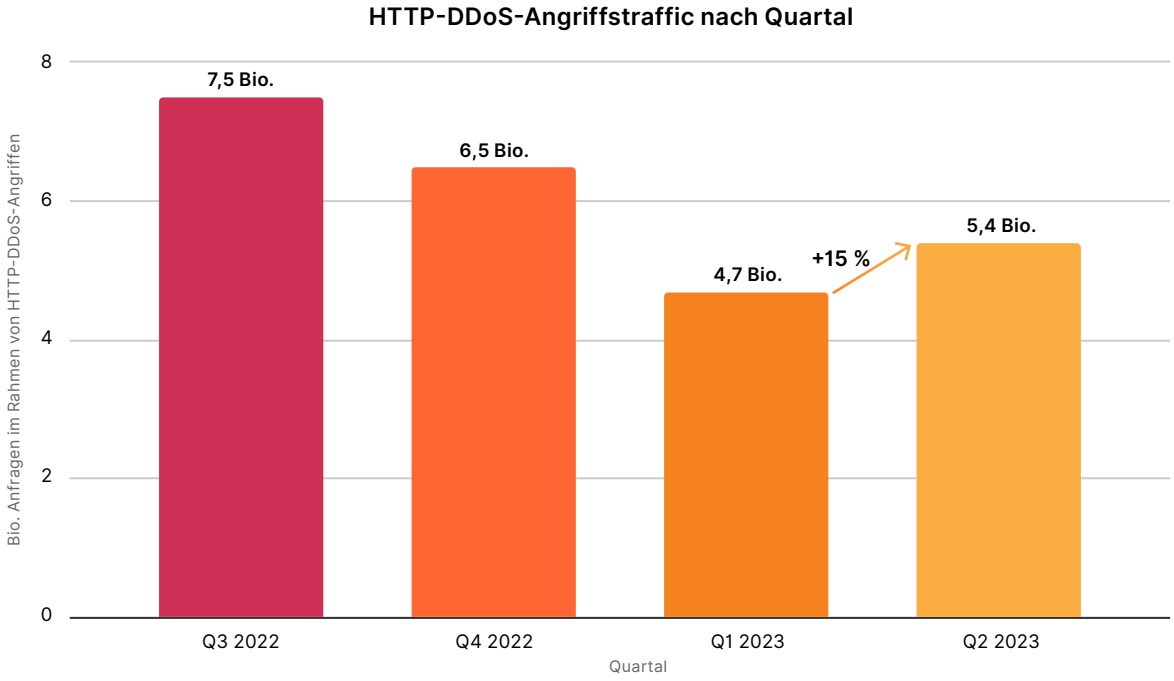
In den folgenden Abschnitte werden die wichtigsten Trends im Hinblick auf Angreifer und Angriffsziele erörtert.

Gesamtveränderung der Trafficmenge

DDoS-Angriffe auf Anwendungs- und Netzwerkschicht sind in den ersten sechs Monaten 2023 im Vergleich zum Vorjahreszeitraum um 35 % bzw. 14 % gesunken. Bei Cloudflare hoffen wir, dass sich dieser Abwärtstrend fortsetzt, da wir und die gesamte Informationssicherheitsbranche Cyberkriminellen das Leben schwerer machen.

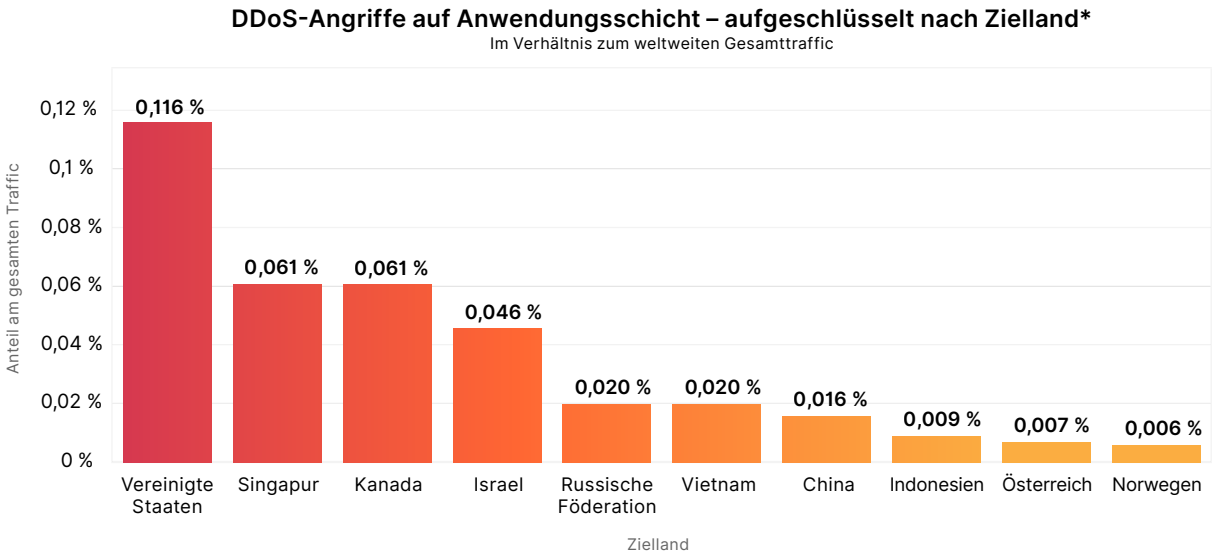
Wir möchten allerdings darauf hinweisen, dass die Zahl der DDoS-Angriffe auf Anwendungsschicht im zweiten Quartal 2023 um 15 % im Jahresvergleich gestiegen ist. Lassen Sie bei Ihren Bemühungen um größtmögliche Sicherheit nicht nach!

Insgesamt haben HTTP-DDoS-Angriffe im Quartalsvergleich um 15 % zugelegt, während sie gegenüber demselben Vorjahreszeitraum um 35 % zurückgegangen sind. Darüber hinaus haben sich die DDoS-Angriffe auf Netzwerkschicht im Berichtsquartal gemessen an den vorangegangenen drei Monaten um etwa 14 % verringert.



Die am stärksten angegriffenen Länder

Im letzten Quartal haben wir berichtet, dass Israel das am häufigsten von DDoS-Angriffen auf Anwendungsschicht betroffene Land war. Diesmal liegen die Websites in den Vereinigten Staaten wieder an der Spitze, gefolgt von denen in Singapur an zweiter und Kanada an dritter Stelle. Die Attacken auf israelische Websites haben um 33 % abgenommen, sodass das Land nun auf Rang vier liegt.



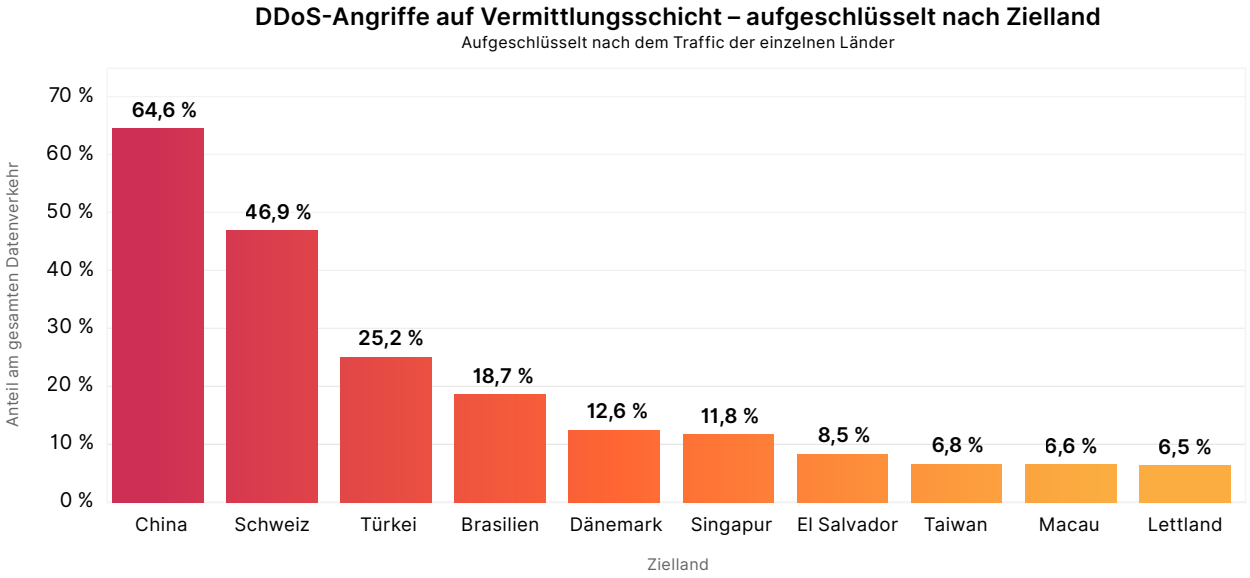
⚠ 2x mehr DDoS-Angriffe auf Anwendungsschicht

Gegen die Vereinigten Staaten richten sich zweimal mehr DDoS-Angriffe auf Anwendungsschicht als gegen das am zweithäufigsten attackierte Land

⚠ Mehr als 10 %

DDoS-Angriffe sind in Palästina und Sankt Kitts und Nevis für mehr als 10 % des gesamten Datenverkehrs auf Anwendungsschicht verantwortlich

Wenn es um die meisten DDoS-Angriffe auf Netzwerkschicht geht, führt China die Länderliste erneut an. Jedes zweite von drei Bytes in chinesischen Netzwerken stand im zweiten Quartal 2023 mit DDoS-Angriffen in Verbindung. Diesen hohen Anteil an bösartigem Datenverkehr, der auf China abzielte, haben wir schon in mehreren Quartalen verzeichnet. Die einzigartige Situation im ersten Quartal 2023, in dem 83 % der für finnische Netzwerke bestimmten Bytes DDoS-Angriffe enthielten, ist inzwischen nicht mehr gegeben. Deshalb ist Finnland nun nicht mehr in den Top Ten der am häufigsten von DDoS-Angriffen betroffenen Länder und Regionen vertreten.

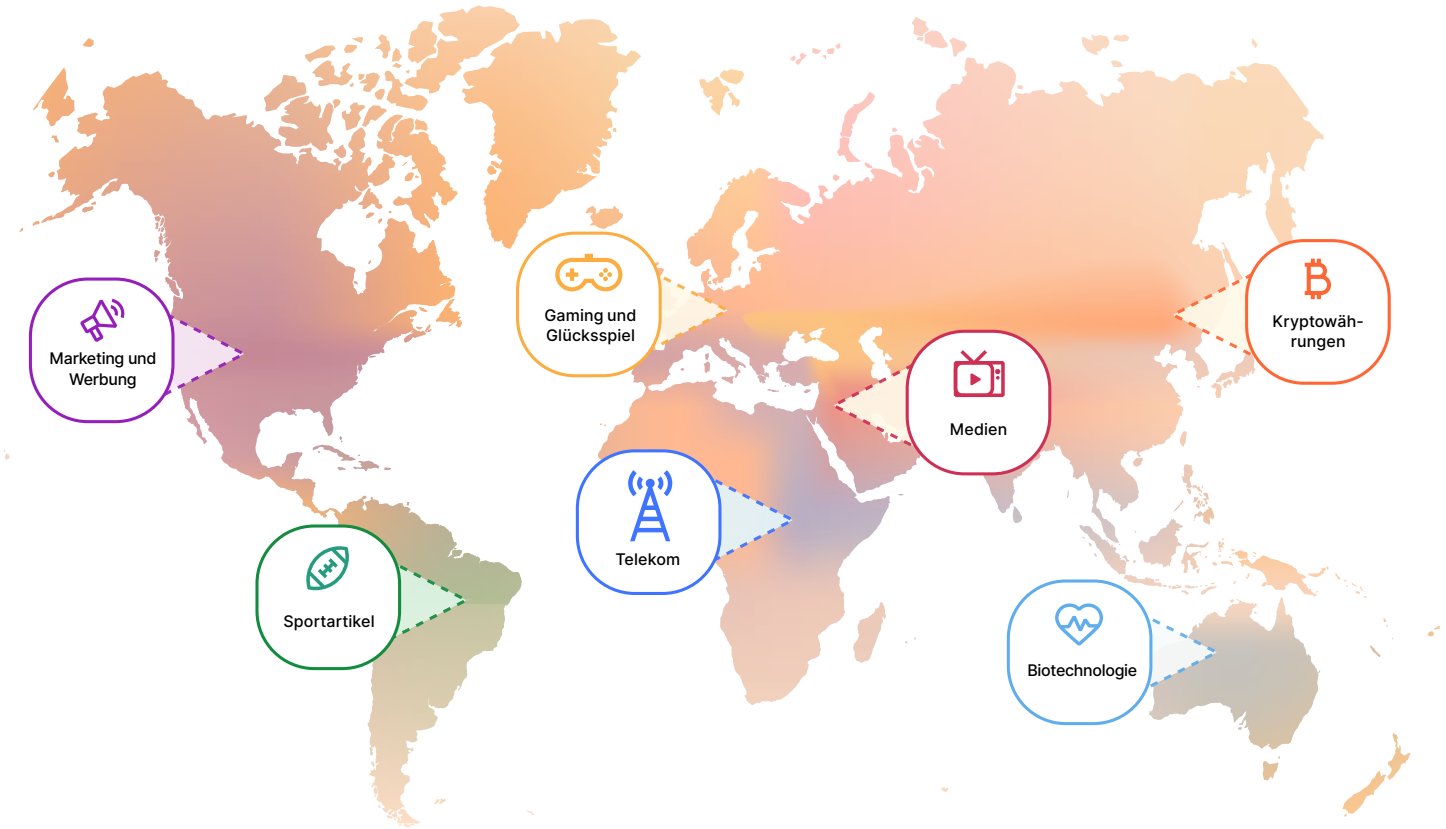


Branchen- und regionsspezifische Unterschiede bei DDoS-Angriffen

Der größte Teil des HTTP-DDoS-Angriffstraffics hat sich im zweiten Quartal 2023 gegen Kryptowährungs-Websites gerichtet. Sechs- von zehntausend HTTP-Anfragen an solche Websites waren Teil dieser Attacken. Das entspricht einem Anstieg von 600 % im Quartalsvergleich.

Gaming- und Glücksspiel-Websites stehen an zweiter Stelle; ihr Anteil an den Angriffen hat sich in derselben Zeit um 19 % erhöht. Knapp dahinter liegen Websites aus dem Bereich Marketing und Werbung, wobei sich ihr Anteil bei den Angriffen kaum verändert hat.

Leider stehen gemeinnützige Organisationen stark unter Beschuss. Tatsächlich handelte es sich bei 12 % des an Non-Profit-Organisationen gerichteten HTTP-Traffics um DDoS-Angriffe, womit die Branche hinsichtlich des Anteils am Datenverkehr Rang zwei erreichte. Im Rahmen des Projekts „Galileo“, das dieses Jahr sein neuntes Jubiläum gefeiert hat, schützt Cloudflare mehr als 2.271 Non-Profit-Organisationen in 111 Ländern . In den vergangenen Monaten waren gemeinnützige Organisationen täglich Ziel von durchschnittlich 67,7 Mio. Cyberangriffen.



Am meisten angegriffene Branche nach Region

Empfehlungen und Schlussfolgerungen

Best Practices	Cloudflare-Nutzung optimieren
Aktualisieren oder erstellen Sie einen Denial-of-Service-Reaktionsplan.	Haben Sie Cloudflare-Warnmeldungen und -Bedrohungsdaten in Ihre Sicherheitsabläufe integriert? Wissen Sie, wie Sie alle erforderlichen Mitarbeitenden im Fall eines Angriffs erreichen können? Sind diese für den Reaktionsplan geschult?
Setzen Sie Bedrohungsdaten und integrierte, automatisierte Lösungen zur DDoS-Abwehr ein.	Nutzen Sie mehrere Erkennungsverfahren, um den in diesem Bericht aufgeführten Angriffstrends zu begegnen: 1. Dynamisches zustandsloses Fingerprinting 2. Auf maschinellem Lernen basierende Klassifizierung 3. Erkennung von irregulärem Datenverkehr 4. Erstellung von Trafficprofilen und zustandsabhängige Abwehrmaßnahmen 5. Bedrohungsdaten zu aktuellen DDoS-Aktivitäten und -Trends
Bringen Sie Ihre Infrastruktur auf den neuesten Stand, um sie entsprechend Ihres Datenverkehrsprofils widerstandsfähiger zu machen. **Verbessern Sie die Netzwerk- und Anwendungsperformance, um Nadelöhre zu vermeiden.**	Stellen Sie sicher, dass die Kapazität Ihrer DDoS-Abwehr-Tools ausreicht, um die gegenüber früheren Zeiten doppelt so großen Angriffe und doppelt so hohen Maximalraten Ihres legitimen Datenverkehrs bewältigen zu können. Nutzen Sie eine automatische Reduzierung der HTTP/2-Multiplexing-Obergrenze bei Angriffen; aktivieren Sie eine WAF. Verwenden Sie einen digitalen Warteraum. 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 für Ihr Unternehmen wichtige und genutzte Ports offen. Verwenden Sie Schemavalidierung und ein API-Gateway für API-Datenverkehr.
Nutzen Sie Bedrohungsdaten und künstliche Intelligenz, um neuen Bedrohungen immer einen Schritt voraus zu sein.	Greifen Sie auf Bot-Scores zurück, die in Firewall- und Durchsatzbegrenzungsregeln verwendet werden können.

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

Im Webinar zum Thema DDoS-Trends erfahren Sie mehr über diese neuen DDoS-Bedrohungen und wie Sie sich davor schützen können.

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

REV:BDES-4839.2023AUG28