Distributed Denial of Service Report

für das 1. Halbjahr 2021

Die Bedrohungslage durch DDoS-Attacken im 1. Halbjahr 2021

+ 33 %

höhere Anzahl an DDoS-Attacken

555 GBPS

als Höchstwert bei der Angriffsbandbreite

+ 36 %

Zunahme des maximalen Angriffsvolumens

+ 100 %

Zunahme der Hochvolumen-Attacken von Q1 vs. Q2 2021

+ 147 %

Anstieg der maximalen Paketrate

65 %

aller Angriffe waren komplexe Multivektor-Attacken

DDoS-Attacken, die im 1. Quartal 2021 für Schlagzeilen sorgten

4. Januar 2021

Schulplattformen unter Beschuss

Bundesweit waren im Januar Schulserver und digitale Lernplattformen wie Moodle, die Schul-Cloud des Hasso-Plattner-Instituts und Lernsax von DDoS-Attacken betroffen. Die Umsetzung des Distanzunterrichts in Pandemiezeiten wurde dadurch erschwert. [1]

13. Januar 2021

Langsames Internet auf Malta

Der maltesische Internet-Provider Melita wurde mit DDoS-Attacken erpresst. Die Angriffe führten für mehrere Stunden zu einer deutlichen Verlangsamung der Internetverbindungen im gesamten Land, konnten dann aber erfolgreich eingedämmt werden. [2]

30. Januar 2021

Digitales Fernsehen in Island nicht erreichbar

Das Streaming-TV-Angebot des isländischen Telekommunikationsanbieters Siminn war auf einen Samstagabend und dazu in Pandemie nicht erreichbar. Nach ca. zwei Stunden war der DDoS-Angriff gestoppt und der Service wieder erreichbar. [3]

Januar - März 2021

Impfportale weltweit durch Angriffe gestört

In mehreren Ländern wie Großbritannien, Deutschland und den USA häuften sich Meldungen von Cyber-Angriffen auf Impfportale. Die Webseiten, die der Buchung von Impfterminen mit dem COVID-19-Impfstoff dienen, wurden mit DDoS-Attacken überlastet. [4]

18. Februar 2021

Österreichweite Internet-Ausfälle

Beim Festnetzinternet des Telekommunikationsanbieters A1 kam es zu einem zweistündigen Ausfall im ganzen Land, was in Pandemiezeiten im Home-Office problematisch war. Schuld waren DDoS-Attacken, die zu einem Routing-Problem geführt hatten. (5)

8. März 2021

Parlamentswebseite in Italien offline

Die institutionelle Webseite der Abgeordnetenkammer, die mit dem Senat das italienische Parlament bildet, war über einen Tag nicht erreichbar. Die Täter hinter dem Angriff und ihr Motiv blieben unklar. [6]

DDoS-Attacken, die im 2. Quartal 2021 für Schlagzeilen sorgten

4. Mai 2021

Staatliche Einrichtungen in Belgien offline

Dienste und Webseiten von mehr als 200 staatlichen Organisationen und Institutionen in Belgien waren mehrere Stunden digital nicht erreichbar. Auslöser waren Angriffe auf den ISP Belnet, der u. a. das Netzwerk für die belgische Regierung bereitstellt. (7)

15. Mai 2021

Versicherer zieht Zorn von Cyberkriminellen auf sich

Nachdem der Versicherungskonzern AXA in Frankreich Kürzungen von Cyberversicherungen für Ransomware-Attacken angekündigt hatte, wurde er selbst attackiert. Etliche Niederlassungen in Südostasien wurden Opfer von Datenverschlüsselung und DDoS-Attacken. (9)

9. Juni 2021

Großflächige Stromausfälle in Puerto Rico

Im Karibikstaat gingen bei gut 700.000 Einwohnern die Lichter aus, nachdem erst eine DDoS-Attacke den Energieversorger getroffen hatte und nur wenige Stunden später ein Umspannungswerk in Flammen aufging. (11)

18. Mai 2021

ISP in Irland im Visier

In der ersten Maihälfte wurden zahlreiche ISPs in Irland das Ziel von DDoS-Attacken. So wurde mit Blacknight einer der größten Web-Hosting-Anbieter des Landes angegriffen. Dabei kam es zu zahlreichen mehrstündigen Ausfällen. Die Angriffe wurden vielfach von DDoS-Erpressungen begleitet. (8)

3. Juni 2021

Kein Online-Banking bei deutschen Volksbanken

Im genossenschaftlichen Bankensektor kam es zu mehrstündigen IT-Großstörungen im Online-Banking sowie bei den Apps. Die Ursache waren DDoS-Attacken auf die Rechenzentren des IT-Dienstleisters. (10)

25. Juni 2021

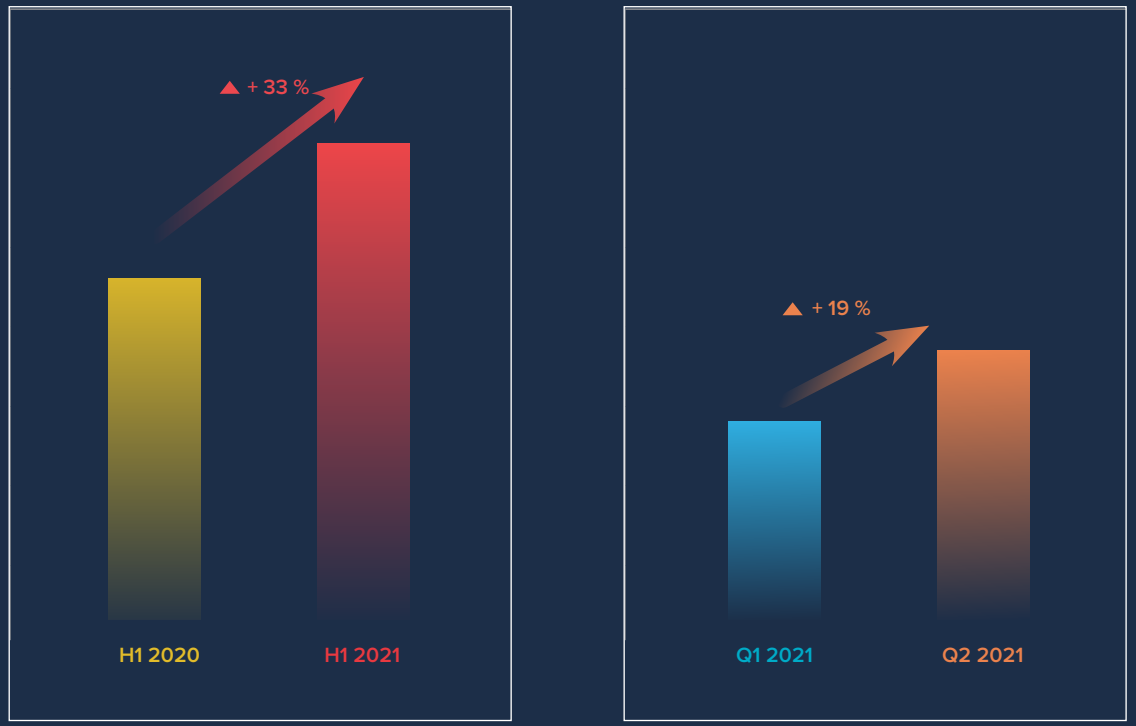
Banken in Israel unter Beschuss

Mehrere Banken in Israel wurden zum Ziel von DDoS-Attacken. Eine pro-palästinensische malayische Hackergruppe bekannte sich auf Telegram zu den Angriffen als Zeichen des politischen Protests im Israel-Gaza-Konflikt. (12)

Weiterer Anstieg bei Anzahl der DDoS-Attacken

Im ersten Halbjahr 2021 starteten Cyberkriminelle eine rekordverdächtige Anzahl von Angriffen. Das LSOC verzeichnete ein Drittel (33 %) mehr Angriffe als im Vorjahreszeitraum des DDoS-Rekordjahres 2020. Mehr als ein Fünftel der Angriffe (27 %) entfielen auf das Wochenende. Die Anzahl und die Wucht von DDoS-Angriffen haben von Januar bis Juni noch einmal zugenommen. So verzeichnete das LSOC im 2. Quartal 19 % mehr Angriffe als im Quartal davor. Damit hat sich die ohnehin hohe Bedrohungslage durch diese Angriffsform noch einmal verschärft. Ein Ende des Booms für DDoS-Attacken ist nicht abzusehen.

Nach Einschätzung der Experten ist diese Entwicklung auf die anhaltenden Pandemie-Bedingungen zurückzuführen, die die Digitalisierung beschleunigt und damit immer neue Einfallstore für Angreifer geöffnet haben. Viele Angriffe zielten auf Web-Services, die das Leben, Lernen und Arbeiten unter Pandemie-Bedingungen sicherstellten. Dazu zählten Impfplattformen, Lernportale und IT-Infrastrukturen für das mobile Arbeiten im Home-Office. Außerdem standen Hosting Provider und ISPs, die die Express-Digitalisierung in Wirtschaft und Gesellschaft erst ermöglichten, unter Beschuss.



Entwicklung der Angriffszahlen

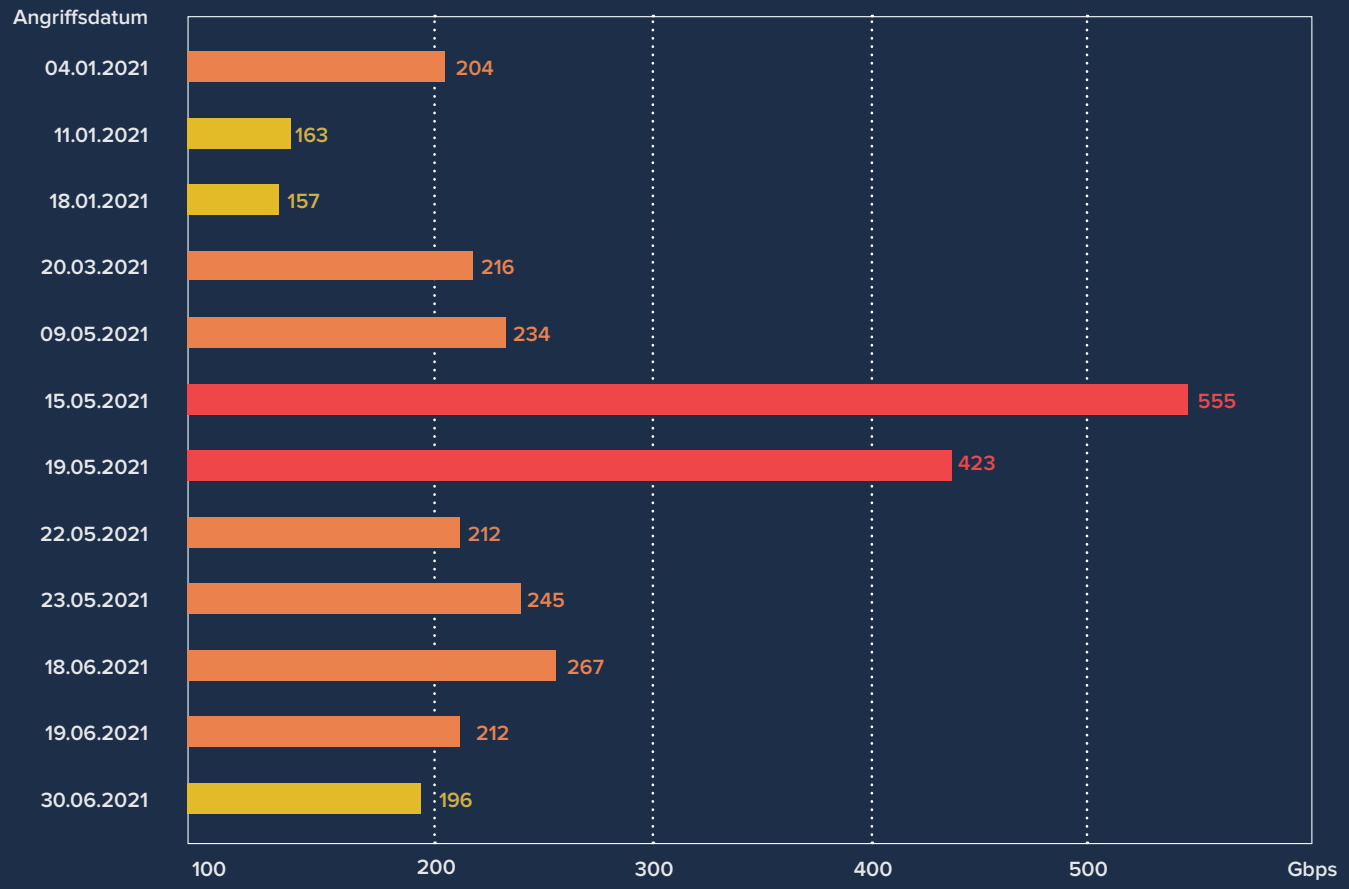
Hochvolumen-Attacken häufen sich

Das LSOC hat von Januar bis Juni über 40 Attacken registriert, deren jeweiliges Angriffs-volumen 100 Gbps überstieg. Im Vorjahreszeitraum waren es nur knapp 30 Angriffe gewesen. Zwei Drittel dieser Angriffe entfielen auf das 2. Quartal 2021. Dazu kamen über beide Quartale hinweg 234 weitere Attacken mit Bandbreitenspitzen zwischen 20 und 100 Gbps. Die größte Attacke des ersten Halbjahres stoppte bei 555 Gbps und überstieg die maximale Angriffsbandbreite des Vorjahreszeitraums um knapp 38 %.

Bei dem Angriff, der Mitte Mai stattfand und auf ein Unternehmen im Bereich Media/ Entertainment zielte, handelte es sich um eine DNS-Reflection-Attacke. Neben dem großen Angriffs-volumen stach die Attacke auch wegen ihrer langen Dauer von 63 Minuten heraus. Meist enden Hochvolumen-Attacken nach wenigen Minuten, um die Ressourcen der Angreifer zu schonen. Im ersten Halbjahr fanden sich zahlreiche weitere Attacken mit großen Angriffs volumen und sehr langer Dauer:

204 Gbps und 173 Minuten
163 Gbps und 724 Minuten
102 Gbps und 62 Minuten
93 Gbps und 75 Minuten
80 Gbps und 500 Minuten.

In keinem der Fälle gelang es dem sehr hartnäckigen Angreifer sein Ziel zu erreichen und sein Ziel offline zu nehmen.



DDoS-Erpressungen: Bitcoin-Forderungen im Namen von Fancy Lazarus

Seit Anfang des Jahres 2021 sorgten mehrere Wellen von DDoS-Erpressungen (RDDoS – Ransom Distributed Denial of Serivce) für eine angespannte Gefahrenlage. Die Höhepunkte der Erpresseraktivitäten lagen im Januar und im Juni. Die Täter gaben sich als Fancy Lazarus aus. Das Vorgehen des oder der Täter war in weiten Teilen identisch mit den kriminellen Aktivitäten der DDoS-Erpresser, die unter den Namen Armada Collective, Fancy Bear und Lazarus-Group seit dem Sommer 2020 agierten.

Ziele in der Wirtschaft

Unternehmen aus den verschiedensten Wirtschaftsbereichen haben die Erpresser-Mails von Fancy Lazarus erhalten, darunter Finanzen, E-Commerce, Medien, Logistik, Produktion, Konsumgüter, Telekommunikation und Hosting-Provider. Meldungen über RDDoS-Angriffe gingen beim LSOC aus mehreren europäischen Ländern wie Deutschland, Österreich, Großbritannien, Irland sowie aus den USA und Kanada ein. Statt wahllos vorzugehen, variierten die Lösegeldforderungen je nach Unternehmensgröße und Branche der Opfer. Vielfach wurden 2 Bitcoins (Stand 2. Juni 2021 ca. 75.000 Euro) gefordert.

Das Vorgehen der Täter

Die Täter informierten sich im Vorfeld über die IT-Infrastruktur des Unternehmens und machten in der Erpresser-Mail eindeutige Angaben dazu, welche Server und IT-Elemente sie für die Warn-Attacken angreifen werden. Sie überprüften zudem anhand von Routing-Informationen, ob ein externer DDoS-Schutz vor das Unternehmens-Netzwerk geschaltet ist, der eingehenden Datenverkehr permanent auf Anomalien prüft. War dies nicht der Fall, starteten die Angreifer als Druckmittel teils mehrstündige Demo-Attacken, die sich durch hohe Volumen von bis zu 200 Gbps auszeichneten. Um diese Angriffsbandbreiten zu erreichen, denen im Allgemeinen nur dedizierte Schutzlösungen von spezialisierten Schutzanbietern standhalten, setzten die Täter Reflection-Amplification-Vektoren wie DNS ein. Sollten die Forderungen nicht erfüllt werden, drohten massive Hochvolumen-Attacken von bis zu 2 Tbps. Für den Transfer der Bitcoins an eine spezifische Bitcoin Wallet blieben dem Unternehmen 7 Tage Zeit.

Nichtzahlung und Folgeangriffe

Unternehmen, die ins Visier der DDoS-Erpresser geraten, stehen vor der Wahl, ob sie zahlen oder sich auf eine Auseinandersetzung mit den Angreifern einlassen. Das LSOC hat keine Informationen vorliegen, ob schon Kryptogelder an Fancy Lazarus geflossen sind. Es gibt allerdings keine Gewissheit, dass mit der Lösegeldzahlung die Angriffe enden. Eine Erpresserwelle folgt der nächsten. Zwar traten immer wieder Tätergruppen mit neuen Namen in Erscheinung, um so ihren Forderungen Nachdruck zu verleihen, unklar blieb jedoch, wer sich tatsächlich hinter den Angriffen verbirgt. Diejenigen Unternehmen, die sich für die Integration eines professionellen DDoS-Schutzes entschieden haben, waren mit Ablauf des gesetzten Ultimatums gut vorbereitet und gegen die Angriffe gewappnet. Die Folge-Attacken liefen ins Leere und konnten erfolgreich abgewehrt werden. Der hohen Anzahl an Notfall-Onboardings, die zwischen Januar und Juni durch das LSOC realisiert wurden, standen keinerlei DDoS-bedingte Ausfallzeiten für die nun geschützten Infrastrukturen gegenüber.

Erpressung mit DDoS-Attacken: eine Chronologie

DDoS-Erpressungen stellen schon seit mehreren Jahren ein ernsthaftes Problem für die Wirtschaft dar. Das LSOC warnte erstmals 2014 vor der Gefahr, die damals von der international agierenden Gruppe DD4BC ausging. Seitdem häuften sich die Vorfälle, und vom KMU bis zum Weltkonzern sind inzwischen Unternehmen fast aller Größen und Branchen zum Ziel geworden. Unter den Tätern gibt es zahlreiche Trittbrettfahrer und Nachahmer, die sich an finanziell scheinbar erfolgreichen Erpresserbanden orientieren und deren Geschäftsmodell von der Kontaktaufnahme bis zum Erpresserschreiben kopieren aber dennoch bluffen. Immer mehr Täter meinen es jedoch sehr ernst und investieren viel kriminelle Energie und Ressourcen, um an Kryptowährungen zu gelangen. Gegen die hartnäckigen Erpressungen und gezielten DDoS-Attacken, mit denen Druck auf das attackierte Unternehmen ausgeübt wird, helfen nach den Erfahrungen des LSOC nur dedizierte Schutzlösungen. Welche Täter das LSOC in der Vergangenheit schon beobachtet hat, zeigt die folgende Chronologie.

2014

Angreifer: DD4BC (DDoS for Bitcoins)

2015

Angreifer: Armada Collective

2016

Angreifer: Kadyrovtsy, Lizard Squad, Armada Collective

Bluffer: New World Hacking Groups, Red Door, Gladius

2017

Angreifer: XMR-Squad, ZZb00t

Bluffer: Stealth Raven, Phantom Squad

2019

Angreifer: Turkish Hackers, Fancy Bear

2020

Angreifer: Armada Collective, Fancy Bear, Cozy Bear, Lazarus Group

2021

Angreifer: Fancy Lazarus

Die 5 bekanntesten DDoS-Erpressungen

Häufig bewahren Unternehmen, die zum Ziel von DDoS-Erpressungen werden, darüber Stillschweigen, um ihr eigenes Image nicht zu beschädigen. Bei exponierten Services wie Banken und Finance sowie E-Commerce sind die Ausfallzeiten jedoch kaum zu verbergen. Andere Firmen suchen hingegen die Öffentlichkeit, um vor der Gefahr zu warnen.

November 2015

Protonmail

Der Schweizer Krypto-Web mailanbieter Protonmail wurde im Namen von Armada Collective erpresst. Das Unternehmen zahlte das Lösegeld in Höhe von gut 5800 Franken. Die Angriffe gingen danach dennoch weiter. (13)

April 2017

DHL, Hermes und Ebay

DDoS-Erpresser unter dem Namen XMR-Squad attackierten gezielt deutsche Versanddienstleister. Neben DHL waren auch Hermes und die Versandseiten des Marktplatzes Ebay Ziel der Angriffe. Die Angreifer forderten 250 Euro für die Prüfung der (DDoS) Protection. (14)

Oktober 2019

Südafrikanische Banken

Zahlreiche große Banken in Südafrika wurden mit DDoS-Attacken erpresst, Online-Banking-Services fielen aus. Es wurde vermutet, dass die Angreifer die Attacke gezielt am Pay Day starteten, um den größtmöglichen Schaden zu verursachen. (15)

März 2020

Lieferdienst Lieferando

Der deutsche Essenslieferdienst Lieferando hatte in den landesweiten Lockdowns der Corona-Krise Hochkonjunktur. Hacker machten sich das zunutze: Sie starteten erst DDoS-Attacken auf Pizza.de und forderten dann zwei Bitcoins, deren Zahlung das Unternehmen aber verweigerte. (16)

August 2020

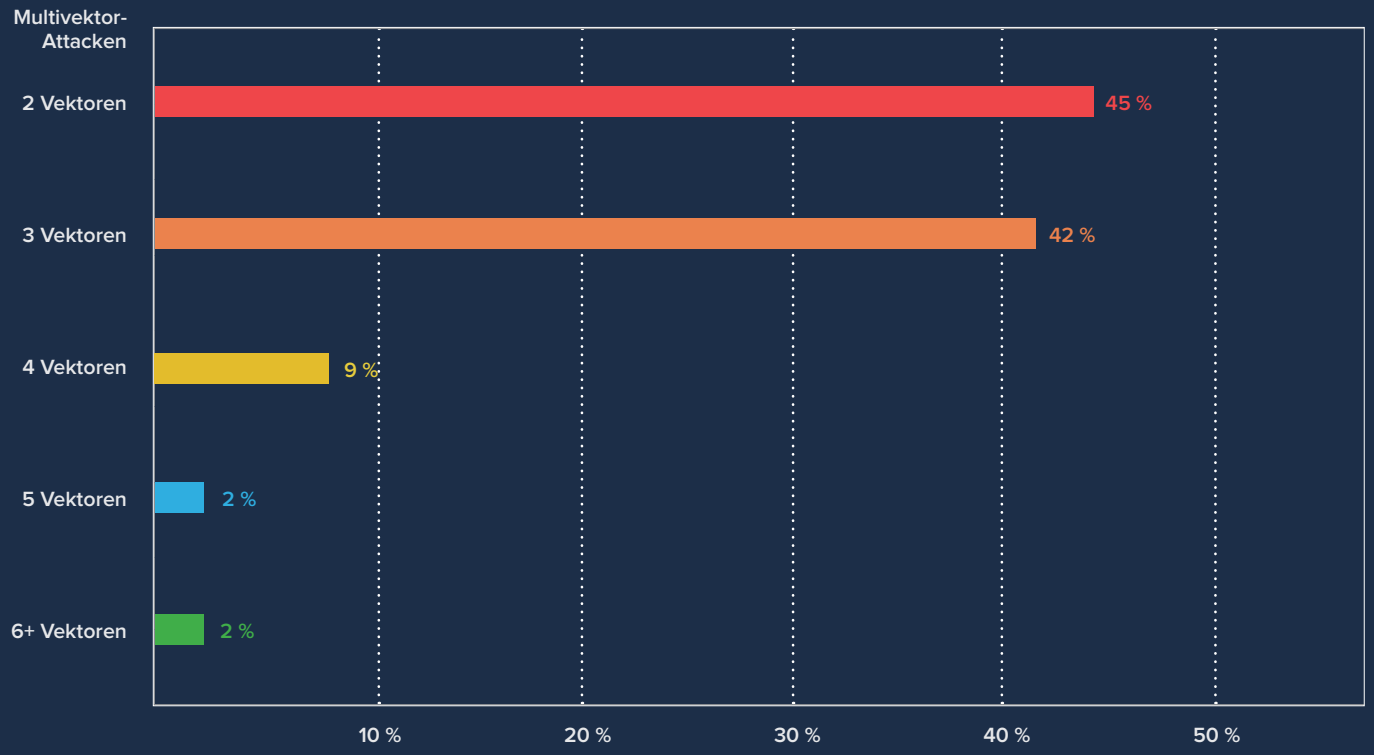
Börse Neuseeland

Die mehrtägigen Ausfälle an der Börse von Neuseeland im August 2020 wurden DDoS-Erpressern zugerechnet. Weitere 100 Banken, Börsen, Versicherungen und andere Finanzunternehmen weltweit, darunter PayPal und MoneyGram, wurden ebenfalls attackiert. (17)

Komplexe Angriffsmuster dominieren

Bei 35 % der Angriffe setzten die Angreifer im 1. Halbjahr auf einen einzelnen Vektor wie UPD oder TCP. Im Vorjahreszeitraum lag der Wert noch bei 48 %. Die Mehrheit der Angriffe (65 %) wies hingegen komplexe Angriffsstrukturen aus, bei denen die Täter mehrere Techniken kombinierten. Die Entwicklung bei DDoS-Attacken geht nach Beobachtung des LSOC seit mehreren Jahren zu deutlich komplexeren Attacken, die parallel auf Schwachstellen in Transport-, Applikations- und Protokollebene zielen. Jede Angriffstechnik und das dafür missbrauchte Protokoll erfordert eine spezielle Strategie in der Erkennung und Abwehr, sodass bei Multivektor-Attacken nicht nur ein Angriff, sondern eigentlich mehrere synchron laufende Attacken gleichzeitig abgewehrt werden müssen. Für die zuverlässige Absicherung der Unternehmens-IT ist es daher wichtig, auf Schutzlösungen zu setzen, die auf allen Filter-Ebenen von Multivektor-Attacken effektiv arbeiten.

Unter den Multivektor-Attacken waren am häufigsten Angriffe mit zwei Vektoren zu finden. Sie machten 45 % aus. Darauf folgten Attacken mit drei Vektoren (42 %) sowie Attacken mit vier Vektoren (9 %). Attacken mit fünf Vektoren machten noch 2 % aller registrierten Angriffe aus. Die höchste Anzahl an Vektoren betrug 12 und wurde in über 20 Angriffen nachgewiesen.



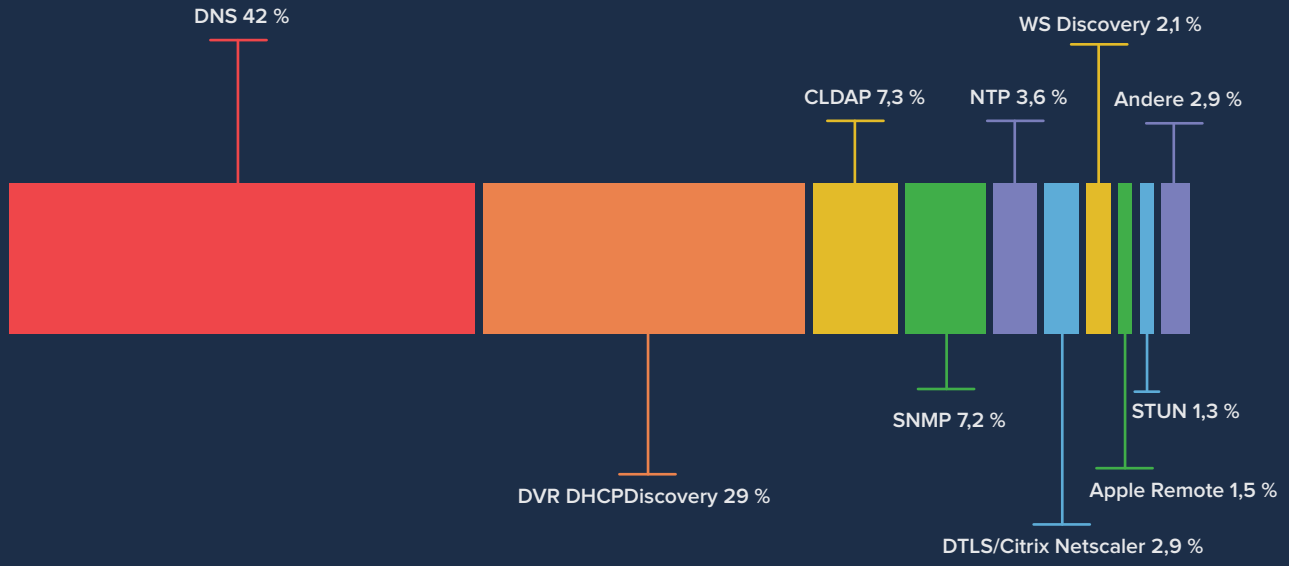
Gefahr durch Reflection-Amplification-Attacken

Reflection-Amplification-Angriffe sind eine Klasse von Multivektor-Angriffen, die verschiedene falsch konfigurierte offene Server und Services im Internet auf ähnliche Art ausnutzen. Dabei wird das Zielsystem nicht direkt angegriffen, sondern es werden dazu Dienste wie DNS oder NTP missbraucht. Der Angreifer sendet dabei zunächst kleine Mengen von Datenpaketen an die zwischengeschalteten Server, die als Verstärker dienen: Sie spiegeln die Anfragen (reflection) und leiten sie vielfach gesteigert (amplification) an das eigentliche Angriffsziel weiter.

Der Internetdienst, der im ersten Halbjahr am häufigsten für Angriffe ausgenutzt und als Verstärker missbraucht wurde, war DNS (42 %) gefolgt von DVR DHCPDiscovery (29 %) und CLDAP (7 %). Das Spektrum dieser auch Reflection-Amplification-Vektoren genannten Dienste wächst mit jedem Jahr und umfasst aktuell über 20 Vektoren. Im 1. Halbjahr sind neue Vektoren wie Datagram Transport Layer Security (DTLS) über Citrix Netscaler und Session Traversal Utilities for NAT (STUN) hinzugekommen:

DTLS wurde entwickelt, um verschlüsselte Daten nicht nur über gesicherte, verbindungsorientierte Transportprotokolle wie TCP, sondern auch über das verbindungslose UDP übertragen zu können.

Ein **STUN**-Server sorgt dafür, dass Endgeräte wie Computer oder VoIP-Telefone, die sich im lokalen Netzwerk hinter einem Router oder einer Firewall verbergen, mit VoIP-Providern im Internet kommunizieren können.



Die wichtigsten Quellenländer für Reflection Amplification Attacken

Die Geräte und Server, die Angreifer für DDoS-Attacken missbrauchen, sind weltweit verteilt. Im 1. Halbjahr kamen die meisten Anfragen von DDoS-Angriffen aus den USA, gefolgt von Deutschland. DDoS-Traffic aus Russland und China, der in den vergangenen Jahren einen Großteil des Datenverkehrs ausgemacht hat, ist deutlich zurückgegangen.

USA	27 %
Deutschland	18 %
China	7 %
Russland	5 %
Brasilien	5 %
Großbritannien	4 %
Ukraine	3 %
Niederlande	3 %
Indien	3 %
Frankreich	2 %

Bei den Quellenländern handelte es sich um den Standort des für den Angriff verwendeten Geräts, nicht um den Standort der Angreifer selbst. Die IP-Adresse der kompromittierten Geräte ist bei Reflection-Amplification-Attacken gespooft, so dass der Ursprung des Angriffs nur sehr schwer zu ermitteln ist.

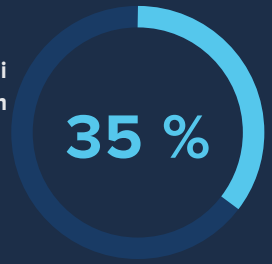
DDoS-Gefahr durch Angriffe aus der Cloud

DDoS-Angreifer holen sich Bandbreite und Rechenleistung für ihre Attacken regelmäßig aus der Cloud. Im 1. Halbjahr 2021 setzten Angreifer bei jeder dritten DDoS-Attacke (35 %) auf Cloud-Ressourcen. Sie kompromittieren Server-Instanzen öffentlicher Cloud Service Provider, indem sie sich über Schwachstellen oder Exploits Zugriff verschafften. Anschließend spielten sie ein vorgefertigtes Script auf, das den Server innerhalb von Minuten in einen DDoS-Bot verwandelt. Die Unternehmen, die die Instanzen angemietet haben, bemerken diesen Fremdzugriff meist nicht oder erst sehr spät, wenn die Abrechnung kommt. Daneben erlangen Kriminelle über gestohlene Kreditkartendaten Zugang und mieten unter falschem Namen Cloud-Instanzen an.

Der Missbrauch der Cloud-Server war Schwankungen unterworfen und reichte von 16 % im Februar bis zu 56 % im Mai 2021. Am häufigsten waren die Cloud-Instanzen von den drei großen Anbieter Amazon Web Services (AWS), Microsoft Azure und Google Cloud nachzuweisen. Daneben nutzten die Angreifer auch Cloud-Angebote aus dem B2B-Bereich wie Oracle Cloud, DigitalOcean IBM Cloud.

Da die Cloud-Nutzung im privaten und im unternehmerischen Umfeld immer weiter wächst, und die Cloud Provider ihre Infrastruktur regelmäßig ausbauen, stehen den Angreifern immer mehr Ressourcen zur Verfügung. DDoS-Angriffe aus der Cloud müssen daher als dauerhafte Bedrohung eingestuft werden.

Anteil der DDoS-Angriffe, bei denen Cloud-Instanzen zum Einsatz kamen



Anteil der DDoS-Attacken nach Cloud Service Provider

27 % aws	15 % Google Cloud	11 % Microsoft Azure	8 % Alibaba Cloud
4 % ORACLE DATA CLOUD	4 % DigitalOcean	2 % IBM Cloud	28 % Andere Cloud-Anbieter

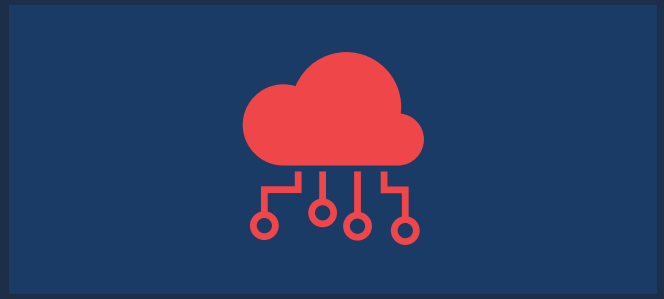
Ausblick auf die Gefahrenlage

Erpressungen mit DDoS-Attacken werden zur Normalität

Für die kommenden Monate ist mit einem weiteren Anstieg von Lösegelderpressungen, wie sie seit dem Sommer 2020 in immer neuen und kürzer auftretenden Wellen zu beobachten sind, zu rechnen. Da Unternehmen ihre Digitalisierung weiter vorantreiben, bieten sie immer mehr Angriffsfläche und werden ohne unzureichenden Schutz anfälliger für Downtimes und Betriebsunterbrechungen. Darüber hinaus werden die geringen Kosten und die einfache Ausführbarkeit von DDoS-Angriffen dafür sorgen, dass Erpressungen weiterhin im Aufwind sind.

Komplexität der Attacken erschwert ihre Abwehr

Die Angreifer verbessern ihre Methoden und beschränken sich immer seltener auf nur eine einzige Angriffstechnik. Vielmehr setzen sie verstärkt Methoden ein, die sowohl die Volumen- als auch die Netzwerk- und Applikationsebene attackieren – und dies gleichzeitig. Der Missbrauch weiterer Protokolle gilt dabei ebenfalls als sicher.
Die gemischten Angriffsformen stellen die Unternehmen vor neue Herausforderungen in der Abwehr. Schutzlösungen, die nur einzelne Angriffsarten abwehren, können diese nicht lösen. An ihre Stelle müssen Systeme mit mehrschichtiger Anomalie-Erkennung und vernetzten Sicherheitsmechanismen treten.



Die Cloud wird zu einer der wirksamsten DDoS-Waffen

DDoS-Attacken werden weiterhin in hohem Maße unter Einsatz kompromittierter Cloud-Server ausgeführt werden. Diese nutzen die Täter zusätzlich zu klassischen Botnetzen aus infizierten Privatrechnern oder Firmenservern sowie IoT-Geräten und verbreitern ihre Auswahl an Angriffswerkszeugen. Gleichzeitig profitieren sie von einer boomenden Infrastruktur. Die Gründe dafür liegen auf der Hand: In Bezug auf Anbindung, Cores und Attacken-Vektoren sind sie anderen Bots wie IoT-Geräten weit überlegen. Ihr Angriffsvolumen liegt bis zu 1.000-fach höher. DDoS-Angriffe und Cloud-Infrastrukturen werden zu einer gefährlichen Kombination.

Quellenangaben

(1) Berliner-Zeitung.de: Schul-Cloud in Brandenburg von Hackern angegriffen, 11.01.2021

(2) Independent.com: Melita services returning to normal after company faces cyber-attack, 13.01.202

(3) Telecompaper.com: Siminn reports DDoS attack hitting television service on 30 January, 03.02.2021

(4) Lfpress.com: ‚Bot' attack slowed London area COVID-19 vaccine booking site: top doc, 22.03.2021

(5) ORF.at: DDoS-Attacke: Österreichweite Ausfälle bei A1-Internet, 18.02.2021

(6) Weirditaly.com: Lower House website under attack, 09.03.2021

(7): Futurezone.at: Massive Cyberattacke legte Internet in Belgien weitgehend lahm, 06.05.2021

(8) Illinoisnewstoday.com: Irish Internet Service Provider Hit by Cyber Attack, 17.08.2021

(9) Infosecurity-magazine.com: AXA faces DDoS after ransomware attack, 18.05.2021

(10) FAZ.net: Sabotageangriff legt Onlinebanking bei Volksbanken lahm, 04.06.2021

(11) Securityaffairs.co: Major blackouts across Puerto Rico. Are the DDoS and the fire linked?, 14.06.2021

(12) Jewishpress.com: Mammoth Cyber Attack on Israel's Banking System Fails, 27.06.2021

(13) Forbes: ProtonMail Pays Crooks $6,000 In Bitcoin To Cease DDoS Bombardment, 05.11.2015

(14) T3n: Erpressergruppe zielt mit DDoS-Attacken auf DHL, Hermes und Ebay, 22.04.2021

(15) Thesslstore.com: Cyber Attacks Hit the City of Johannesburg and South African Banks, 29.04.2021

(16) n-tv.de: Hacker erpressen Lieferando, 20.03.2020

(17) Handelsblatt: Cyber-Angriffe legen Börsenhandel in Neuseeland dritten Tag in Folge lahm, 27.08.2020

Über den Report

Methodik

Der Link11 DDoS-Report 2020 basiert auf Daten aus der Überwachung des globalen Netzwerkes von Link11. Die abgewehrten Angriffe zielten auf Webseiten und Server, die durch Link11 vor DDoS-Attacken geschützt werden. Die Daten wurden vom 1. Januar bis zum 30. Juni 2021 erhoben. Neben Netzwerkanalysen und der Auswertung von DDoS-Attacken-Daten stützt sich der Link11 DDoS-Report auch auf Open-Source-Intelligence-Analysen (OSINT).

Über das LSOC

Ein Team aus erfahrenen DDoS-Schutzexperten bildet das Link11 Security Operation Center (LSOC). Im 24/7-Betrieb betreut es namhafte Unternehmen beim Schutz vor Cybercrime und DDoS-Attacken. Die Weiterentwicklung der Link11 Cloud Security Plattform und der permanente Ausbau der dafür benötigten Infrastruktur liegen ebenfalls im Zuständigkeitsbereich des LSOC. Die Ergebnisse seiner Arbeit und die Analysen der Angriffe veröffentlicht das LSOC regelmäßig in Reports sowie als Warnmeldungen und Analysen zu aktuellen DDoS-Sicherheitsvorfällen auf dem IT-Security-Blog von Link11 auf www.link11.com/de/blog.

Über Link11

Link11 ist der im Bereich Cyber-Resilienz führende europäische IT-Sicherheitsanbieter mit Hauptsitz in Deutschland und weltweiten Standorten in Europa, Nordamerika, Asien und dem Nahen Osten. Die cloudbasierten Security-Services sind vollständig automatisiert, reagieren in Echtzeit und wehren alle Angriffe, sowohl bekannte als auch neue Muster, garantiert in unter 10 Sekunden ab. Damit bietet Link11 laut einhelliger Analysten-Meinung (Gartner, Forrester) die schnellste Erkennung und Abwehr (TTM), die auf dem Markt verfügbar ist. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) weist Link11 als qualifizierten DDoS-Schutzanbieter für kritische Infrastrukturen aus.
Um Cyber-Resilienz zu gewährleisten, sorgen u.a. Web- und Infrastruktur-DDoS-Schutz, Bot-Management, Zero-Touch-WAF bis hin zu Secure-CDN-Services für eine ganzheitliche und plattformübergreifende Härtung der Netzwerke und kritischer Anwendungen von Unternehmen. Das 24/7 besetzte Link11 Security Operation Center, das nach dem Follow-the-Sun-Prinzip auf die Standorte in Deutschland und Kanada verteilt ist, stellt den reibungslosen Ablauf aller Systeme sicher und betreut den Ausbau des globalen MPLS-Netzwerks mit 43 PoPs und über 4 Tbps Kapazität. Garantierte Schutzbandbreiten bis zu 1Tbps bieten höchste Zuverlässigkeit. Die internationalen Kunden können sich so auf ihr Geschäft und digitales Wachstum konzentrieren. Seit der Gründung des Unternehmens im Jahr 2005 wurde Link11 mehrfach für seine innovativen Lösungen und sein Wachstum mit verschiedenen Preisen ausgezeichnet.

Redaktion

Link11 / Katrin Gräwe
k.graewe@link11.com

Bildnachweis

iStock 962404026 (Cover)
Unsplash / André François McKenzie (Seite 7)
Pixabay 3374479 (Seite 8)
Pixabay 4700815 (Seite 9)

Grafiken

Link11 GmbH