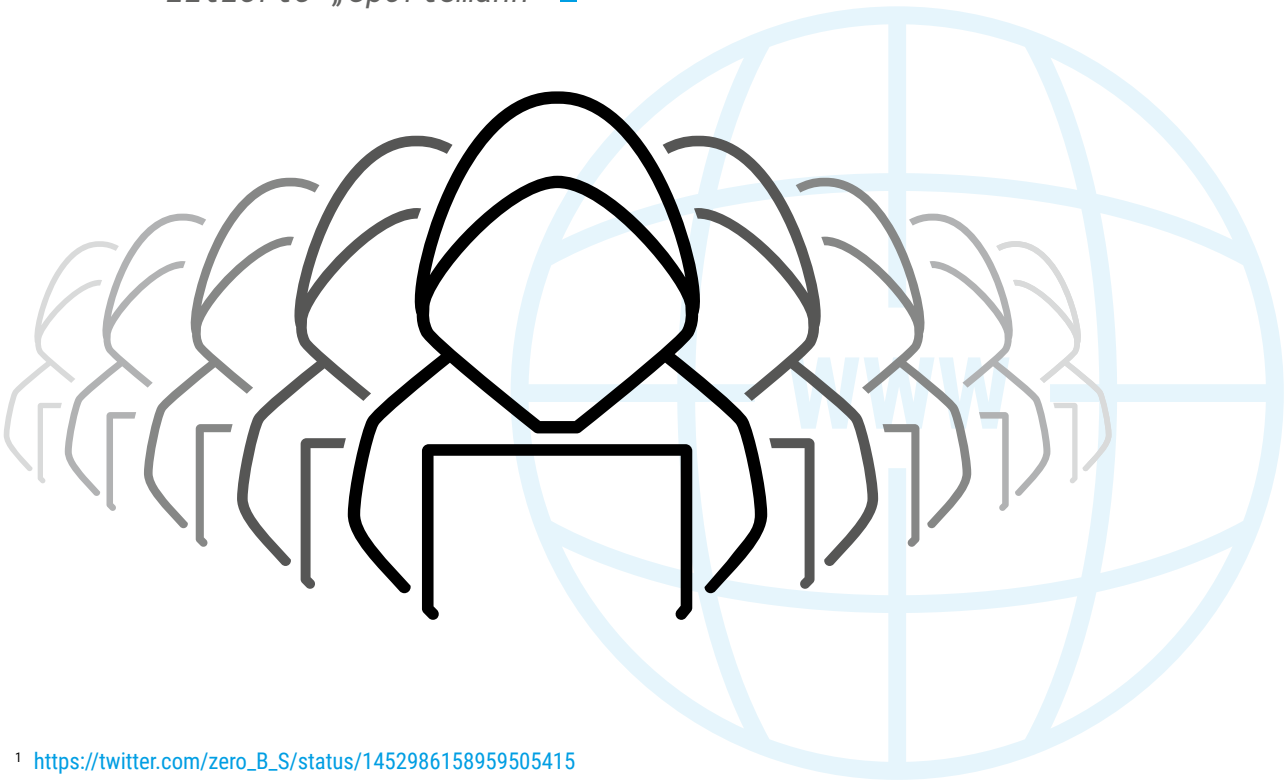
Summary 2021

State of DDoS

TL;DR: Angreifer werden immer fortschrittlicher, aber die erfahrenen Schutzanbieter wissen, wie man mit den Angriffen umgeht.

Die DDoS-Bedrohungslage hat sich in den letzten Jahren nicht wirklich verbessert – DDoS-basierte Erpressung erscheint immer noch lukrativ genug. Zusätzlich sehen wir für 2021 eine Renaissance von DDoS-Attacken[1] für viele Akteure, sei es Erpressung, Hacktivismus oder der viel-zitierte „Sportsmann“ ■



[1] https://twitter.com/zero_B_S/status/1452986158959505415

Aktuelle Trends – und was wir für die nahe Zukunft erwarten.

Seit 2020 ist eine DDoS-Ransomware-Gang mit wechselnden Namen sehr aktiv (von uns hier[2] nachverfolgt), die ungeschützte Unternehmen mit sehr gezielten Angriffen attackiert.

Markenzeichen dieser Bande:

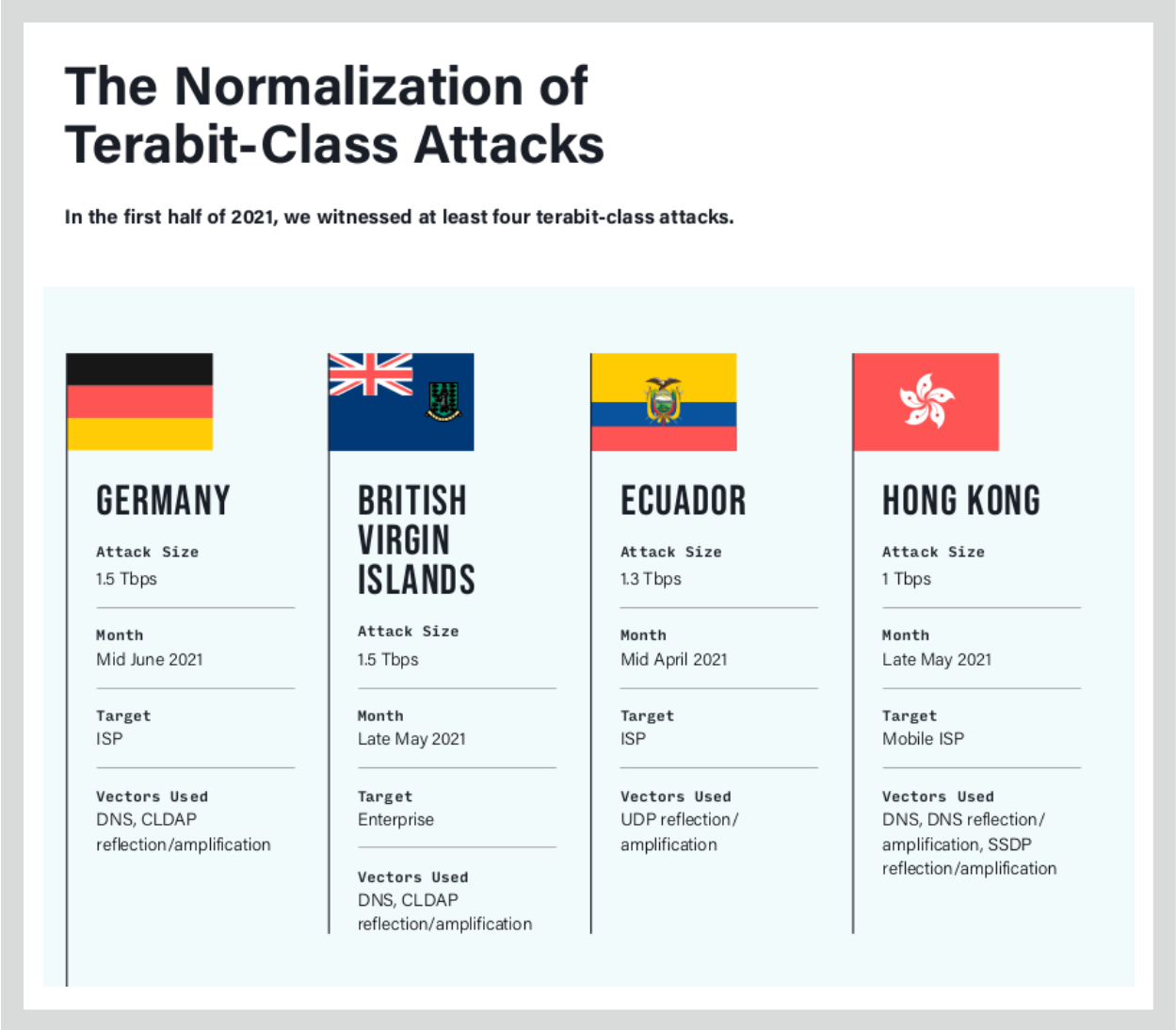
- Maßgeschneiderte und gezielte Angriffe nach Aufklärung mit hoher Durchschlagskraft;
- APT-Verspottung mit ständig neuen Namen (Fancy Bear, Armada Collective, Lazarus Group oder neuerdings Revil);
- Angriffe auf mehrere Ziele einer Branche (bisher: Banken, Reisebranche, ISP, Telcos, VOIP-Anbieter, Glücksspielbranche, E-Mail-Anbieter);
- Angriffe von globalem Ausmaß.

Weitere Trends

- DDoS-Kampagnen im Jahr 2021 sind gezielter, vektorübergreifend und hartnäckiger geworden (Neustar, Netscout);
- Ransom-DDoS-Kampagnen (RDDoS) haben deutlich zugenommen (ENISA, Cloudflare, Netscout);
- Cybercrime-as-a-Service (auch bekannt als Booter/Stresser-Services) fungiert als Verstärker für webbasierte und volumetrische DDoS-Angriffe technische Trends;
- TCP-basierte Angriffsvektoren rücken aufgrund neuer Forschungen[3] (Link zum Paper direkt[4]) in den Fokus, das erwartete Potenzial für volumetrische TCP-Angriffe ist riesig;
- DDoS verlagert sich in Richtung mobiler Netzwerke und IoT (ENISA) und unterstützt lokalisierten DDoS, bei dem ein Angreifer die Konnektivität eines bestimmten Gebiets stört und damit Dienste wie Online-Banking und alle Dienste mit einer großen Kundenbasis, die mobile Geräte/Verbindungen nutzen, bedroht;
- TCP-Amplification und Reflection werden in den kommenden Jahren zu einer großen Bedrohung werden, insbesondere bei Amplification-Raten > 1000. Wir erwarten, dass fortgeschrittene Angreifer diesen Vektor immer erfolgreicher einsetzen werden;
- Recon, Target-Analyse und Mitigation/Monitoring ist bei Ransom-DDoS und fortgeschrittenen Angreifern üblich;
- Botnet-Größe von 50.000 Bots und mehr ist die neue Norm[5] für IoT-Botnets;

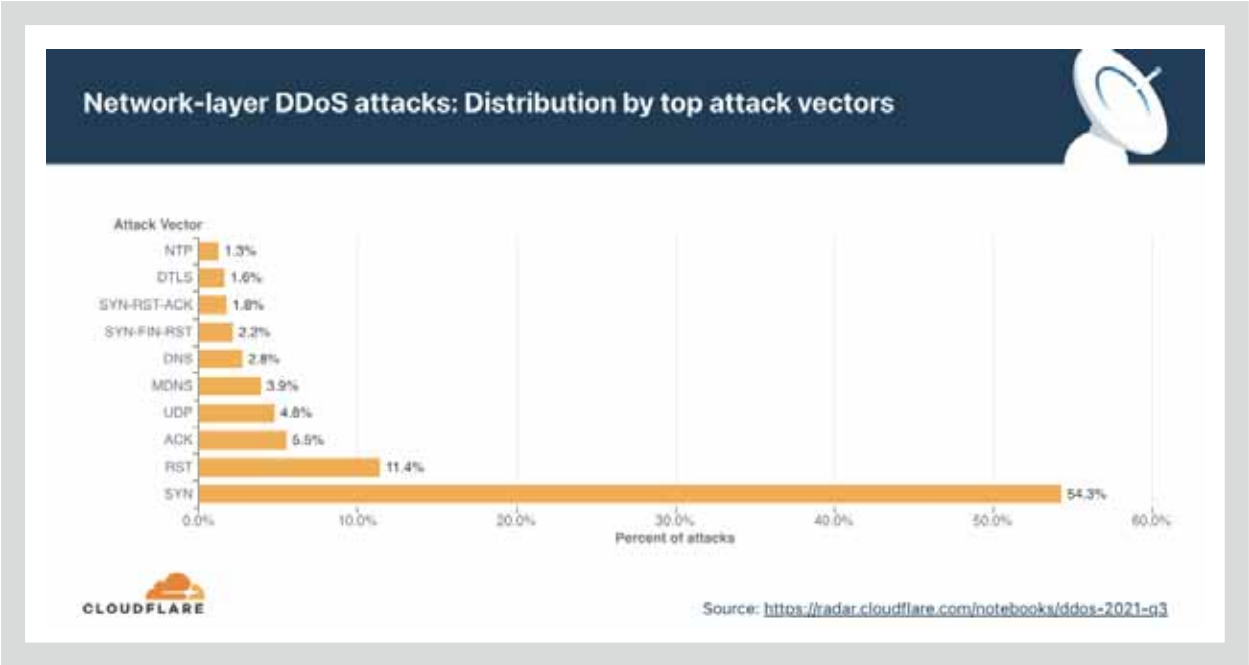
[1] https://twitter.com/zero_B_S/status/1452986158959505415
[2] https://zero.bs/sb-2030-global-ddos-campaign-targeting-isps-correlates-with-isc-bind-vuln-cve-2020-8620.html
[3] https://therecord.media/firewalls-and-middleboxes-can-be-weaponized-for-gigantic-ddos-attacks/
[4] https://www.usenix.org/system/files/sec21fall-bock.pdf
[5] https://www.bleepingcomputer.com/news/security/new-m-ris-botnet-breaks-ddos-record-with-218-million-rps-attack/

- 1TB/s volumetrische Angriffe definieren die neue Obergrenze und wurden von vielen Anbietern (Netscout, Cloudlfare, Google, Neustar) beobachtet;
- Die Straßenpreise für DDoS-Attacken[6] sind in den letzten 2 Jahren stabil geblieben;
- DTLS und GRE sind neue Vektoren.

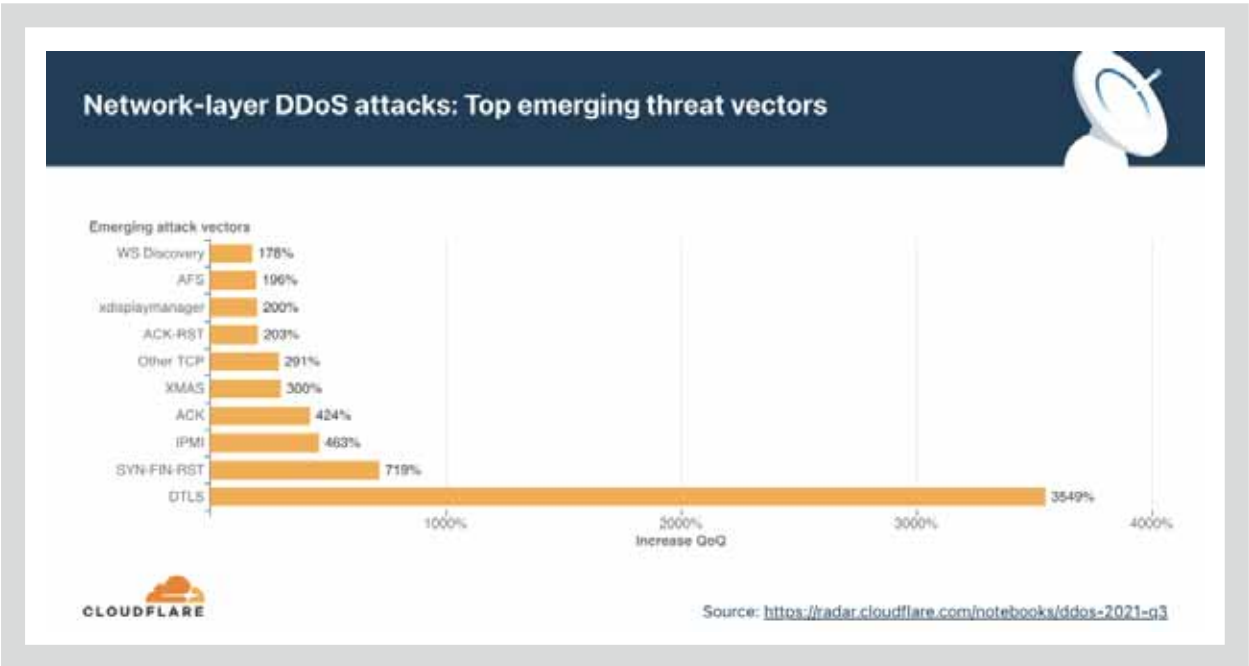


[tb_is_norm.png] ↗ src: Netscout Threat Report 2021

[6] https://zero.bs/street-prices-for-ddos-attacks.html



[ddos-vectors.png] ↗ src: Cloudflare: DDoS Attack-Vectors for Q3 2021



[ddos-vectors.png] ↗ src: Cloudflare: DDoS Attack-Trends for Q3 2021

Technische Reports und Analysen

- Der aktuelle ENISA-REPORT[7] behandelt DDoS ausführlich in Abschnitt 8. BEDROHUNGEN DER VERFÜGBARKEIT UND INTEGRITÄT. Organisationen in Europa sollten sich darüber im Klaren sein, dass "... das Bedrohungspotenzial von DDoS-Angriffen höher ist als die derzeitigen Auswirkungen in der EU ...", was durchaus zu einem Anstieg der Angriffe im EU-Raum führen kann.
- NETSCOUTs 2021 Threat Intelligence Report[8] bietet eine sehr detaillierte Entwicklung, Analyse und Übersicht über die DDoS-Bedrohungslage im Jahr 2021 im Vergleich zu den Vorjahren. Eine der wichtigsten Erkenntnisse (neben dem, was bereits oben erwähnt wurde): TB-Angriffe beginnen, "die Norm" zu werden
- Cloudflares Bericht über einen DDoS-Angriff mit 17,2 Mio. RPS[9] bietet einen interessanten Einblick in ein großes IoT-Botnet.
- DDoS Attack Trends for Q3 2021[10] von Cloudflare gibt einen hervorragenden Überblick über die globalen Aktivitäten und Trends.

[1] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
[1] https://www.netscout.com/press-releases/cybercriminal-attacks-accelerate-global-cybersecurity
[1] https://blog.cloudflare.com/cloudflare-thwarts-17-2m-rps-ddos-attack-the-largest-ever-reported/
[1] https://blog.cloudflare.com/ddos-attack-trends-for-2021-q3/

Über zeroBS

Die zeroBS GmbH aus Kiel bietet seit 2017 realitätsnahe DDoS-Stresstests über eine eigene cloudbasierte Plattform1 an und hat sich im Laufe der Jahre als Marktführer im DACH-Raum etabliert. Zu den Kunden gehören Unternehmen aus dem Banken- und Finanzsektor, Industrie, Ecommerce und Telekommunikation. Darüber hinaus bestehen Kooperationen mit mehreren Security – Dienstleistern, die das Spezialwissen im Bereich DDoS-Assessment / DDoS-Testing von zeroBS für ihre Kunden einkaufen.

Bei insgesamt über 200 Stresstests hat zeroBS nicht nur alle Anbieter aus der BSI-Publikation „Qualifizierte DDoS-Mitigation Dienstleister“ 2 getestet, sondern Erfahrungen zu allen namhaften Herstellern und Schutzanbietern gesammelt, egal ob Appliance, Scrubbingcenter, Hybridlösung, Reserveproxy oder Schutzlos. Dabei deckt die Expertise von zeroBS sowohl Volumenangriffe (Layer3, 4) als auch Angriffe auf Applikationen (Layer 7) ab.

Mit unserer Stresstest-Plattform können echte Botnetz-Angriffe mit bis zu 100.000 Bots in verschiedenen Angreiferleveln (Skriptkiddy, Botnet, Advanced Attacker, State-Sponsored) simuliert werden, gängig sind Konstellationen und Prüfungen mit 1000, 5000 und 10.000 Bots.

zeroBS führt als Unternehmen mit Sitz in Kiel, Schleswig Holstein, das „IT Security Made in Germany“-Logo.