enisa

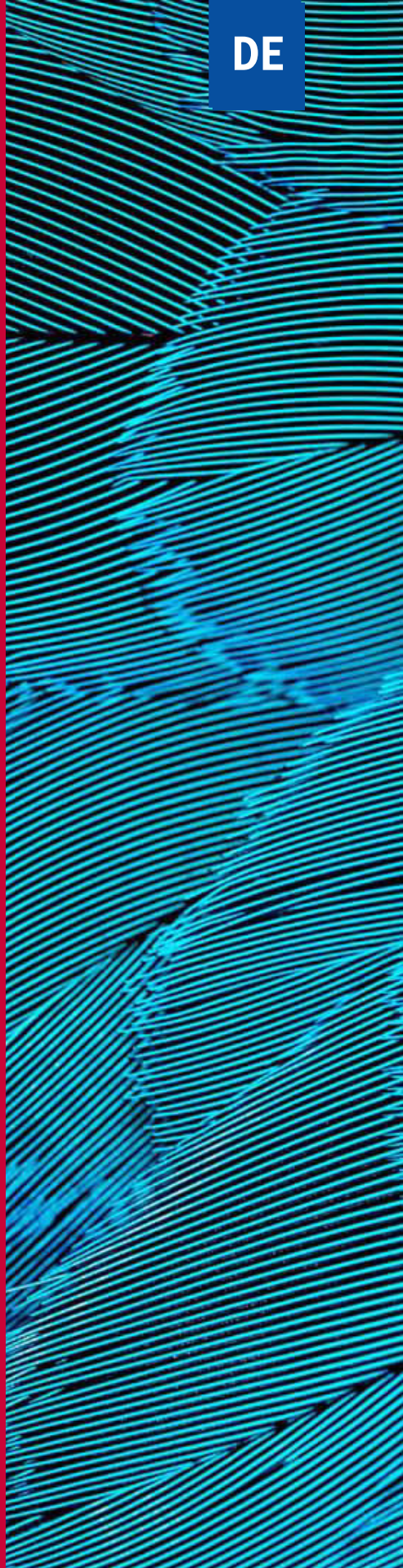
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

DE

Von Januar 2019 bis April 2020

Distributed Denial-of-Service

ENISA Threat Landscape



Überblick

Distributed Denial of Service (DDoS)-Angriffe treten bekanntermaßen auf, wenn Benutzer eines Systems oder Dienstes nicht auf die relevanten Informationen, Dienste oder anderen Ressourcen zugreifen können. Diese Phase kann erreicht werden, wenn der Dienst erschöpft oder die Komponente der Netzwerkinfrastruktur überlastet ist.[1] Böswillige Akteure erhöhen die Angriffe, indem sie auf mehr Sektoren mit unterschiedlichen Motiven abzielen. Während Verteidigungsmechanismen und -strategien robuster werden, verbessern böswillige Akteure auch ihre technischen Fähigkeiten. Berichte[3,4,5] deuten darauf hin, dass die Verwendung von reflektierten und verstärkten Angriffstechniken, die andere Vektoren als die allgemein bekannten (UDP-Verstärkung usw.) ermöglichen, zugenommen hat[6] Böswillige Akteure verbessern auch ihre kommerzielle Taktik, indem sie damit beginnen, ihre Dienste auf der Website zu bewerben. Früher wurden DDoS-Dienste in Foren des Dark Web beworben, jetzt nutzen sie jedoch gängige Social-Media-Kanäle wie YouTube und Redit, um für ihre Dienste zu werben.[2]

Im Jahr 2019 wurden neue Einträge in die Top-10-Liste der Quellenländer aufgenommen, die DDoS-Verkehr erzeugen (Hongkong, Südafrika usw.).[7] In diesem Jahr nahm auch die DDoS-Aktivität durch Botnetze zu. IoT-Geräte sind eine Brutstätte für DDoS-Botnetze, und China (24 %), Brasilien (9 %) und der Iran (6 %) wurden als die Länder angesehen, die am stärksten mit Botnetz-Agenten infiziert sind.[3] Ein Sicherheitsforscher prognostizierte, dass die Implementierung und die Verteilung von 5G-Netzwerken die Anzahl der verbundenen Geräte exponentiell erhöhen wird, daher die Erweiterung von Botnetz-Netzwerken.[3]

Obwohl DoS-Angriffe für Cybersicherheits- und Netzwerkverteidiger nichts Neues sind, nimmt ihr Grad an Raffinesse zu, und es wird beobachtet, dass böswillige Akteure aktiv mehr Auskundschaftungsaktivitäten durchführen als zuvor.[3,8]

Erkenntnisse

241 % Anstieg der Anzahl der Angriffe im dritten Quartal 2019 im Vergleich zum gleichen Zeitraum von 2018[3]

79,7 % aller DDoS-Angriffe waren SYN-Floods[7]

86 % der abgeschwächten Angriffe im dritten Quartal 2019 verwendeten mehr als zwei Vektoren[9]

84 % der DDoS-Angriffe dauerten weniger als 10 Minuten[10,11]

509 Stunden dauerte der längste DDoS-Angriff im zweiten Quartal 2019[3]

Kill chain

Denial of service - Serviceverweigerung

Ausspähung	Wappnung	Lieferung	Betreibung

Schritt des Angriffs-Workflows

Umfang des Zwecks

Installation

Command & Control

Zielführende Maßnahmen

Das Cyber Kill Chain® Framework wurde von Lockheed Martin entwickelt und basiert auf einem militärischen Konzept, das mit der Struktur eines Angriffs zusammenhängt. Um einen bestimmten Angriffsvektor zu untersuchen, verwenden Sie dieses Kill-Chain-Diagramm, um jeden Schritt des Prozesses sowie die vom Angreifer verwendeten Hilfsmittel, Techniken und Verfahren festzuhalten.

WEITERE INFORMATIONEN

Vorfälle

Die Top 5 DDoS-Angriffe

500-580 MILLIONEN PAKETE PRO SEKUNDE SYN FLOODS. Unter all den Techniken, die von böswilligen Akteuren verwendet werden, wird SYN Flood aufgrund seiner Eigenschaften, der anvisierten Infrastruktur und der Tatsache, dass mehr Hardware für die Verarbeitung eines hohen Paketvolumens erforderlich ist, immer noch als schwierig zu entschärfen angesehen. Im Januar 2019 beobachtete ein Sicherheitsforscher eine Aufzeichnung der SYN-Flood-Aktivität, die 500 Millionen Pakete pro Sekunde (mpps) an einen seiner Kunden verteilte, und anschließend stieg das Volumen im April 2019 auf 580 mpps.[12]

WS-DISCOVERY. Web Services Dynamic Discovery[13] (WS-Discovery) ist ein Multicast-Erkennungsprotokoll. Es wurde beobachtet, dass es hauptsächlich von IoT-Geräten verwendet wird, um jeden Knoten in lokalen Netzwerken (LANs) automatisch zu erkennen, aber wie andere Protokolle kann es nicht nur für den beabsichtigten Zweck verwendet werden, insbesondere im IoT-Bereich[5]. Böswillige Akteure haben festgestellt, dass es eine gute Brutstätte für das Verstärken von Angriffen ist. Ein Sicherheitsforscher berichtete[3] über einen Verstärkungsfaktor von 95x, während ein anderer Forscher einen Anstieg von 15.000 % gegenüber der ursprünglichen Bytegröße meldete.[14]

REFLEKTIERTE UND VERSTÄRKTE ANGRIFFE. Es ist allgemein bekannt, dass diese Arten von Angriffen eine kleine Anforderung zur Bereitstellung einer größeren Payload enthalten. Zusammenfassend lässt sich sagen, dass der böswillige Akteur die IP-Adresse des Absenders (des Opfers) fälscht und anschließend der Host des Empfängers alle zugehörigen Antworten an das Opfer sendet.[9] Diese Methode ist hauptsächlich für UDP-basierte Protokolle wirksam, da sie verbindungslos sind und einen Verstärkungsfaktor aufweisen (d. h. CLDAP hat einen Verstärkungsfaktor von x50-x70). Das TCP-Protokoll ist jedoch nicht anfällig für diese Art von Angriff.[15]

Ein gutes Beispiel für solche Versuche sind SYN-ACK-reflektierte und verstärkte Flooding-Angriffe. Diese Art von Flood muss nicht unbedingt eine hohe Bandbreite aufweisen, um Auswirkungen zu haben. Im Gegensatz dazu kann ein hohes Paket pro Sekunde den Angriff unter dem Radar halten und seine Effektivität erhöhen.[3]

BIT-AND-PIECE / CARPET BOMBING DDoS. Es ist bekannt, dass diese Art von DRDoS-Angriff (Distributed and Reflective Denial of Service) hauptsächlich auf Telekommunikations- und Dienstanbieterindustrien abzielt.[17] In einem Fall[18] dieses Angriffs wurde eine zufällige Auswahl von IP-Adressen eines Internetdienstanbieters ausgewählt, um den Datenverkehr an die Edge-Router des Anbieters zu reflektieren. Somit konnte das Opfer das DDoS nicht identifizieren, bis deren Dienst von ihrem eigenen ausgewählten IP-Bereich überfordert war.[19]

MULTI-VEKTOR DDOS-ANGRIFFE. Böswillige Akteure führen häufig mehrere Vektoren von DoS-Angriffen aus, um ihrem Versuch Komplexität und Vielfalt zu verleihen. Dies bedeutet, dass durch die bloße Automatisierung verschiedener Angriffsarten der Anwendungsschicht (HTTP-Flood, DNS-Flood usw.) und der Netzwerkschicht (UDP/TCP-Reflexion/-Verstärkung usw.) versucht wird, die Auswirkungen zu maximieren, indem sowohl die Bandbreite als auch die Ressourcen oder Dienstleistungen in der Zielumgebung gesättigt werden.[16]

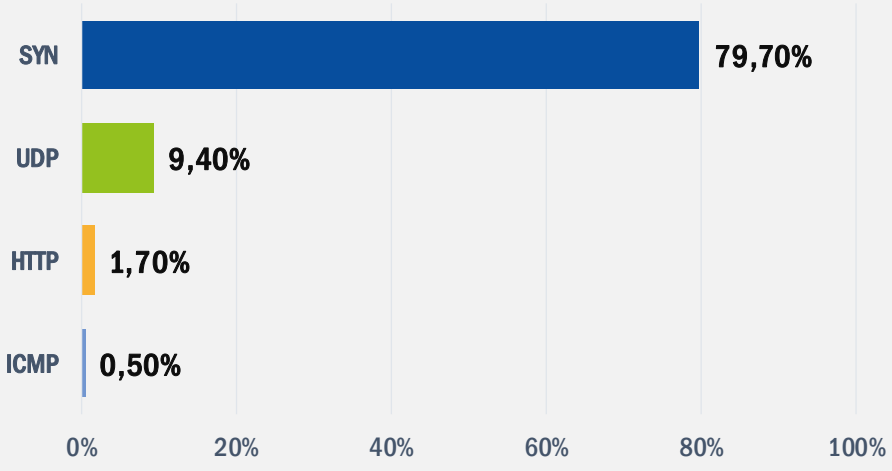


Abbildung 1: Verteilung der DDoS-Angriffe nach Typ. Quelle: Kapersky[16]

Angriffsvektoren

_ Wie

Ähnlich wie in den Vorjahren war 2019 keine Ausnahme in Bezug auf UDP-Floods. Laut einem Sicherheitsforscher war die UDP-Flood der beliebteste Angriffsvektor, und das Team ist der Ansicht, dass dies möglicherweise mit der dominierenden Übernahme dieses Protokolls in Hochrisikobranchen wie dem Glücksspiel zusammenhängt. SYN-Flood, DNS-Reaktion und TCP-basierte Angriffe folgten UDP-Floods in der Liste der Top-Angriffsvektoren.

In diesem Zeitraum wurden auch Multi-Vektor-Angriffe beobachtet. Ein Sicherheitsforscher ist jedoch der Ansicht, dass einige der Multi-Vektor-Angriffe ein unbeabsichtigtes Nebenprodukt eines DoS-Versuchs sind.[11]

In einem Cybersicherheitsbericht[17] wurde vorgeschlagen, dass DNS-Amplifikationsangriffe von seinem Team als wichtigster DDoS-Angriffsvektor beobachtet wurden, gefolgt von HTTP-Flood- und TCP-SYN-Angriffen. Die Beobachtungen der Angriffsvektoren im dritten Quartal 2019 waren ähnlich wie bei SYN-Floods, dem obersten Vektor, gefolgt von UDP-, TCP- und HTTP-Angriffen.

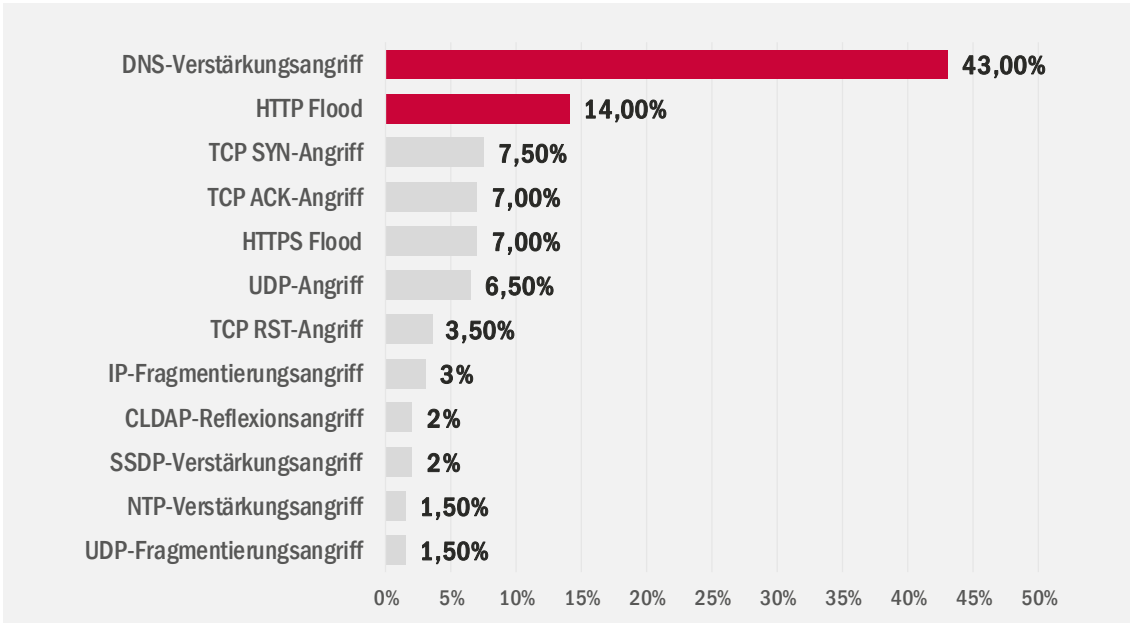


Abbildung 2: Verteilung der DDoS-Angriffe nach Vektoren. Quelle: NexusGuard[17]

Dauer des Angriffs

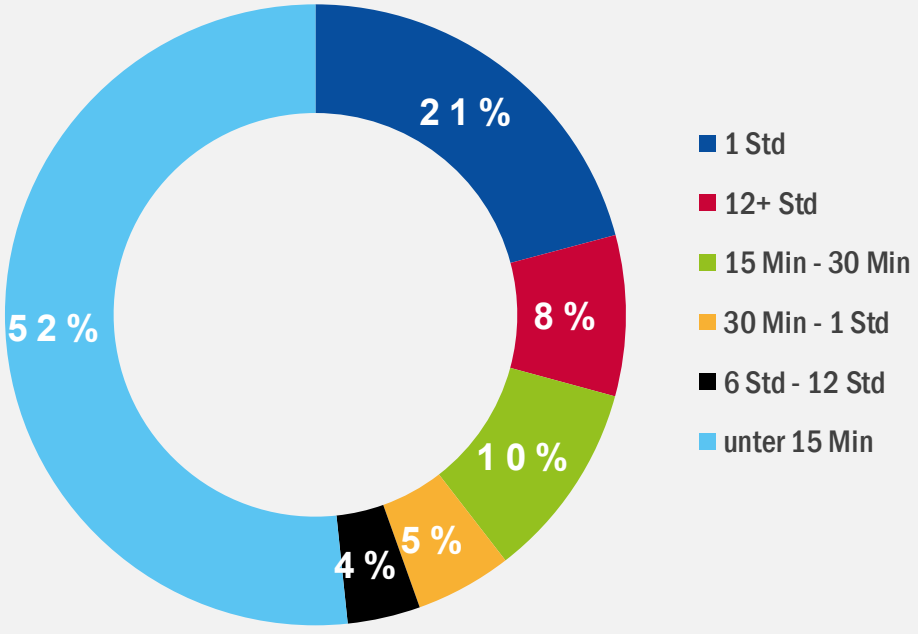


Abbildung 3 - Quelle: Imperva[11]

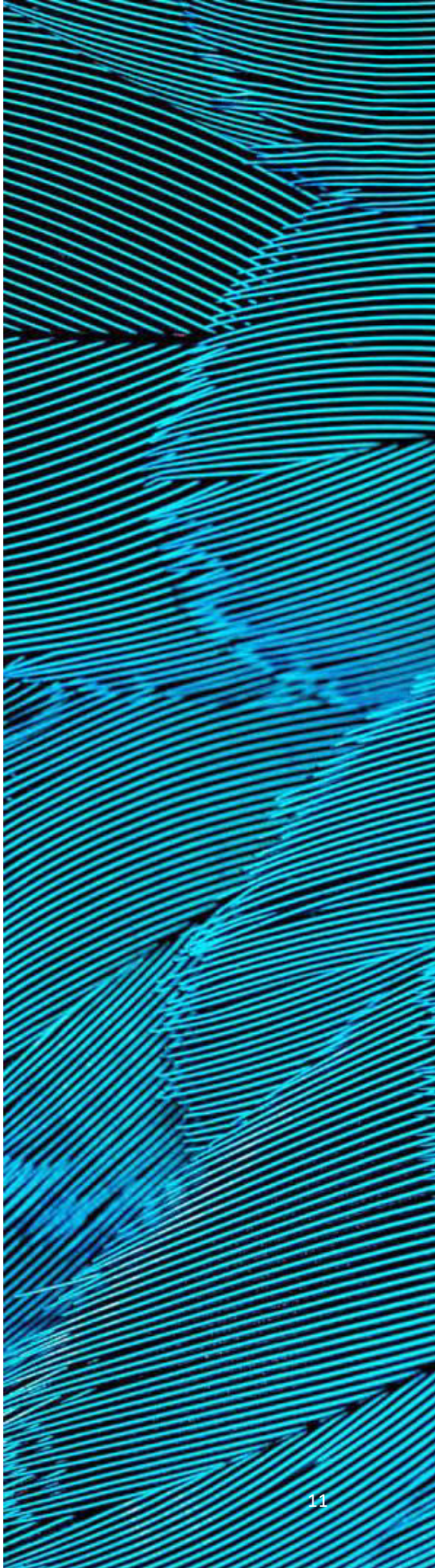
Minderung

Vorgeschlagene Maßnahmen

- Verstehen von Diensten und kritischen Ressourcen und Priorisieren der Verteidigung, wo diese überlastet werden können. Sicherstellen, dass für solche Szenarien ein Reaktionsplan vorhanden ist.[20]
- Abhängig von den Anforderungen unter Berücksichtigung des DDoS-Schutzdienstes oder eines DDoS-Managed-Service-Providers. Verwendung von Methoden wie Überwachung zur schnellen Identifizierung von Infektionen.[1]
- Ähnlich wie oben beschrieben kann das Veröffentlichen von Diensten über Content Delivery-Netzwerke ein wirksames Mittel sein, um volumetrische Versuche zu absorbieren (erfordert andere Techniken für komplexere Angriffe).[21]
- Internetdienst- und Cloud-Anbieter spielen eine wichtige Rolle bei der Abwehr von DDoS-Angriffen. Ein klarer Kommunikationsplan und ein klarer Kommunikationskanal sind der Schlüssel für eine erfolgreiche Reaktion auf einen Denial-of-Service-Angriff.
- Entwickeln einer proaktiven und starken Verteidigungshaltung, bevor ein kritischer Fehler auftritt, an dem das zugehörige Team und die Anbieter beteiligt sind, um Steuerelemente basierend auf bestimmten Geschäftsanforderungen zu konfigurieren und zu optimieren.[22] Erleichterung von Cache-Servern oder Löschen unangemessener Ab- oder Anfragen auf Anwendungsebene an der Quelle und Implementierung von BCP[23] für Service-Anbieter sind gute Beispiele für proaktive Maßnahmen.
- Stellen Sie sicher, dass Sie Ihre Verteidigungstechniken, Technologien und Anbieter testen und neu bewerten.
- Erstellen Sie ein Risikoregister, indem Sie Ihre Umgebung von innen nach außen analysieren. Angefangen von Ihren kritischen Ressourcen im Inneren bis hin zu Ihrem Internet-Fußabdruck und -Präsenz.[24]

„Obwohl DDoS-Angriffe für Cybersicherheits- und Netzwerkverteidiger nichts Neues sind, nimmt ihr Grad an Raffinesse zu, und es wird beobachtet, dass böswillige Akteure aktiv mehr Ausspähungsaktivitäten durchführen als zuvor.“

In ETL 2020



Literaturangaben

1. "Understanding Denial-of-Service Attacks" 20. November, 2019. CISA. https://www.us-cert.gov/ncas/tips/ST04-015

2. Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. "DDoS attacks in Q1 2019" 21. Mai, 2019. Kaspersky. https://securelist.com/ddos-report-q1-2019/90792/

3. "Q4 2019 - The State of DDoS Weapons Report." 2019. A10 Networks. https://www.a10networks.com/marketing-comms/reports/state-ddos-weapons/

4. Chad Seaman. "Anatomy of a SYN-ACK Attack." 2. Juli, 2019. Akamai. https://blogs.akamai.com/sitr/2019/07/anatomy-of-a-syn-ack-attack.html

5. Brandon Vigliarolo. "A new type of DDoS attack can amplify attack strength by more than 15,300%." 18. September, 2019. TechRepublic. https://www.techrepublic.com/article/a-new-type-of-ddos-attack-can-amplify-attack-strength-by-more-than-15300/

6. Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. "DDoS attacks in Q4 2018" 7. Februar, 2019. Kaspersky. https://securelist.com/ddos-attacks-in-q4-2018/89565/

7. Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. "DDoS attacks in Q3 2019" 11. November, 2019. Kaspersky. https://securelist.com/ddos-report-q3-2019/94958/

8. "2019 Website Threat Research Report." 2019. sucuri

9. "DDoS attacks up 241% in Q3 2019 compared to same period last year." 19. November, 2019. Neustar. https://www.home.neustar/about-us/news-room/press-releases/2019/ddos-attacks-up-241--in-q3-2019-compared-to-same-period-last-year#

10. "2019 Half-Year DDoS Trends Report." 2019. Corero Security. https://www.corero.com/blog/infographic-2019-mid-year-ddos-trends-report/

11. Nadav Avital, Avishay Zawoznik, Johnathan Azaria, Kim Lambert. "2019 Global DDoS Threat Landscape Report." 2019. Imperva. https://www.imperva.com/blog/2019-global-ddos-threat-landscape-report/

12. Tomer Shani. "Updated: This DDoS Attack Unleashed the Most Packets Per Second Ever. Here's Why That's Important." 30. April, 2019. Imperva. https://www.imperva.com/blog/this-ddos-attack-unleashed-the-most-packets-per-second-ever-heres-why-thats-important/

13. "Web Services Dynamic Discovery (WS-Discovery) Version 1.1" 1. Juli, 2009. OASIS. http://docs.oasis-open.org/ws-dd/discovery/1.1/wsdd-discovery-1.1-spec.html

14. Jonathan Respeto. "New DDoS Vector Observed in the Wild: WSD attacks hitting 35/Gbps." 18. September, 2019. Akamai. https://blogs.akamai.com/sitr/2019/09/new-ddos-vector-observed-in-the-wild-wsd-attacks-hitting-35gbps.html

15. "Threat Alert: TCP Amplification Attacks." 9. November, 2019. Radware. https://blog.radware.com/security/2019/11/threat-alert-tcp-reflection-attacks/

16. "Kaspersky report finds over half of Q3 DDoS attacks occurred in September." 11. November, 2019. Kaspersky. https://usa.kaspersky.com/about/press-releases/2019_kaspersky-report-finds-over-half-of-q3-ddos-attacks-occurred-in-september

17. "DDoS Threat Report 2019 Q1." 2019. NexusGuard. https://blog.nexusguard.com/threat-report/ddos-threat-report-2019-q1

18. "International traffic – DDoS." 22. September, 2019. Cool Ideas. https://coolzone.cisp.co.za/announcements.php?announcement=2038-international-traffic-ddos-cool-ideas

19. Catalin Cimpanu. "Carpet-bombing' DDoS attack takes down South African ISP for an entire day." 24. September, 2019. ZDNet. https://www.zdnet.com/article/carpet-bombing-ddos-attack-takes-down-south-african-isp-for-an-entire-day/

20. "Guidance following recent DoS attacks in the run up to the 2019 General Election." 13. November, 2019. NCSC. https://www.ncsc.gov.uk/guidance/guidance-following-recent-dos-attacks-2019-general-election

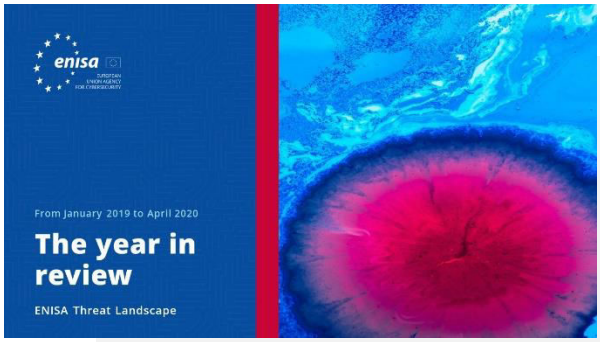
21. V. Revuelto, S. Meintanis, K. Socha. "DDoS Overview and Response Guide." 10. März, 2017. CERT-EU. https://cert.europa.eu/static/WhitePapers/CERT-EU_Security_Whitepaper_DDoS_17-003.pdf

22. "State of the Internet/Security DDoS and Application Attacks, Volume 5, Issue 1." 2019. Akamai. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-ddos-and-application-attacks-2019.pdf

23. P. Fergusson, D. Senie. "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing." Mai 2000. IETF Tools. https://tools.ietf.org/html/bcp38

24. Pierluigi Paganini. "Cyber Defense Magazine Sept Edition 2019." 4. September, 2019. SecurityAffairs. https://securityaffairs.co/wordpress/90795/breaking-news/cyber-defense-magazine-september-2019.html

Themenbezogen



ENISA Threat Landscape Bericht **Das Berichtsjahr**

Eine Zusammenfassung der Cybersicherheitstrends für den Zeitraum zwischen Januar 2019 und April 2020.

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht **Liste der 15 größten Bedrohungen**

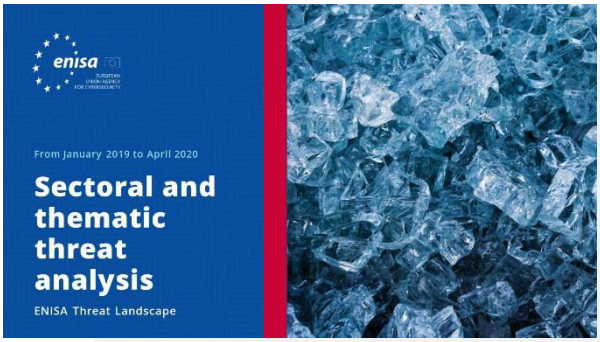
ENISAs-Liste der 15 größten Bedrohungen im Zeitraum zwischen Januar 2019 und April 2020.

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht **Forschungsthemen**

Empfehlungen zu Forschungsthemen aus verschiedenen Quadranten der Cybersicherheit und Cyber Threat Intelligence.

LESEN SIE DEN BERICHT



ENISA Threat Landscape-Bericht
Sektorale und thematische Bedrohungsanalyse

Kontextualisierte Bedrohungsanalyse zwischen Januar 2019 und April 2020.

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht
Aufkommende Trends

Die bedeutendsten Cybersicherheitstrends, die zwischen Januar 2019 und April 2020 beobachtet wurden.

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht
Übersicht über Cyber Threat Intelligence

Der aktuelle Stand der Cyber Threat Intelligence in der EU.

LESEN SIE DEN BERICHT

Über

_ Die Agentur

Die Agentur der Europäischen Union für Cybersicherheit, ENISA, hat die Aufgabe, zu einer hohen Cybersicherheit innerhalb der Union beizutragen. Die Agentur der Europäischen Union für Cybersicherheit wurde 2004 gegründet und durch das EU-Gesetz zur Cybersicherheit gestärkt. Sie trägt zur Unionspolitik im Bereich der Cybersicherheit bei, erhöht die Vertrauenswürdigkeit von ICT-Produkten, -Diensten und -Prozessen durch Programme für die Cybersicherheitszertifizierung, sie kooperiert mit den Mitgliedstaaten und Organen der EU und unterstützt Europa dabei, sich den künftigen Herausforderungen im Bereich der Cybersicherheit zu stellen. Durch Wissensaustausch, Aufbau von Fähigkeiten und Sensibilisierung in Bezug auf Cybersicherheit arbeitet die Agentur gemeinsam mit ihren wichtigsten Interessenträgern darauf hin, das Vertrauen in die vernetzte Wirtschaft zu stärken, die Infrastruktur der Union abwehrfähiger zu machen und schließlich ein sicheres digitales Umfeld für die Gesellschaft und die Bürger Europas zu gewährleisten. Weitere Information über die ENISA und ihre Arbeit finden Sie unter www.enisa.europa.eu.

Mitwirkende

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) und *alle Mitglieder der ENISA CTI Interessenvertreter:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) und Thomas Hemker.

Herausgeber

Marco Barros Lourenço (ENISA) und Louis Marinos (ENISA).

Kontaktangaben

Für Fragen über dieses Dokument, verwenden Sie bitte enisa.threat.information@enisa.europa.eu.

Für Medienanfragen zu dieser Stellungnahme verwenden Sie bitte die folgenden Kontaktangaben: press@enisa.europa.eu.

Wir würden gerne Ihr Feedback zu diesem Bericht erhalten!
Bitte nehmen Sie sich einen Moment Zeit, um den Fragebogen auszufüllen. Um das Formular zu öffnen, können Sie hier klicken.

Impressum/Rechtshinweise

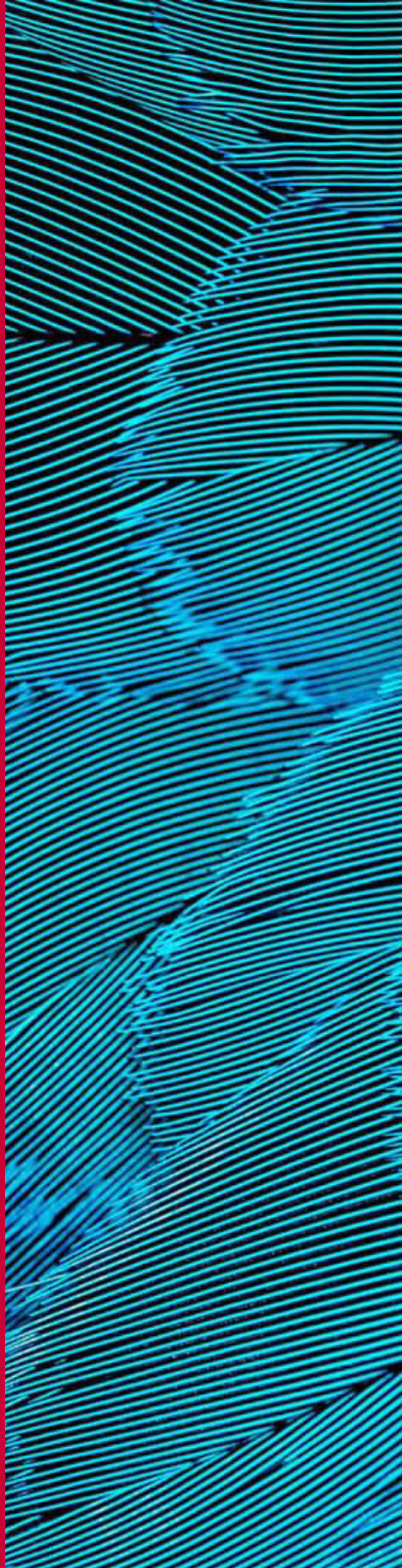
Sofern nichts anderes angegeben ist, gibt diese Veröffentlichung die Ansichten und Auslegungen der ENISA wieder. Diese Veröffentlichung ist nicht als eine Maßnahme der ENISA oder ihrer Gremien auszulegen, sofern sie nicht gemäß der Verordnung (EU) Nr. 526/2013 angenommen wurde. Diese Veröffentlichung entspricht nicht unbedingt dem neuesten Stand und kann in angemessenen Abständen aktualisiert werden.

Quellen von Dritten werden zitiert, sofern erforderlich. Die ENISA haftet nicht für den Inhalt der externen Quellen, einschließlich externer Websites, auf die in dieser Veröffentlichung verwiesen wird.

Die vorliegende Veröffentlichung ist nur für Informationszwecke gedacht. Sie muss kostenlos zugänglich sein. Weder die ENISA noch in deren Namen oder Auftrag tätige Personen können für die Nutzung der in dieser Veröffentlichung enthaltenen Informationen haftbar gemacht werden.

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Griechenland
Tel.: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu



enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu