



From January 2019 to April 2020

# Distributed denial of service

ENISA Threat Landscape

# Overview

Distributed Denial of Service (DDoS) attacks are known to occur when users of a system or service are not able to access the relevant information, services or other resources. This stage can be accomplished by exhausting the service or overloading the component of the network infrastructure.<sup>1</sup> Malicious actors increased the number of attacks by targeting more sectors with different motives. While defence mechanisms and strategies are becoming more robust, malicious actors are also advancing their technical skills. Reports<sup>3,4,5</sup> suggest that the usage of reflected and amplified attack techniques facilitating new vectors other than the commonly known ones (UDP amplification etc.) has increased.<sup>6</sup> Malicious actors are also improving their commercial tactics by starting to advertise their services on the web. Historically, DDoS services were advertised in the dark web forums, but now they use common social media channels such as YouTube and Redit to promote their services.<sup>2</sup>

In 2019, we saw new entries in the top 10 list of source countries generating DDoS traffic (Hong Kong, South Africa, etc.).<sup>2</sup> It was also the year that saw an increase in DDoS activity by botnets. IoT devices are a 'hotbed' for DDoS botnets, and China (24%), Brazil (9%) and Iran (6%) were considered as the countries most infected with botnet agents.<sup>3</sup> A security researcher predicted that, the implementation and distribution of 5G networks will exponentially increase the number of connected devices, hence the expansion of botnet networks.<sup>3</sup>

Although DoS attacks are not new to cybersecurity and network defenders, their level of sophistication is increasing, and malicious actors are observed to be actively running more reconnaissance activities than before.<sup>3,8</sup>





## **Findings**

**241%** increase in total number of attacks during Q3 2019 compared with the same period of 2018<sup>3</sup>

**79,7%** of all DDoS attacks were SYN-Floods<sup>7</sup>

**86%** of the mitigated attacks during Q3 2019 were using more than two vectors<sup>2</sup>

**84%** of the DDoS attacks lasted less than 10 minutes<sup>10,11</sup>

**509** hours was the duration of the longest DDoS attack in Q2 2019<sup>3</sup>



# Kill chain



Denial of service

Reconnaissance

Weaponisation

Delivery

Exploitation

 *Step of Attack Workflow*  
 *Width of Purpose*



The Cyber Kill Chain® framework was developed by Lockheed Martin, adapted from a military concept related with the structure of an attack. To study a particular attack vector, use this kill-chain diagram to map each step of the process and reference the tools, techniques and procedures used by the attacker.

[MORE INFORMATION](#)

## The top five DDoS attacks

**500-580 MILLION PACKETS PER SECOND SYN FLOODS.** Among all the techniques used by malicious actors, SYN Flood is still considered to be challenging to mitigate based on its characteristics, the infrastructure targeted and the fact that they require more hardware to handle a high volume of packets. In January 2019, a security researcher observed a record of SYN flood activity distributing 500 million packets per second (mpps) targeting one of its clients and, subsequently, in April 2019, the volume increased to 580 mpps.<sup>12</sup>

**WS-DISCOVERY.** Web services dynamic discovery<sup>13</sup> (WS-Discovery) is a multicast discovery protocol. It has been observed being used mostly by IoT devices to automatically discover each node on local area networks (LANs) but, like other protocols, it may not be used only for its intended purpose, especially in the IoT realm<sup>5</sup>. Malicious actors have found it to be a good hotbed for amplifying attacks. A security researcher reported<sup>3</sup> an amplification factor of 95x while another researcher reported an increase of 15.000% compared with the original byte size.<sup>14</sup>

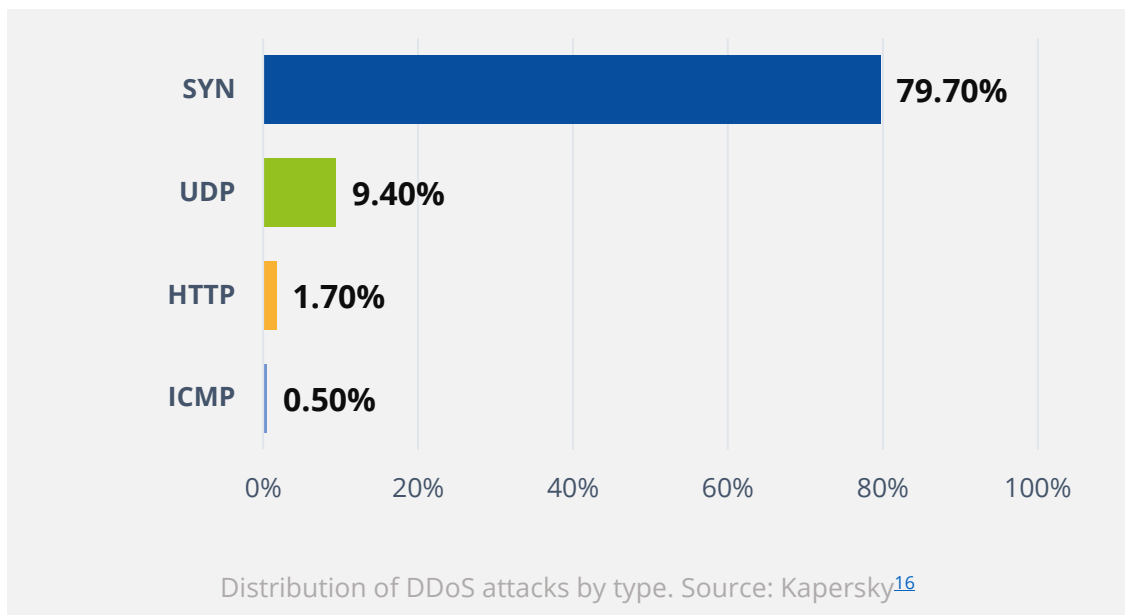
**REFLECTED AND AMPLIFIED ATTACKS.** These types of attacks are widely and historically known to feature a small request to deliver a larger payload. In summary, the malicious actor will spoof the sender's (victim) IP address and subsequently, the recipient host will send all the related responses to the victim.<sup>9</sup> This methodology is mainly effective on UDP based protocol because of their connectionless nature and amplification factor (i.e. CLDAP has an amplification factor of x50-x70). However, TCP protocol is not prone to this type of attack.<sup>15</sup>



A good example of such attempts are SYN-ACK reflected and amplified flooding attacks – this type of flood does not necessarily need to be high bandwidth to have an impact. In contrast, having a high packet per second ration can keep the attack below the radar and increase its effectiveness.<sup>3</sup>

**BIT-AND-PIECE/CARPET BOMBING DDoS.** This type of distributed and reflective denial of service (DRDoS) attack is known to target mostly telecommunication and service provider industries.<sup>17</sup> In one instance<sup>18</sup> of this attack, a random selection of IP addresses of an Internet Service Provider was targeted to reflect the traffic to the edge routers of the provider. Thus, the victim was not able to identify the DDoS until their service was overwhelmed by their own selected IP range.<sup>19</sup>

**MULTI-VECTOR DDOS ATTACKS.** Malicious actors often carry out multiple vectors of DoS attacks to add complexity and variety to their attempt. This means that by merely automating different application layer (HTTP Flood, DNS Flood etc.) and network layer (UDP/TCP reflection/amplification etc.) types of attack, they will try to maximise its impact by saturating the bandwidth as well as resources or services in the targeted environment.<sup>16</sup>



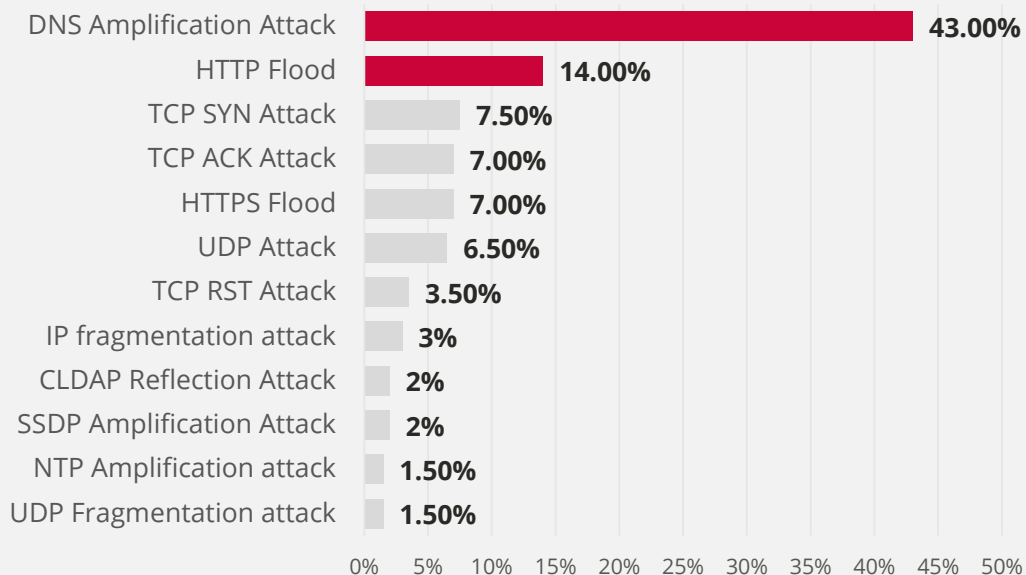
# Attack vectors

## How

Similar to previous years, 2019 was no exception in terms of UDP floods. According to a security researcher, UDP flood was the most popular attack vector and the team believes that might be related to the dominate adoption of this protocol in high-risk industries such as gaming. SYN flood, DNS response and TCP based attacks followed UDP floods in the list of top attack vectors.

Multi-vector attacks were also observed during this period. However, a security researcher believes that some of the multi-vector attacks are an unintended by-product of a DoS attempt.<sup>11</sup>

A cybersecurity report<sup>17</sup> suggested that DNS Amplification attacks were observed by its team as the top DDoS attack vector followed by HTTP flood and TCP SYN attacks. The observations of attack vectors in Q3 2019 were similar with SYN floods, the top vector followed by UDP, TCP and HTTP attacks.

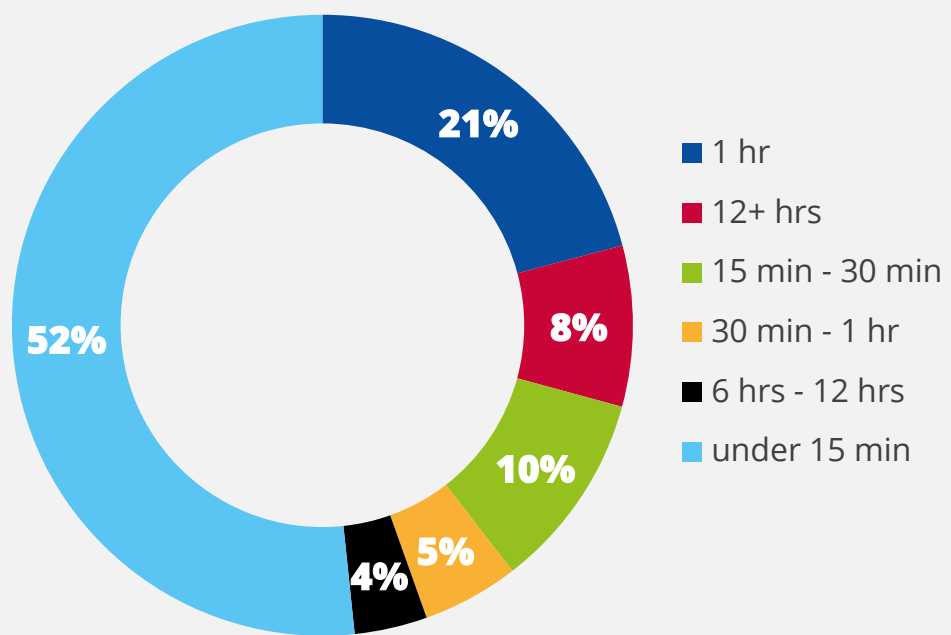


Distribution of DDoS attack vectors. Source: NexusGuard<sup>17</sup>





## Attack Duration



Source: Imperva<sup>11</sup>

## Proposed actions

- Understanding services and critical resources and prioritising defence where these can be overloaded. Ensuring a response plan is in place for such scenarios.<sup>20</sup>
- Depending on the requirements, considering DDoS protection service or a DDoS managed service provider . Use of methods such as monitoring for fast identification of infections.<sup>1</sup>
- Similar to the above point, publishing services through content delivery networks can be an effective way of absorbing volumetric attempts (requires other techniques in place for more sophisticated attacks).<sup>21</sup>
- Internet Service and Cloud Providers play a critical role in defending against DDoS attacks. Having a clear communication plan and channel with them is key to a successful response to a denial of service attack.
- Developing a proactive and strong defensive posture before a critical failure occurs involving the related team and vendors to configure and tune controls based on specific business requirements.<sup>22</sup> Facilitating cache servers or dropping inappropriate queries/request in the application layer at source and implementing BCP<sup>23</sup> for service providers are good instances of proactive measures.
- Ensure you test and re-evaluate your defence techniques, technologies and providers.
- Produce a risk register by analysing your environment inside-out. Starting from your critical assets inside and working your way to your Internet footprint and presence.<sup>24</sup>

**“Although DDoS attacks are not new to cybersecurity and network defenders, their level of sophistication is increasing, and malicious actors are observed to be actively running more reconnaissance activities than before”**

in ETL 2020

# References

1. "Understanding Denial-of-Service Attacks" November 20, 2019. CISA. <https://www.us-cert.gov/ncas/tips/ST04-015>
2. Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. "DDoS attacks in Q1 2019" May 21, 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." July 2, 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%." September 18, 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" February 7, 2019. Kaspersky. <https://securelist.com/ddos-attacks-in-q4-2018/89565/>
7. Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. "DDoS attacks in Q3 2019" November 11, 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." November 19, 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." April 30, 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" July 1, 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." September 18, 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." November 9, 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." November 11, 2019. Kaspersky. [https://usa.kaspersky.com/about/press-releases/2019\\_kaspersky-report-finds-over-half-of-q3-ddos-attacks-occurred-in-september](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." September 22, 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." September 24, 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.” November 13, 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.” March 10, 2017. CERT-EU. [https://cert.europa.eu/static/WhitePapers/CERT-EU\\_Security\\_Whitepaper\\_DDoS\\_17-003.pdf](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.” May 2000. IETF Tools. <https://tools.ietf.org/html/bcp38>
- 24.** Pierluigi Paganini. “Cyber Defense Magazine Sept Edition 2019.” September 4, 2019. SecurityAffairs. <https://securityaffairs.co/wordpress/90795/breaking-news/cyber-defense-magazine-september-2019.html>

# Related



[READ THE REPORT](#)

## ENISA Threat Landscape Report **The year in review**

A summary on the cybersecurity trends for the period between January 2019 and April 2020.



[READ THE REPORT](#)

## ENISA Threat Landscape Report **List of Top 15 Threats**

ENISAs' list of the top 15 threats of the period between January 2019 and April 2020.

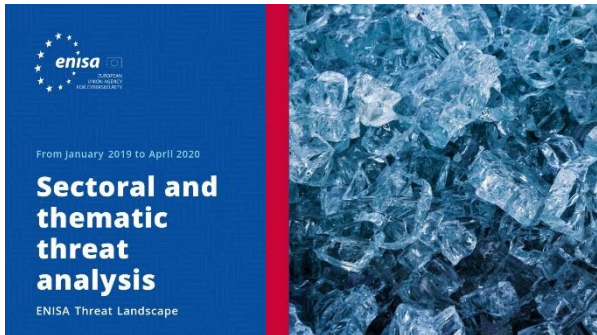


[READ THE REPORT](#)

## ENISA Threat Landscape Report **Research topics**

Recommendations on research topics from various quadrants in cybersecurity and cyber threat intelligence.





[READ THE REPORT](#)

## ENISA Threat Landscape Report **Sectoral and thematic threat analysis**

Contextualised threat analysis between January 2019 and April 2020.



[READ THE REPORT](#)

## ENISA Threat Landscape Report **Emerging trends**

Main trends in Cybersecurity observed between January 2019 and April 2020.



[READ THE REPORT](#)

## ENISA Threat Landscape Report **Cyber Threat Intelligence overview**

The current state of play of cyber threat intelligence in the EU.

## – The agency

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at [www.enisa.europa.eu](http://www.enisa.europa.eu).

### **Contributors**

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) and *all members of the ENISA CTI Stakeholders Group*: Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) and Thomas Hemker.

### **Editors**

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

### **Contact**

For queries on this paper, please use [enisa.threat.information@enisa.europa.eu](mailto:enisa.threat.information@enisa.europa.eu).

For media enquiries about this paper, please use [press@enisa.europa.eu](mailto:press@enisa.europa.eu).







## Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

## Copyright Notice

© European Union Agency for Cybersecurity (ENISA), 2020  
Reproduction is authorised provided the source is acknowledged.

Copyright for the image on the cover: © Wedia. For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.

**ISBN:** 978-92-9204-354-4

**DOI:** 10.2824/552242



Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Greece  
Tel: +30 28 14 40 9711  
[info@enisa.europa.eu](mailto:info@enisa.europa.eu)  
[www.enisa.europa.eu](http://www.enisa.europa.eu)



All rights reserved. Copyright ENISA 2020.

<https://www.enisa.europa.eu>