



# 2022

# Summary of Cloud DDoS Protection

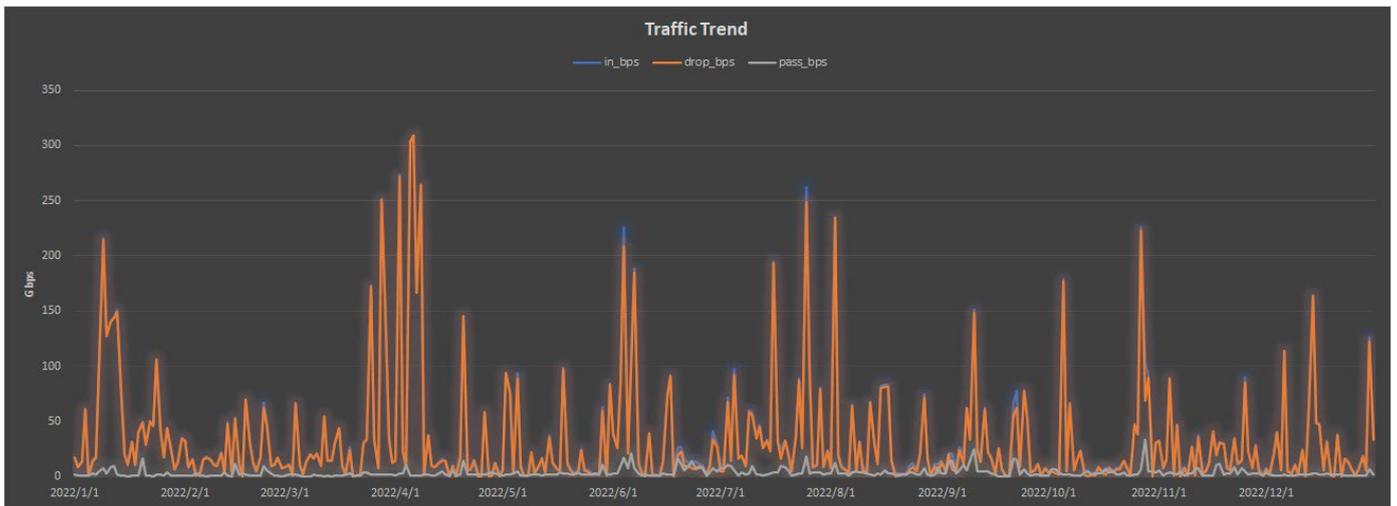
NSFOCUS Security Operation Center

The NSFOCUS logo is displayed in white, bold, uppercase letters. It is positioned in the lower-left corner of a dark green background that features a complex network of glowing green lines and dots, resembling a data network or a globe with digital connections.

# 1. Overview

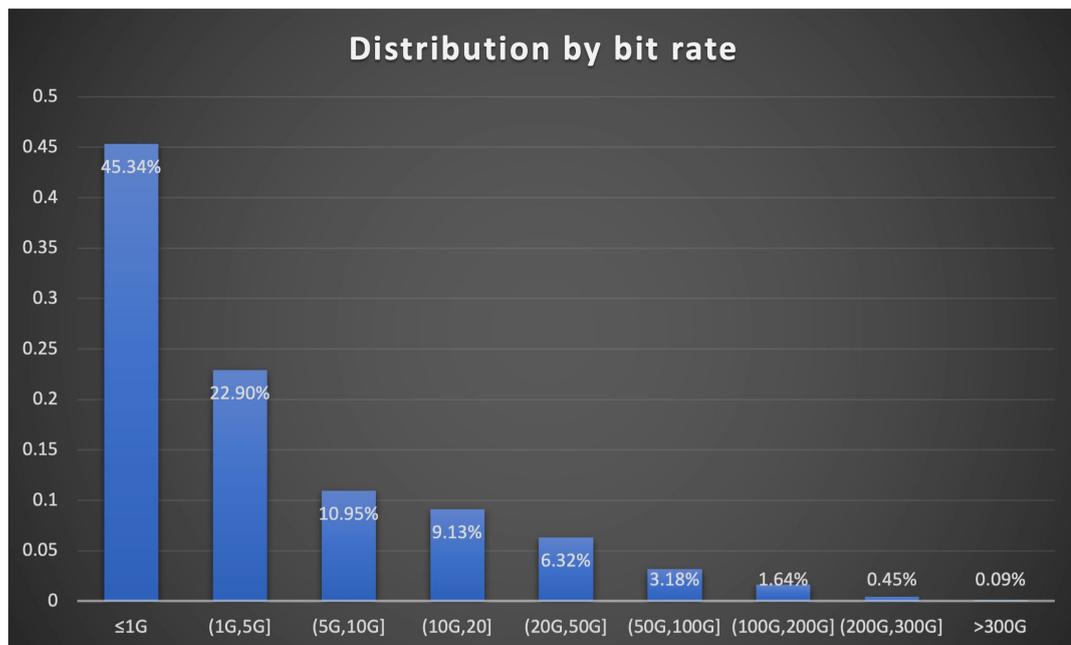
2022 has ended. NSFOCUS SOC team summarized the DDoS attacks protected by NSFOCUS cloud-based DDoS Protection System (DPS) and wrapped up attack trends and attack size distribution in 2022. All the data in this article comes from NSFOCUS's Active Defense Business Operations System (ADBOS).

## 2. Traffic Trend 2022



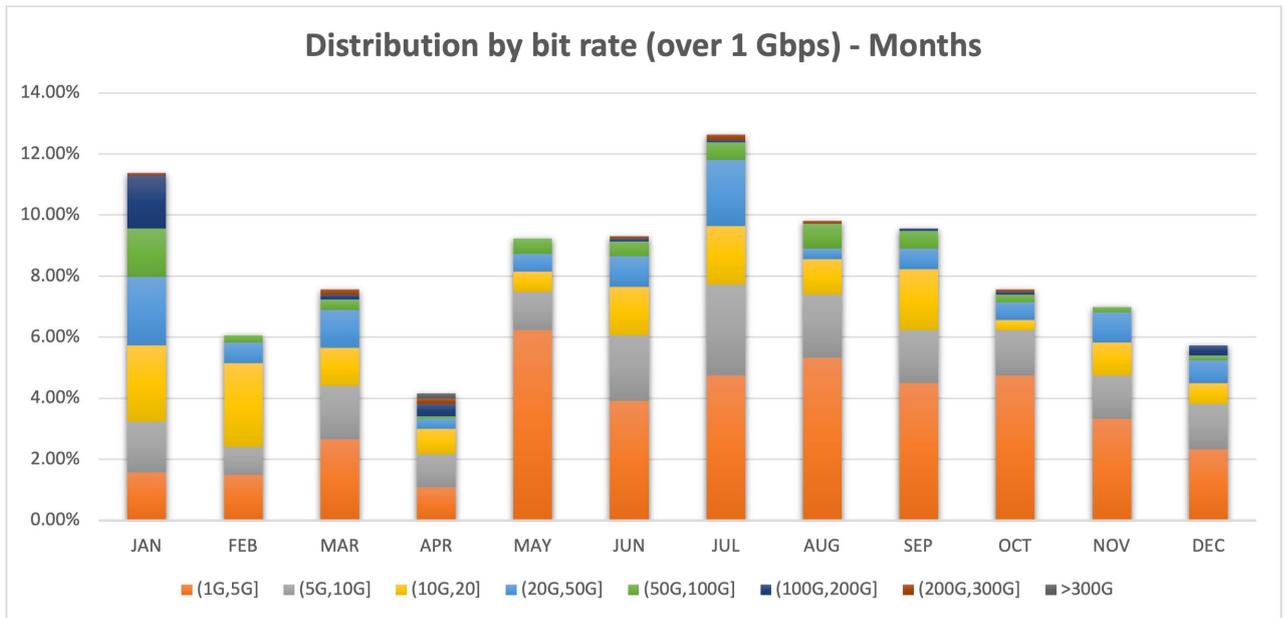
The overall attack traffic trend in 2022 was relatively stable. More than 150Gbps attacks were recorded every month.

## 3. Attack Distribution by Bit Rate

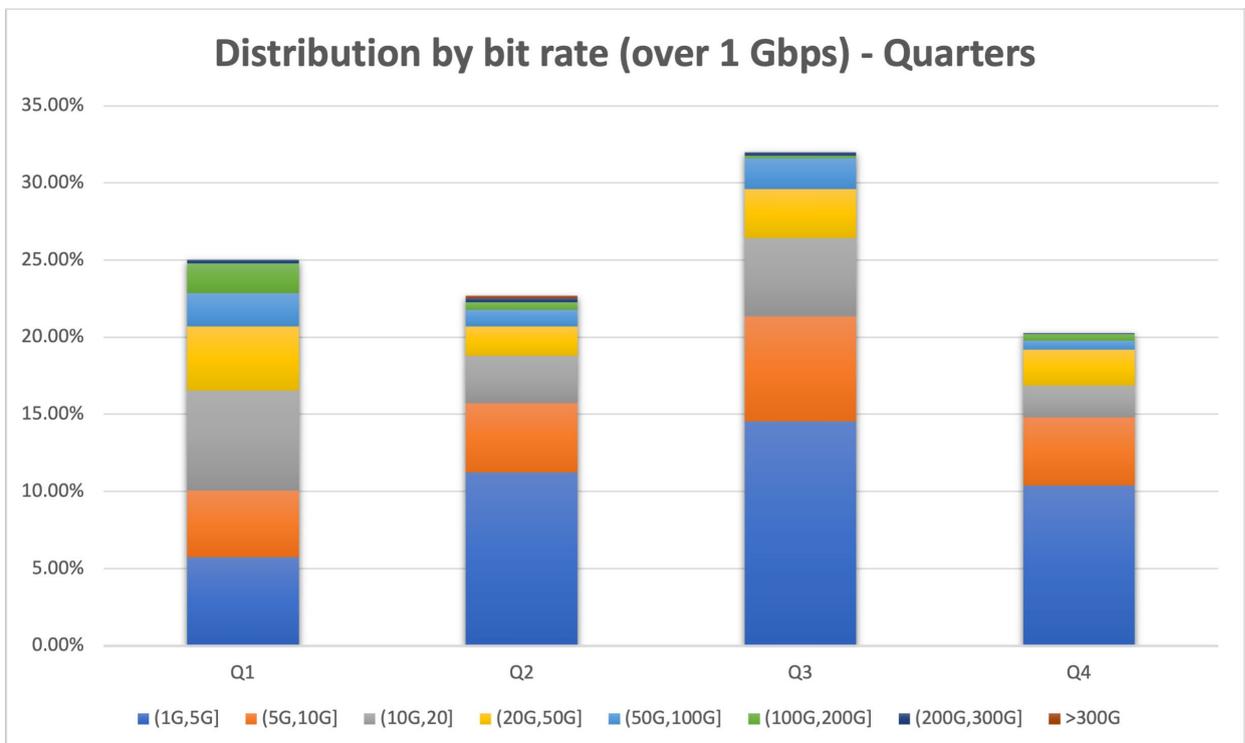


Of the attacks recorded in 2022, 68.24% were smaller than 5Gbps, and 2.18% were larger than 100Gbps.

## 4. Distribution by Bit Rate (Larger than 1Gbps) per Month

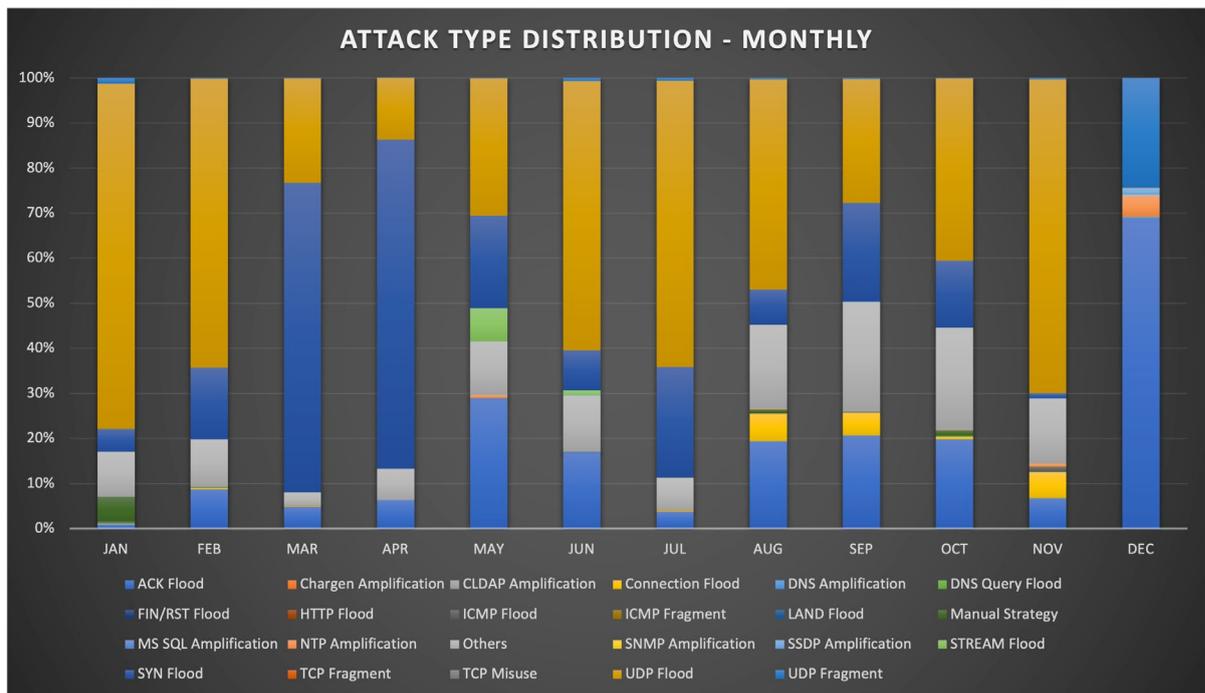


## 5. Attack Distribution by Bit Rate (Larger than 1Gbps) per Quarter



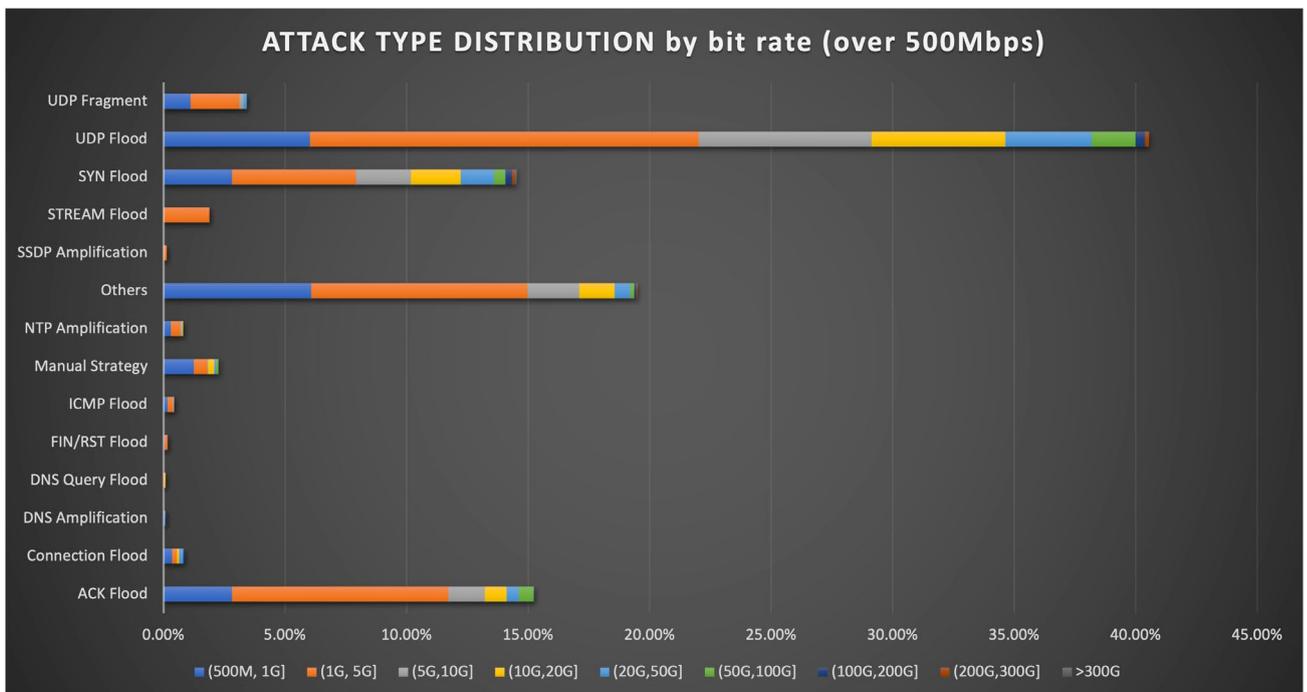
The third quarter of 2022 saw record-level volumes, accounting for 30% of the total attacks larger than 1Gbps in the whole year.

## 6. Attack Type Distribution per Month



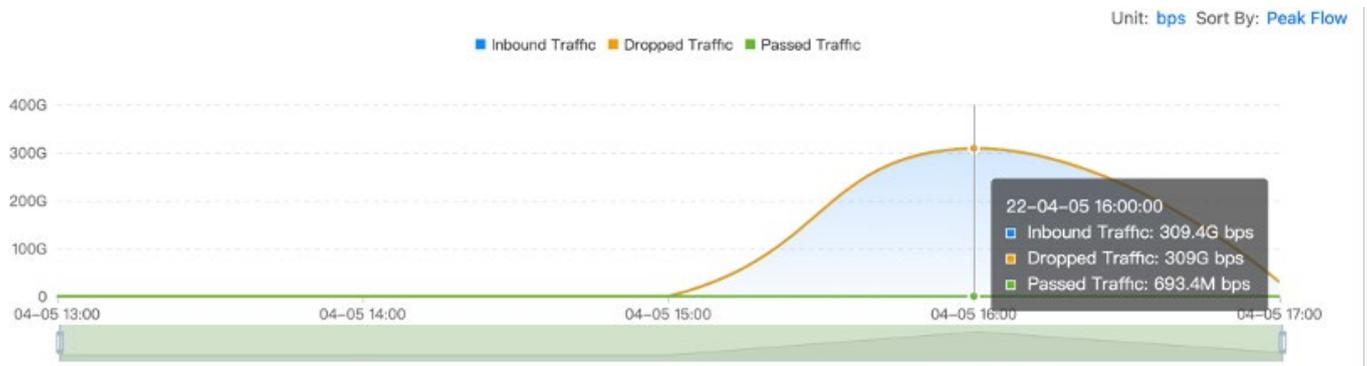
The UDP Flood was still the predominant attack type and was underscored in January 2022. The ACK Flood ranked second.

## 7. Attack Type Distribution by Bit Rate



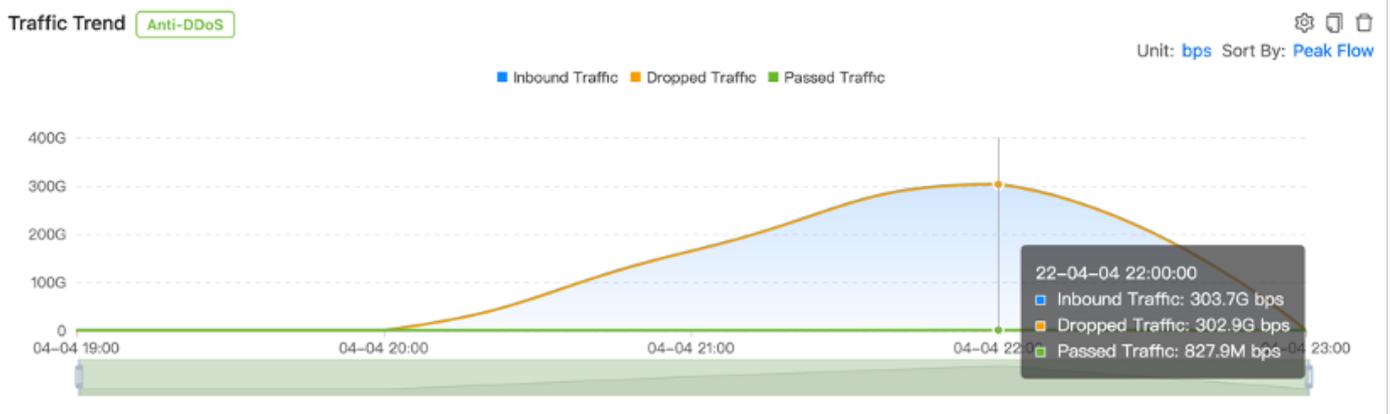
# 8. TOP 3 Attack Peaks

## 8.1 Peak attack size 309.4Gbps



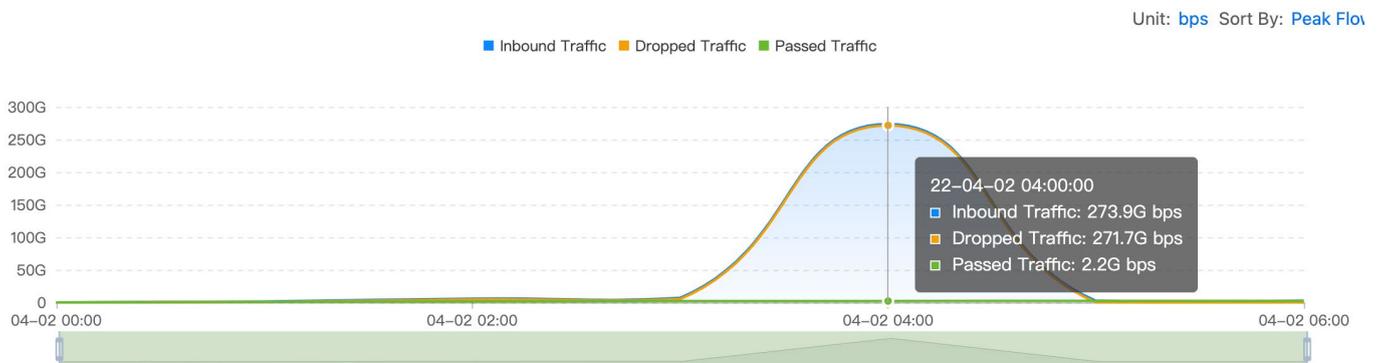
In April 2022, NSFOCUS mitigated a volumetric DDoS attack at a peak of 309.4Gbps, including 302.2Gbps SYN Flood, with cleaning efficiency reaching 99.87%.

## 8.2 Peak attack size 303.7Gbps



Another volumetric DDoS attack NSFOCUS mitigated was at a peak of 303.7Gbps, including 302.9Gbps SYN Flood, with cleaning efficiency reaching 99.73%.

## 8.3 Peak attack size 273.9Gbps



A volumetric DDoS attack containing 271.6Gbps UDP Flood with the attack peak reaching 273.9Gbps was mitigated by NSFOCUS. The cleaning efficiency was 99.19%.

# 9. New Types of Attacks in 2022

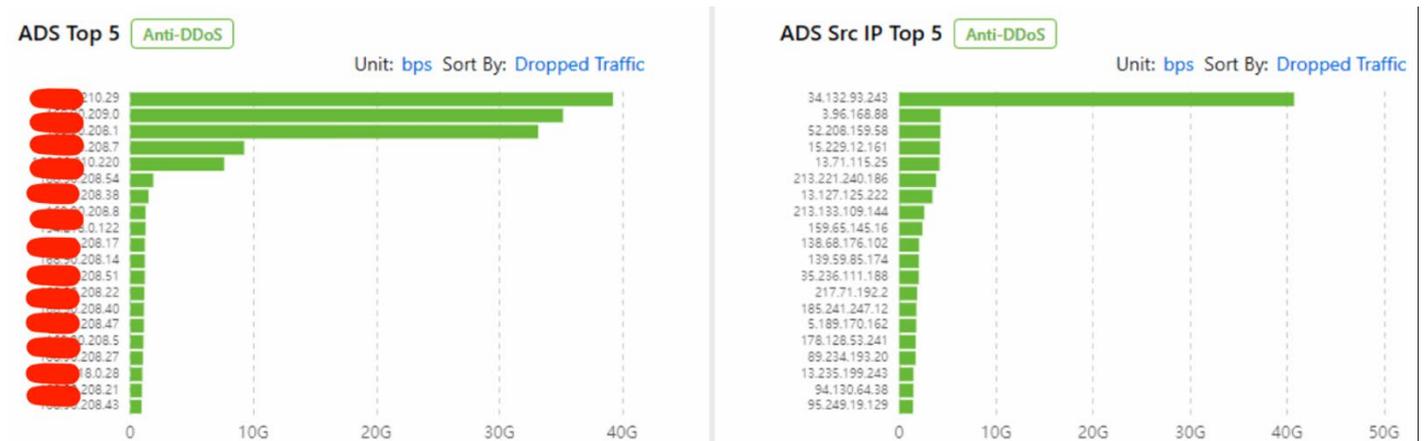
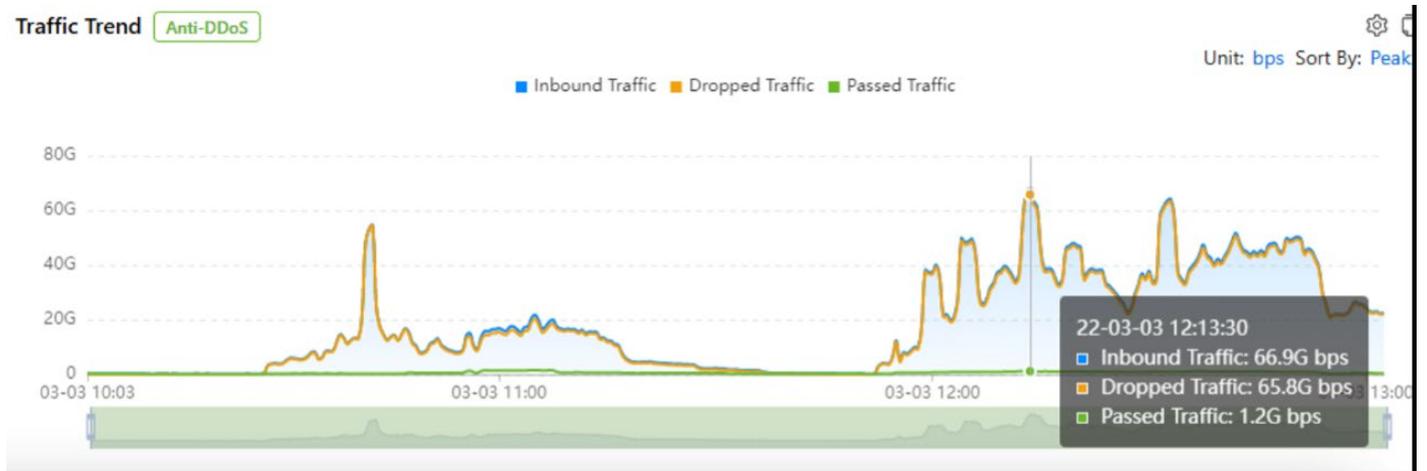
## 9.1 Reflection amplification attack based on CVE-2022-26143

### 9.1.1 Overview

NSFOCUS captured a customer's UDP Flood traffic and found that the destination port is 10074, related to vulnerability exploits discovered not long ago (See the [CVE detail](#)).

### 9.1.2 Details

An attacker leveraging TP-240 reflection/amplification can launch a high-impact DDoS attack using a single packet. Examination of the tp240dvr binary reveals that, due to its design, an attacker can theoretically cause the service to emit 2,147,483,647 responses to a single malicious command. Each response generates two packets on the wire, leading to some 4,294,967,294 amplified attack packets being directed toward the attack victim.



### 9.1.3 Protection

Limited the UDP traffic for the protection group in which the customer's IP address was contained.

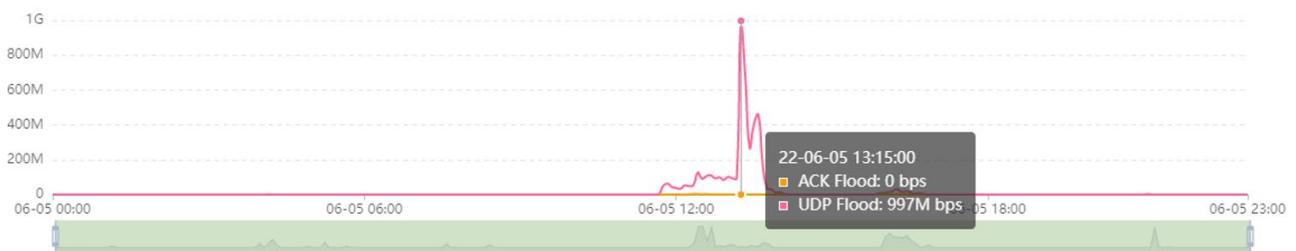
## 9.2 HTTPU attack

### 9.2.1 Overview

NSFOCUS captured some packages when some UDP Flood escaped from the protection algorithm and found that the UDP has HTTP headers information in Data.

### 9.2.2 Details

Such packets are often used for communications between IoT devices. Attackers can use reflection to make some IoT devices on the public network become reflection sources for DDoS attacks.



Time	Source	Destination	Protocol	Length	Time to Live	Sequence Number (raw)	Acknowledgment number (raw)	Source Port	Destination Port	Info
1 0.000000			UDP	440	56					58664 → 39088 Len=398
2 0.067793			UDP	372	60					38738 → 61753 Len=330
3 0.072330			UDP	461	55					38376 → 3029 Len=419
4 0.072332			UDP	470	55					38376 → 3029 Len=428
5 0.072834			UDP	541	55					41591 → 3029 Len=499
6 0.073289			UDP	525	55					38376 → 3029 Len=483
7 0.117465			UDP	470	54					35083 → 32853 Len=419
8 0.117465			UDP	461	54					35083 → 32853 Len=419
9 0.118683			UDP	525	54					35083 → 32853 Len=483
10 0.122158			UDP	541	54					43635 → 32853 Len=499
11 0.137633			UDP	463	57					60559 → 32423 Len=421
12 0.137642			UDP	472	57					60559 → 32423 Len=430
13 0.137645			UDP	527	57					60559 → 32423 Len=485
14 0.137890			UDP	543	57					42370 → 32423 Len=591
15 0.144223			UDP	461	53					50675 → 34019 Len=419
16 0.144234			UDP	470	53					50675 → 34019 Len=428
17 0.144236			UDP	533	53					50675 → 34019 Len=491
18 0.144831			UDP	505	53					40162 → 34019 Len=463
19 0.145226			UDP	470	53					36826 → 34019 Len=428
20 0.145227			UDP	509	53					36826 → 34019 Len=467
21 0.145842			UDP	541	53					33045 → 34019 Len=499
22 0.146604			UDP	470	53					48358 → 34019 Len=428
23 0.147111			UDP	529	53					48358 → 34019 Len=487
24 0.148314			UDP	523	53					56452 → 34019 Len=481
25 0.149608			UDP	489	56					30286 → 8391 Len=447
26 0.149716			UDP	445	55					30838 → 8391 Len=403
27 0.149718			UDP	454	55					30838 → 8391 Len=412

Frame 11: 463 bytes on wire (3704 bits), 463 bytes captured (3704 bits) on  
Ethernet II, Src: CASwell\_09:57:34 (08:35:71:09:57:34), Dst: Aristalle\_25:d7:ab (28:99:3a:25:d7:ab)  
Internet Protocol Version 4, Src: [REDACTED], Dst: [REDACTED]  
User Datagram Protocol, Src Port: 60559, Dst Port: 32423  
Data (421 bytes)  
Data: 485454502f312e3120323030204f4b0d0a43414348452d434f4e54524f4c3a206d61782d...  
[Length: 421]

```
0020 f1 e2 ec 8f 7e a7 01 ad bb 04 48 54 54 50 2f 31 ..... HTTP/1
0030 2e 31 20 32 30 20 4f 4b 0d 0a 43 41 43 48 45 ..1.200 OK - CACHE
0040 2d 43 4f 4e 54 52 4f 4c 3a 20 6d 61 78 2d 61 67 ..CONTROL: max-ag
0050 65 3d 33 36 30 30 0d 0a 44 41 54 45 3a 20 53 75 ..e=3600 - DATE: Su
0060 6a 2c 20 30 35 20 40 75 6a 20 32 30 32 32 20 36 ..n, 05 Jun 2022 0
0070 32 3a 33 31 3a 31 39 20 47 4d 54 0d 0a 45 58 54 ..2:31:19 GMT -EXT
0080 3a 0d 0a 4c 4f 43 41 54 49 4f 4e 3a 20 68 74 74 ..-LOCAT ION: htt
```

```
HTTP/1.1 200 OK
CACHE-CONTROL: max-age=3600
DATE: Sun, 05 Jun 2022 02:31:19 GMT
EXT:
LOCATION: http://192.168.1.200:90/upnpdevicedesc.xml
OPT: "http://schemas.upnp.org/upnp/1/0/"; ns=01
01-NLS: 6ecc2d06-1dd2-11b2-9d22-adb5077379a2
SERVER: Linux/3.18.20, UPnP/1.0, Portable SDK for UPnP devices/1.6.18
X-User-Agent: redsonic
ST: upnp:rootdevice
USN: uuid:48433138-3331-3832-3633-64DB8BAAFB81::upnp:rootdevice
```

## 9.2.3 Protection

- 1) Performed pattern matching on UDP traffic and dropped packets starting with HTTP/1.1 in the Data field.
- 2) Worked with the customer to block traffic on the customer's non-business port.

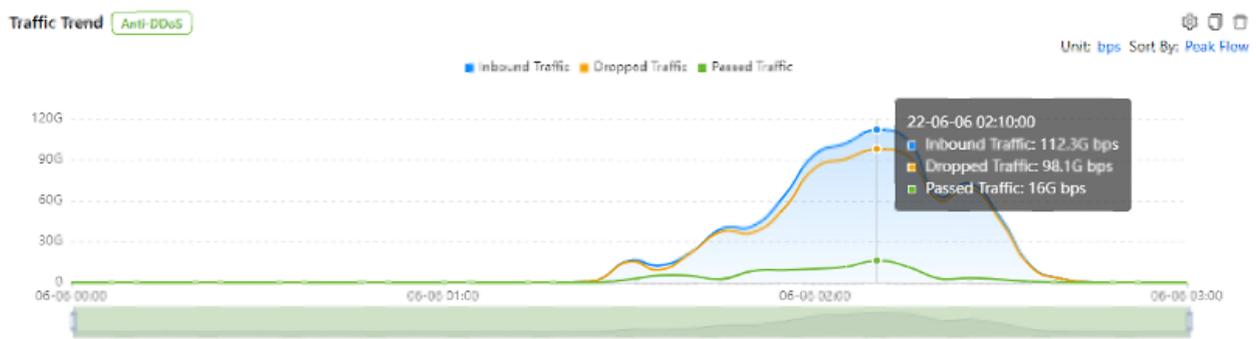
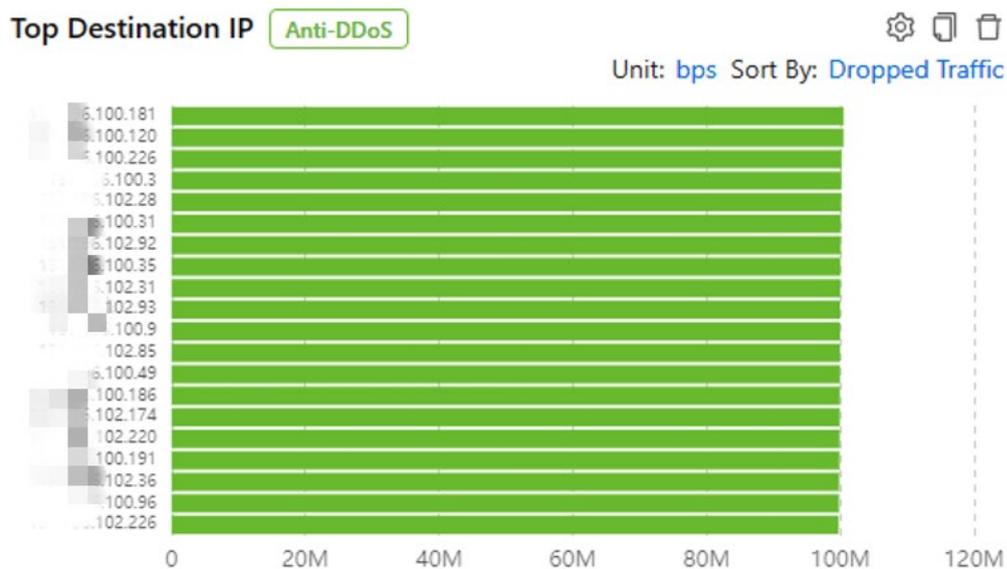
## 9.3 UDP-based carpet-bombing attack

### 9.3.1 Overview

Every IP address in the same network prefix of the customer was attacked with 100Mbps UDP at the same time, causing the customer's bandwidth affected.

### 9.3.2 Details

The attacker used a large number of bot devices on the public network to send a small number of UDP data packets to multiple IP addresses of the target network segment. In this way, it was very easy to achieve the attacker's purpose of occupying the target bandwidth, as the small number of packets is hard to trigger the protection threshold.



### 9.3.3 Protection

#### 1) Short-term measures

Put the victim IP segment in a separate protection group and used a lower UDP threshold to limit the speed of UDP.

#### 2) Recommendation for long-term protection

Leverage NSFOCUS Threat Intelligence (NTI) to identify and block IP addresses on the public network where carpet bombing attacks exist.

## About NSFOCUS

NSFOCUS is an iconic internet and application security company with over 22 years of proven industry experience. Today, we are operating globally with over 5000 employees at two headquarters in Beijing, China and Santa Clara, CA, USA with over 50 offices worldwide. NSFOCUS protects 6 of the 10 largest global telecommunications companies and 4 of the 5 largest global financial institutions.

With its multi-tenant and distributed cloud security platforms, NSFOCUS effectively moves security into the internet backbone by: operating in data centers around the world, enabling organizations to fully leverage the promise of cloud computing, providing unparalleled and uncompromising protection and performance, and empowering our partners to provide better security as a service in a smart and simple way. NSFOCUS delivers holistic, carrier-grade, hybrid DDoS and web security powered by industry-leading threat intelligence. For more information about NSFOCUS, please visit <http://www.nsfocusglobal.com>.