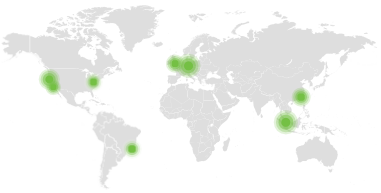
REPORT



2022

Summary of Cloud DDoS Protection

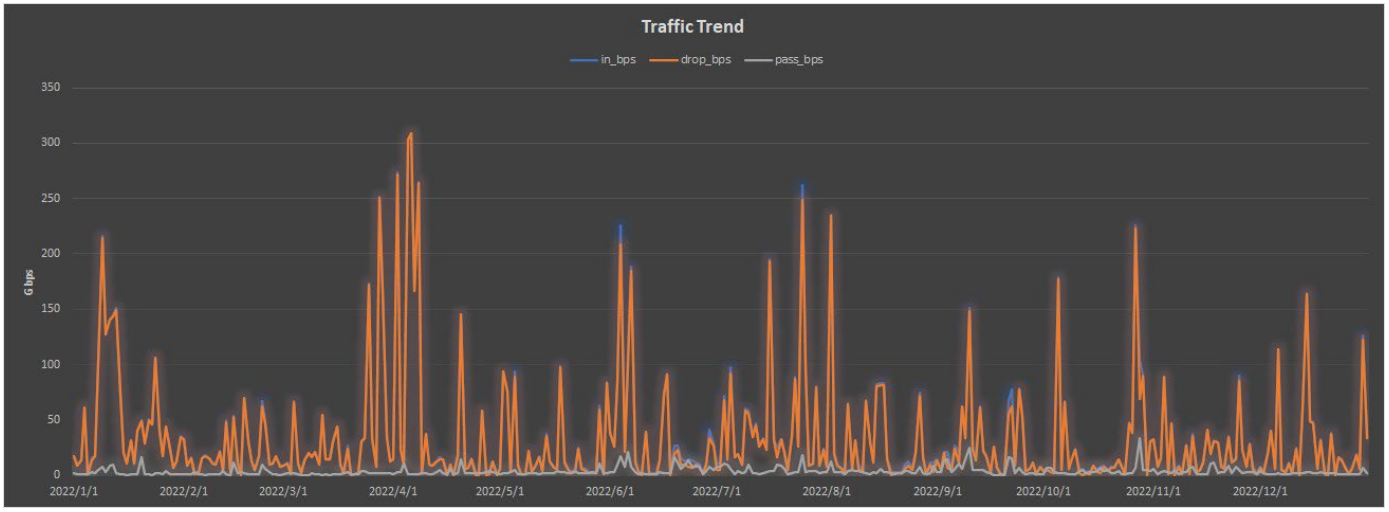
NSFOCUS Security Operation Center

NSFOCUS

1. Overview

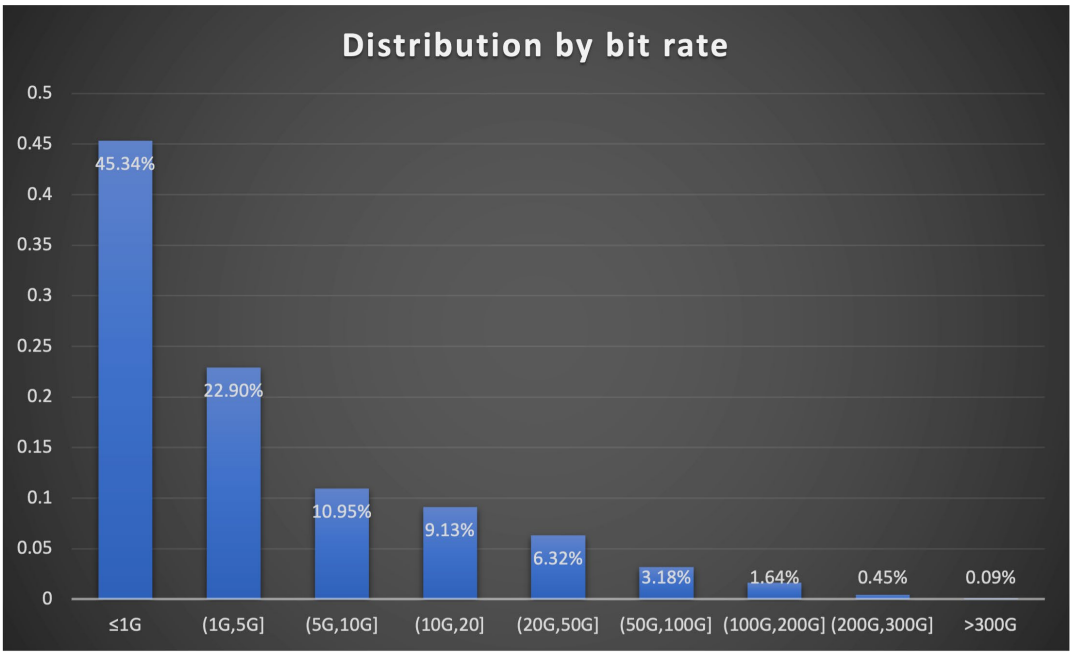
2022 has ended. NSFOCUS SOC team summarized the DDoS attacks protected by NSFOCUS cloud-based DDoS Protection System (DPS) and wrapped up attack trends and attack size distribution in 2022. All the data in this article comes from NSFOCUS's Active Defense Business Operations System (ADBOS).

2. Traffic Trend 2022



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

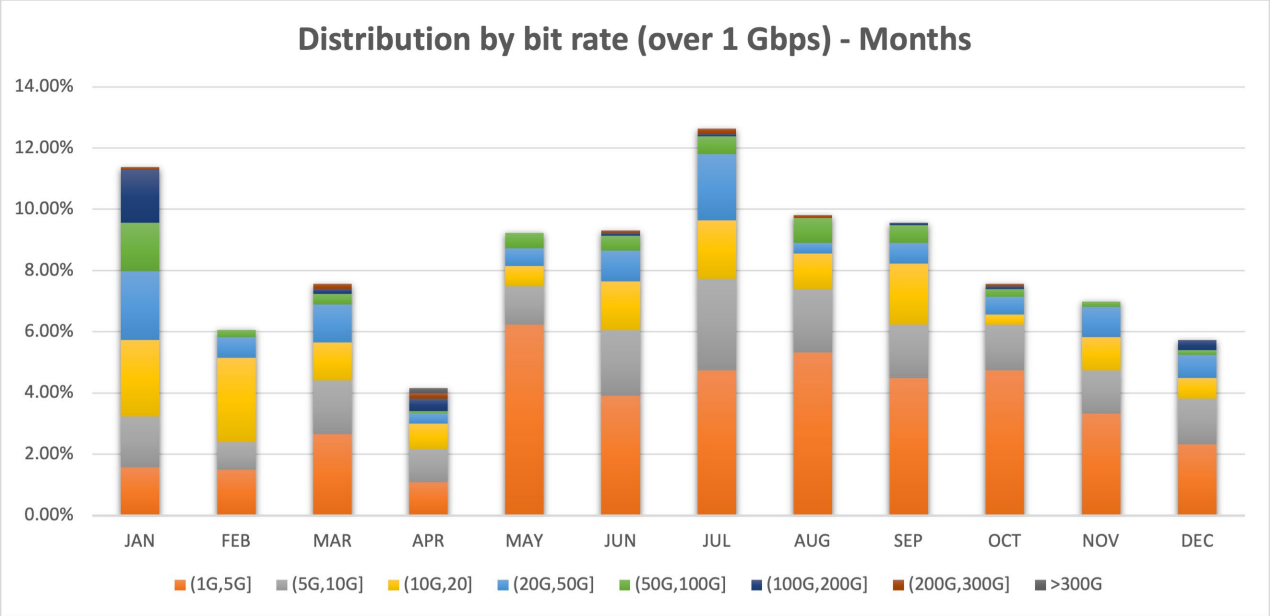
3. Attack Distribution by Bit Rate



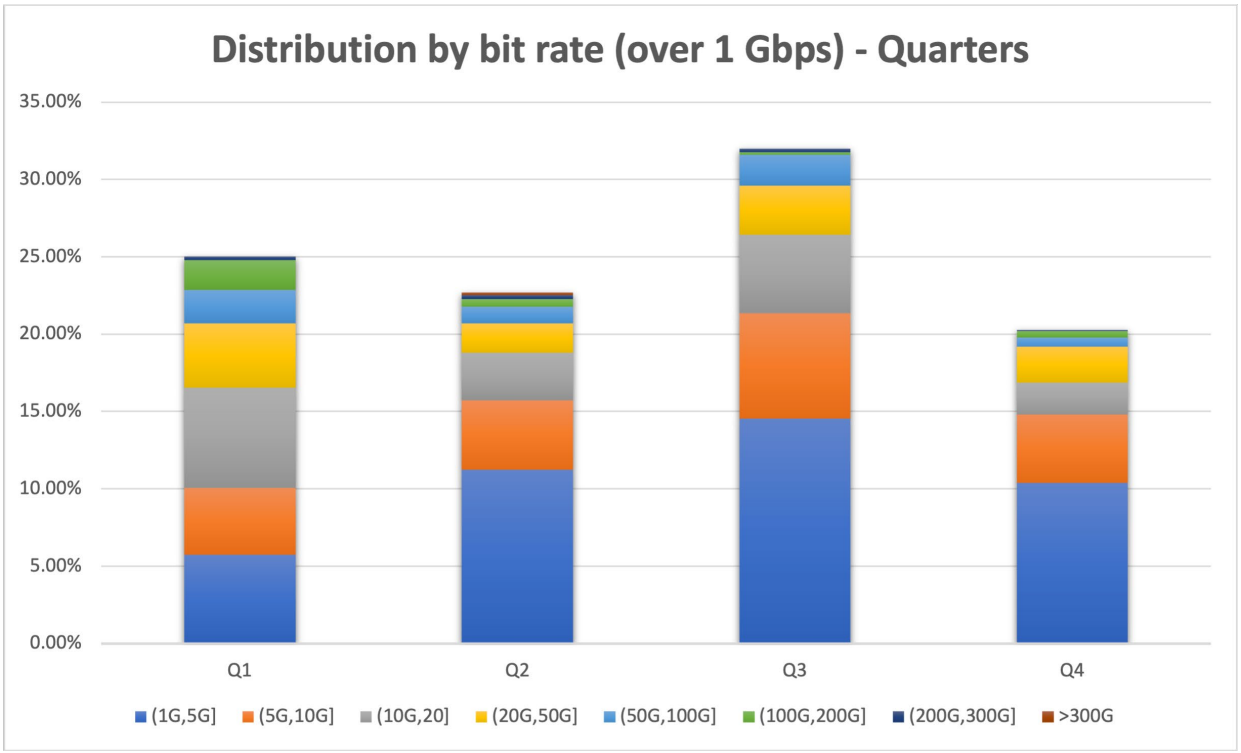
Of the attacks recorded in 2022, 68.24% were smaller than 5Gbps, and 2.18% were larger than 100Gbps.

© COPYRIGHT 2023, NSFOCUS. ALL RIGHTS RESERVED. SUMMARY OF DPS ATTACKS IN 2022

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



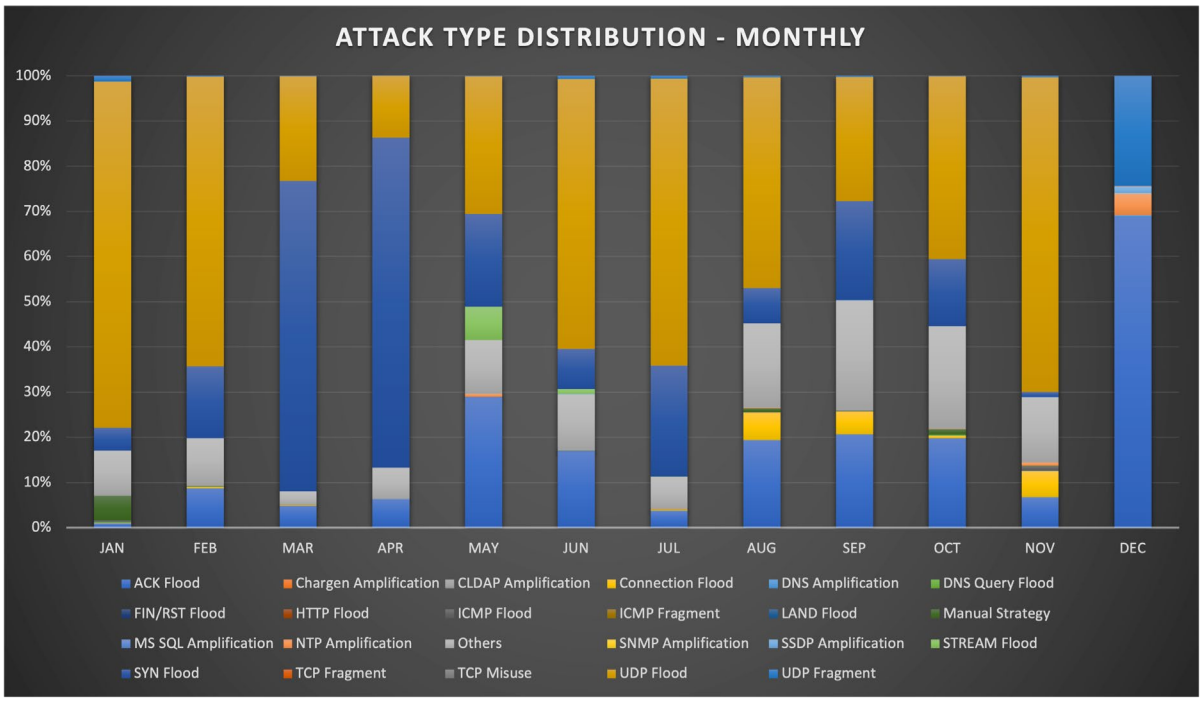
5. Attack Distribution by Bit Rate (Larger than 1Gbps) per Quarter



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

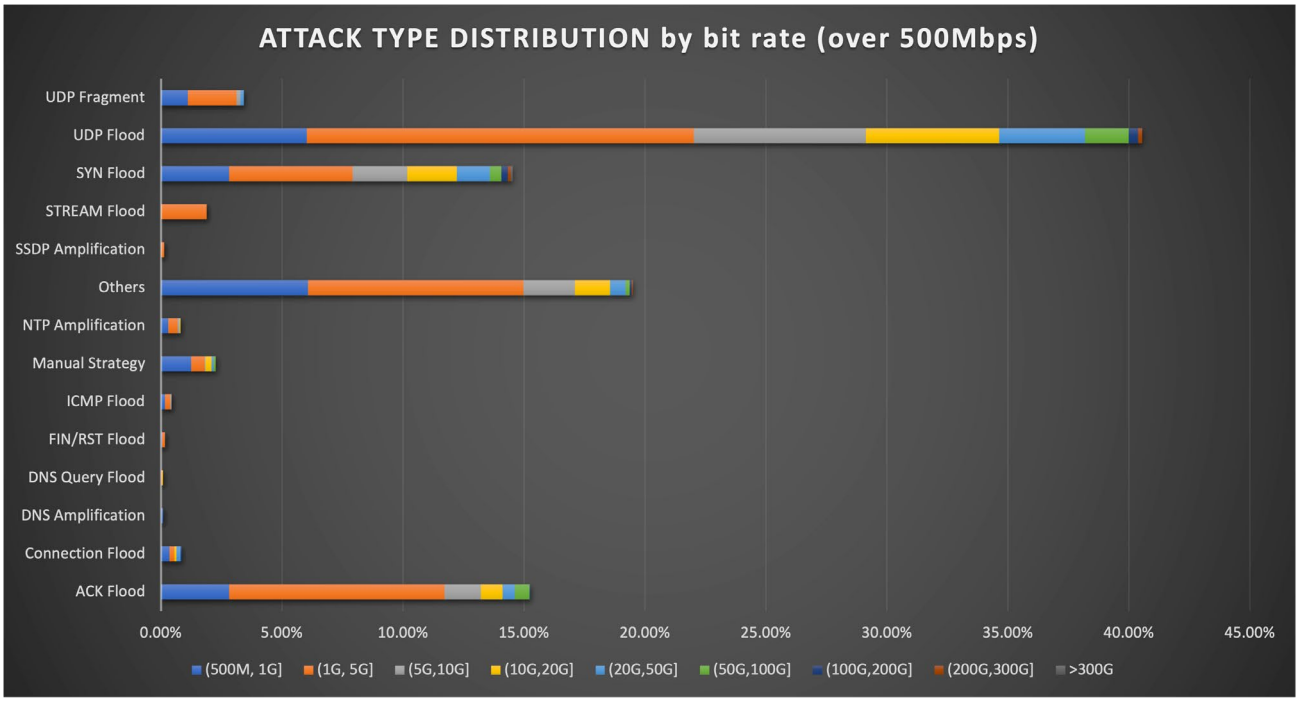
© COPYRIGHT 2023, NSFOCUS. ALL RIGHTS RESERVED. SUMMARY OF DPS ATTACKS IN 2022

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.

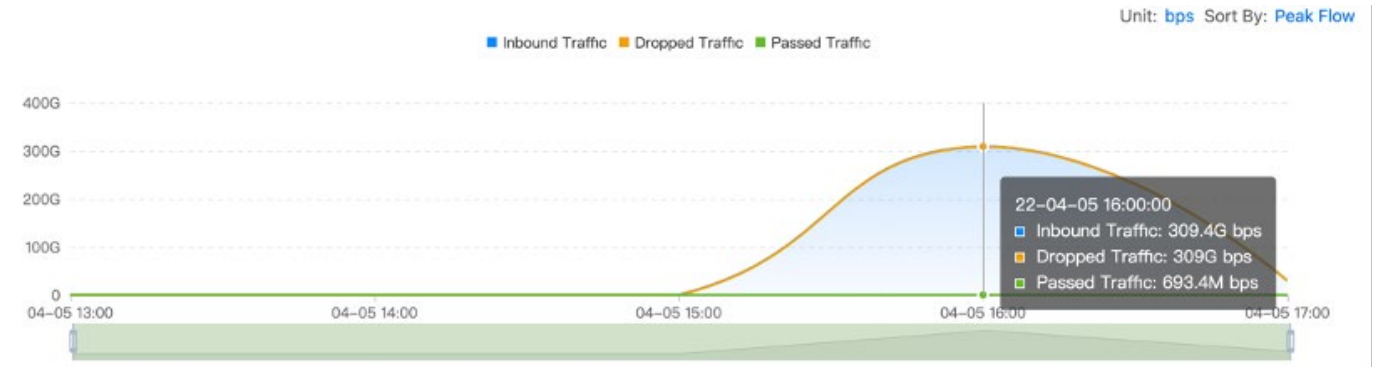
7. Attack Type Distribution by Bit Rate



© COPYRIGHT 2023, NSFOCUS. ALL RIGHTS RESERVED. SUMMARY OF DPS ATTACKS IN 2022

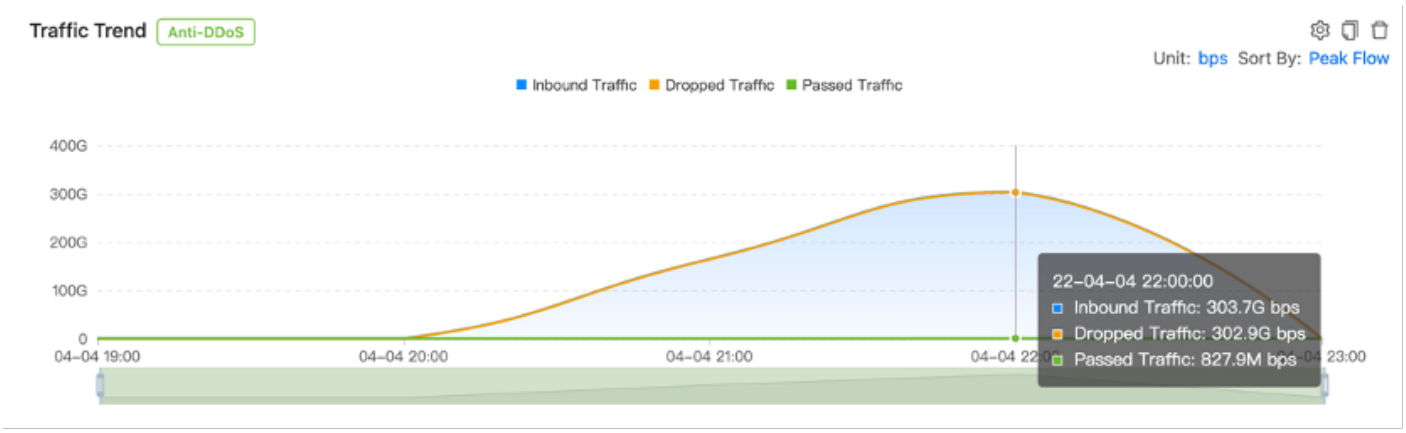
8. TOP 3 Attack Peaks

8.1 Peak attack size 309.4Gbps



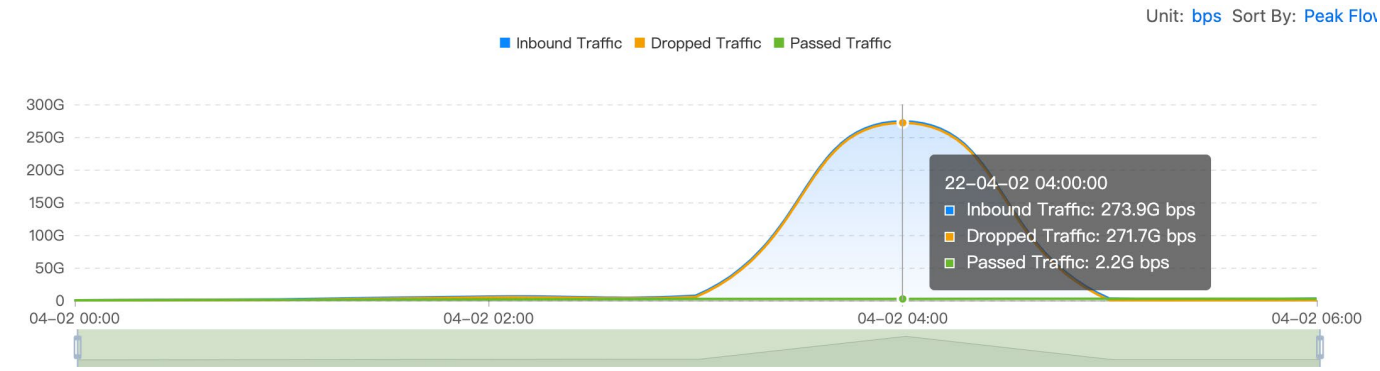
In April 2022, NSFOCUS mitigated a volumetric DDoS attack at a peak of 309.4Gpbs, including 302.2Gbps SYN Flood, with cleaning efficiency reaching 99.87%.

8.2 Peak attack size 303.7Gbps



Another volumetric DDoS attack NSFOCUS mitigated was at a peak of 303.7Gpbs, 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%.

© COPYRIGHT 2023, NSFOCUS. ALL RIGHTS RESERVED. SUMMARY OF DPS ATTACKS IN 2022

9. New Types of Attacks in 2022

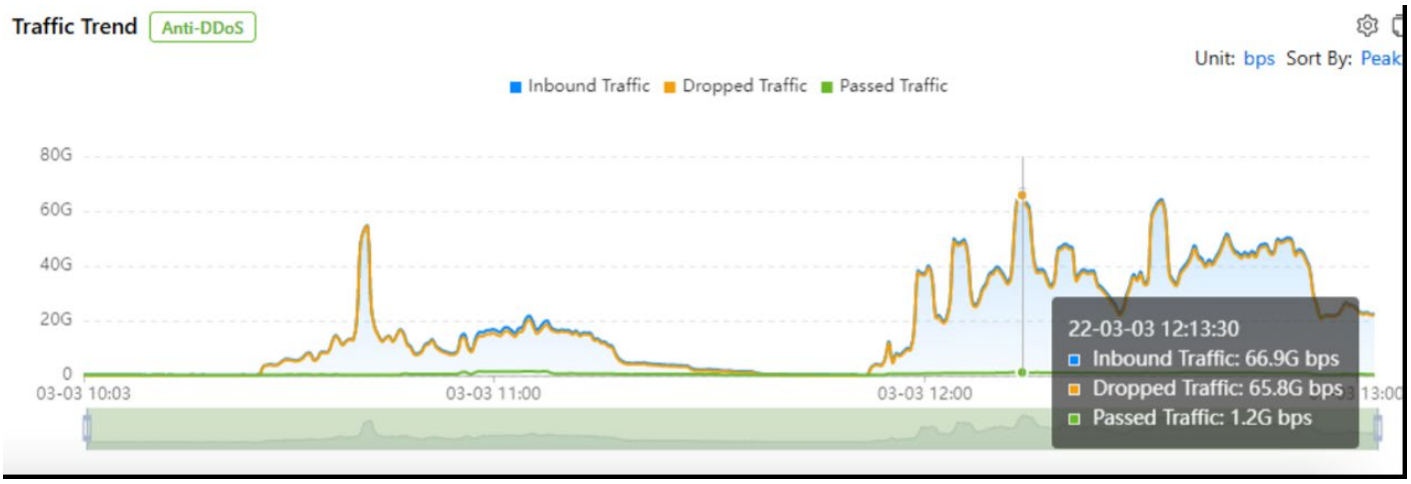
9.1 Reflection amplification attack based on CVE-2022-26143

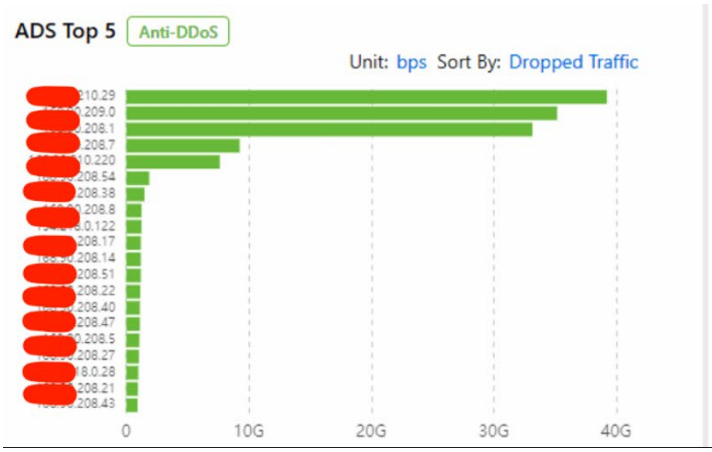
9.1.1 Overview

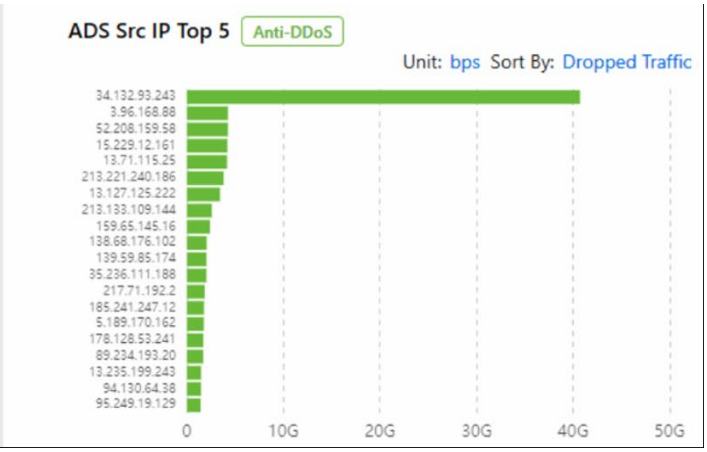
NSFOCUS captured a customer's UDP Flood traffic and found that the destination port is 10074, related to vulnerability exploits discovered not long ago (See the CVE detail).

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.

© COPYRIGHT 2023, NSFOCUS. ALL RIGHTS RESERVED. SUMMARY OF DPS ATTACKS IN 2022

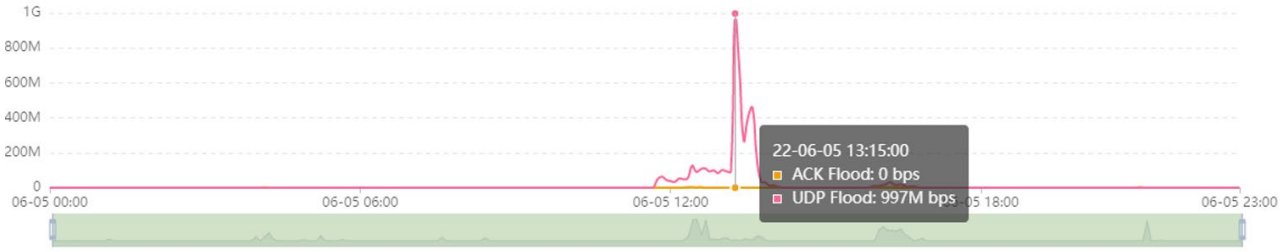
9.2 HTTPU attack

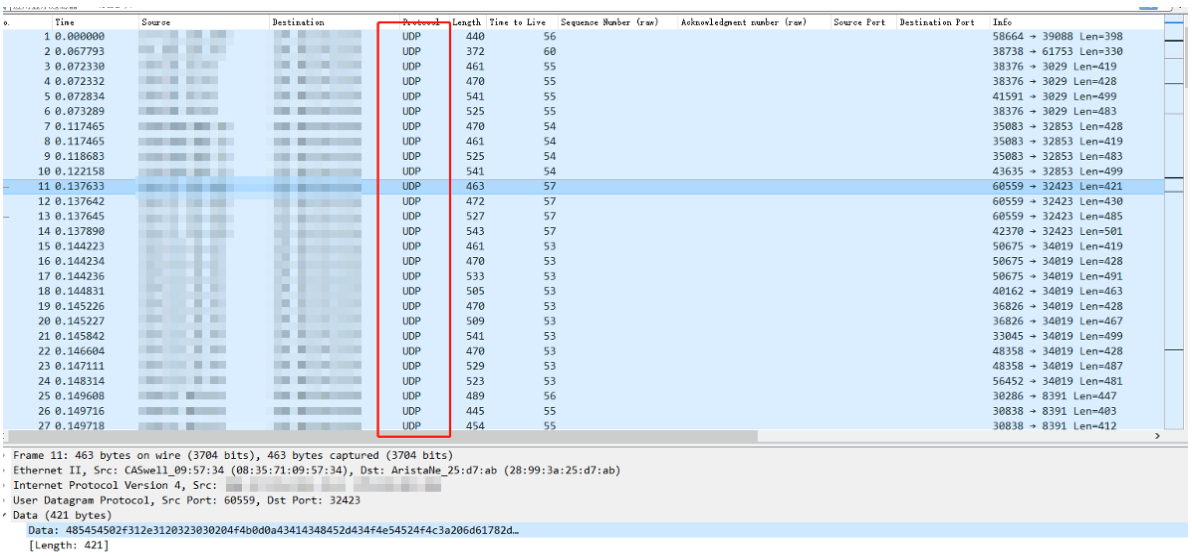
9.2.1 Overview

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.






```
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
```


© COPYRIGHT 2023, NSFOCUS. ALL RIGHTS RESERVED. SUMMARY OF DPS ATTACKS IN 2022

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.

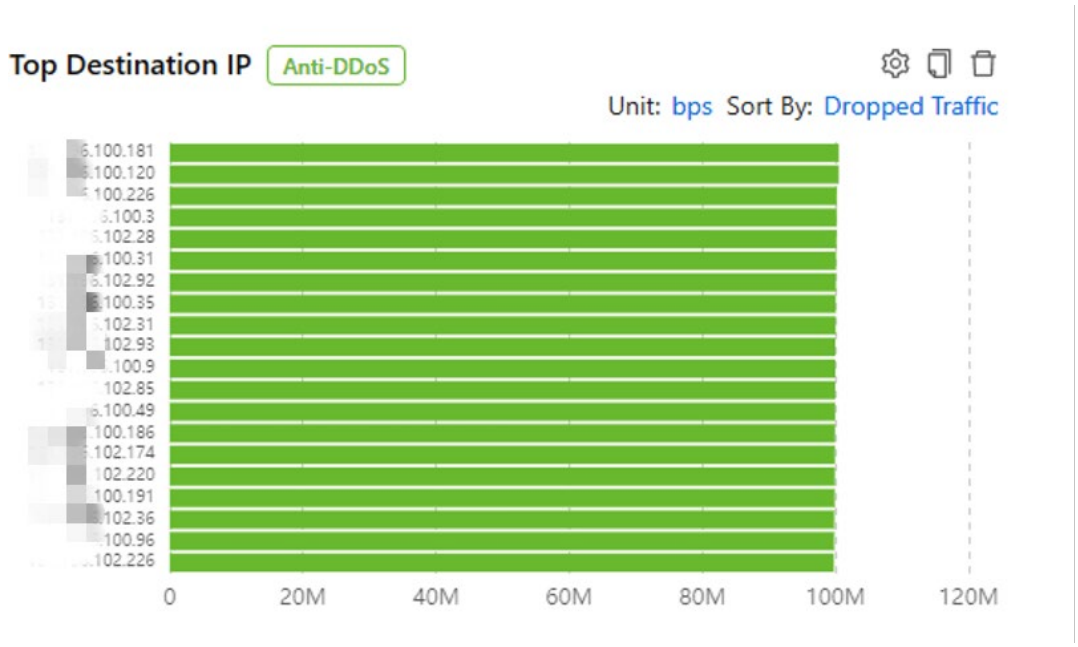
9.3 UDP-based carpet-bombing attack

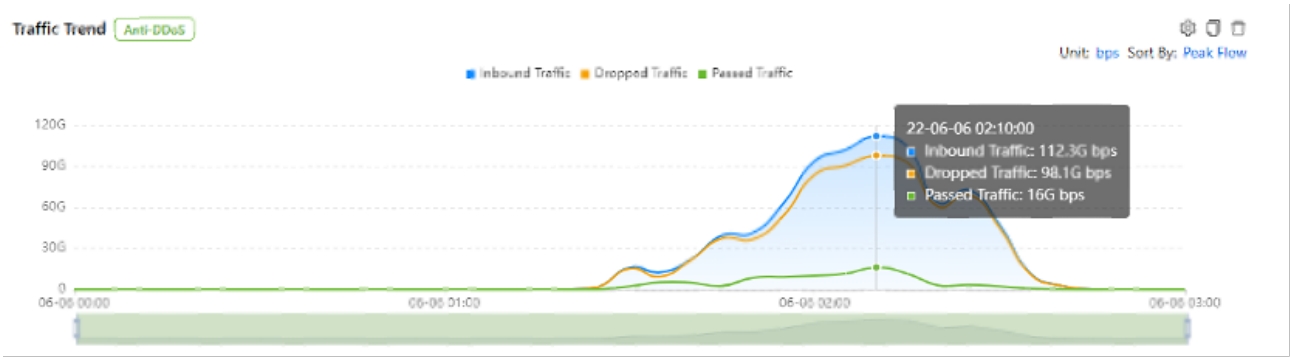
9.3.1 Overview

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.





© COPYRIGHT 2023, NSFOCUS. ALL RIGHTS RESERVED. SUMMARY OF DPS ATTACKS IN 2022

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.

© COPYRIGHT 2023, NSFOCUS. ALL RIGHTS RESERVED. SUMMARY OF DPS ATTACKS IN 2022