2022

Global DDoS Attack Landscape Report

NSFOCUS

2022 Global DDoS Attack Landscape

NSFOCUS

Key Findings

01

The number of DDoS attacks in 2022 increased by 273% compared to 2021. DDoS threats have maintained consistent growth over the past four years.

02

Attacks greater than 100 Gbps increased by more than 50% year on year, representing an attack over 100 Gbps every hour on average. The attack peak exceeded 1 Tbps in six months, and UDP-based attacks were the most common. About one-third of terabit attacks were reflective UDP attacks, while the rest were mainly non-reflective UDP attacks.

03

Southeast Asia was the attack hotspot. North America was the predominant source of application-layer DDoS attack traffic. Peru was hit hardest by application-layer DDoS attacks.

04

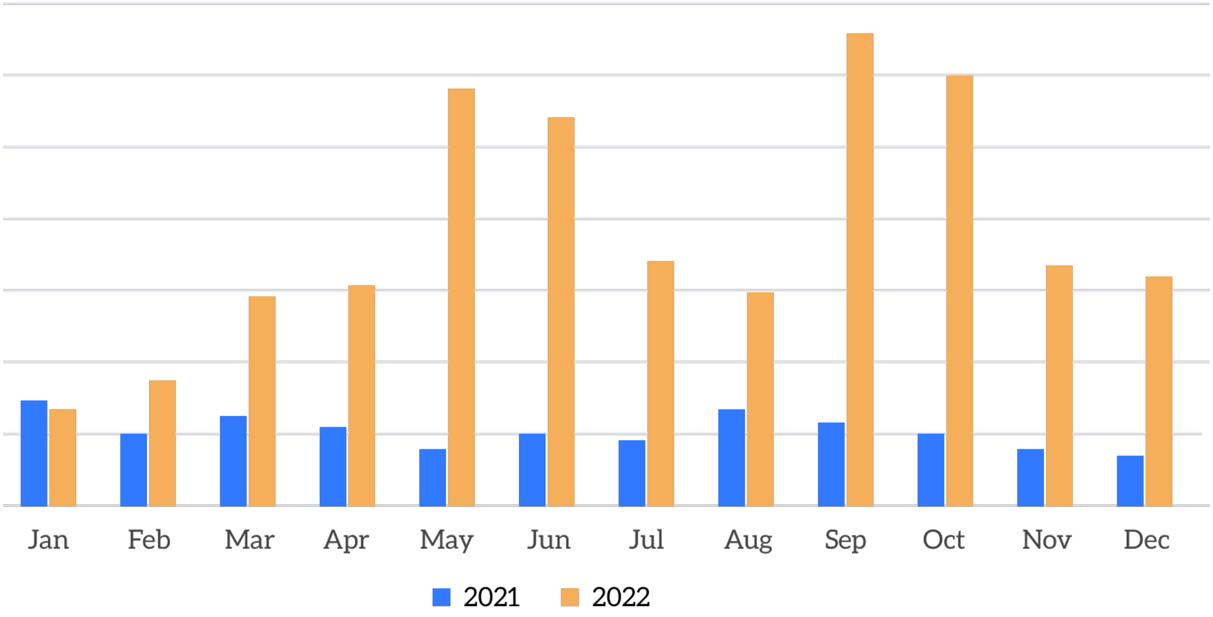
DDoS attacks against critical infrastructure were on the rise. Hacking gangsters have the ability to exploit critical vulnerabilities at any time to expand their botnet for DDoS attacks, which poses a great threat to critical infrastructure.

TABLE OF CONTENTS

1. Global DDoS Attack Trends

DDoS Attacks Increased Dramatically

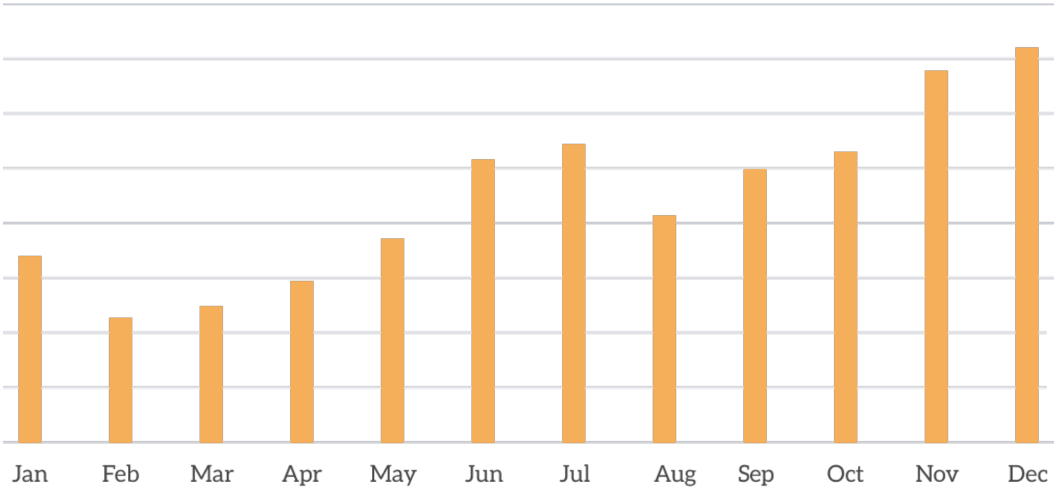
The data shows that DDoS attacks in 2022 increased by 273% compared to 2021. Except January, DDoS attacks in each month of 2022 increased significantly compared to 2021. May, September, and October saw the most DDoS attacks.



DDoS attack trends (2021 and 2022)

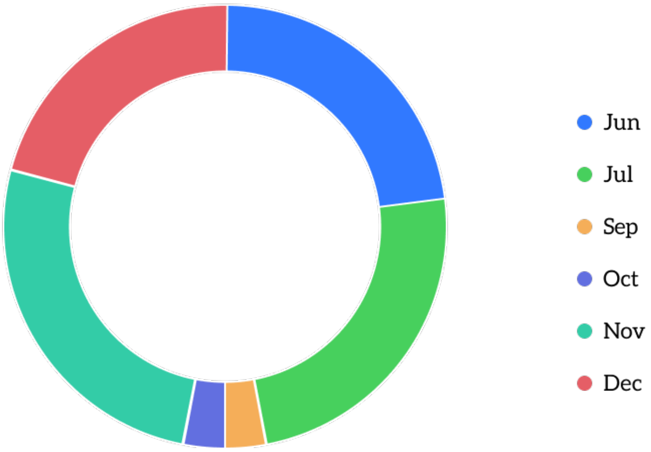
High-Volume DDoS Attacks Were on the Rise

In 2022, the number of terabit-level DDoS attacks was approximately 40, and the attack peak exceeded 1 Tbps in six months.

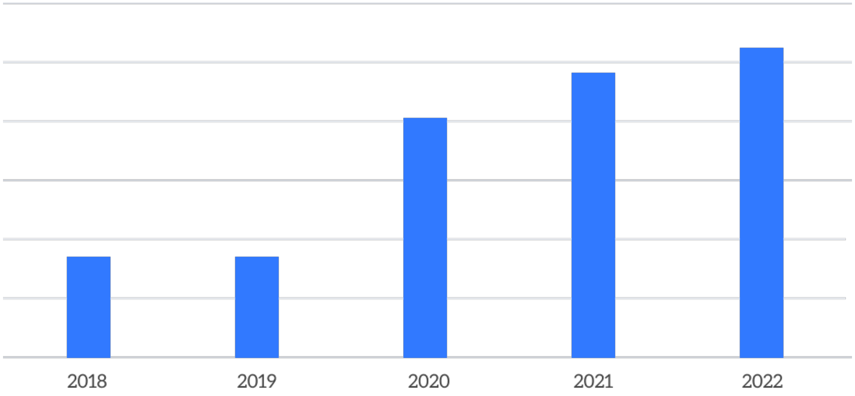


Distribution of peak DDoS attack traffic by month in 2022

Terabit-level attacks emerged most in June to July and November to December, accounting for 94% in 2022.



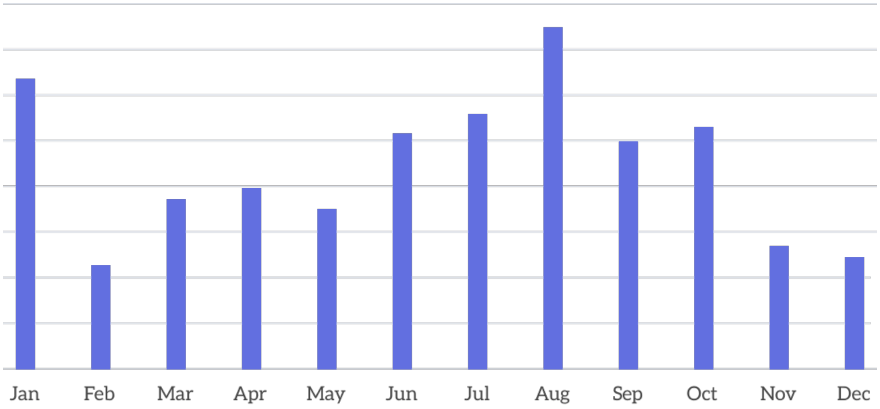
Distribution of terabit-level DDoS attack traffic by month in 2022



Trend of high-volume DDoS attack traffic larger than 100 Gbps

In 2022, the number of attacks greater than 100 Gbps hit a record high, with a year-on-year increase of more than 50%. On average, an attack exceeding 100 Gbps happened every hour.

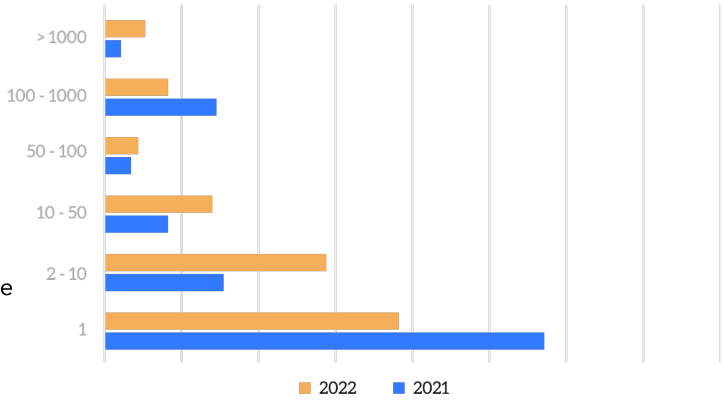
High-volume attacks larger than 100 Gbps continued to rise since February, and August recorded the peak, about three times the count in February.



Trend of high-volume DDoS attack traffic over 100 Gbps by month in 2022

DDoS Attack Targets Became More Specific and Attacks Were More Persistent Year over Year

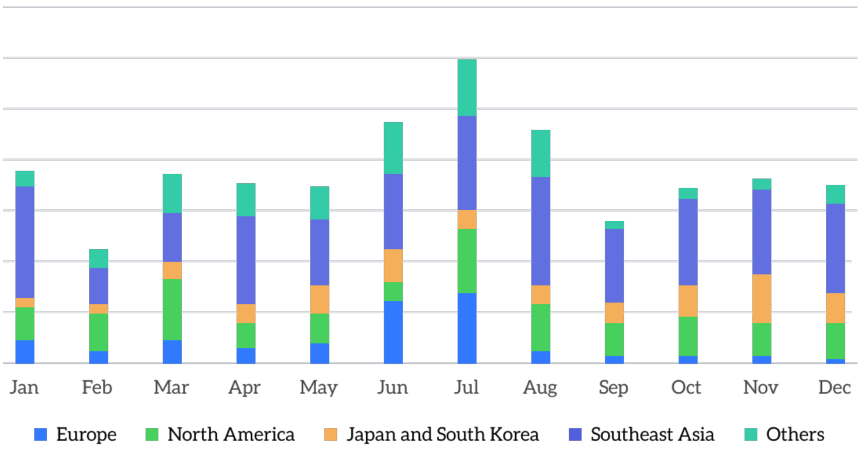
The analysis on the attacked frequency of targets reveals that the number of repeatedly attacked IP addresses in 2022 was significantly greater than that in 2021. DDoS attacks against a single target became increasingly persistent. 56.91% of victims experienced only one DDoS attack in 2021, whereas victims were more prone to multiple DDoS attacks once identified as the target in 2022. The increasing attack persistence undoubtedly puts a greater challenge to DDoS protection.



DDoS attack persistence distribution (2021 and 2022)

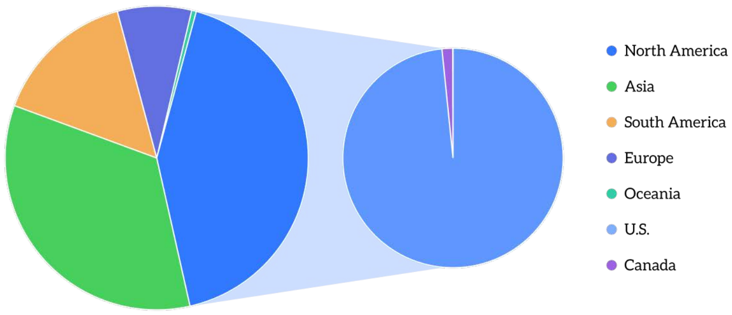
Southeast Asia Remained a Hotspot for Cyberattacks

With the rapid regional economic development and the rapid growth of the Internet industry as well as a huge number of connected young users, DDoS attacks in Southeast Asia increased significantly, accounting for more than 40% in 2022 and ranking first almost every month. Southeast Asia became a hotspot for DDoS attacks.



Distribution of regions mostly targeted by DDoS attacks in 2022

North America Was a Predominant Source of Application-layer DDoS Attack Traffic

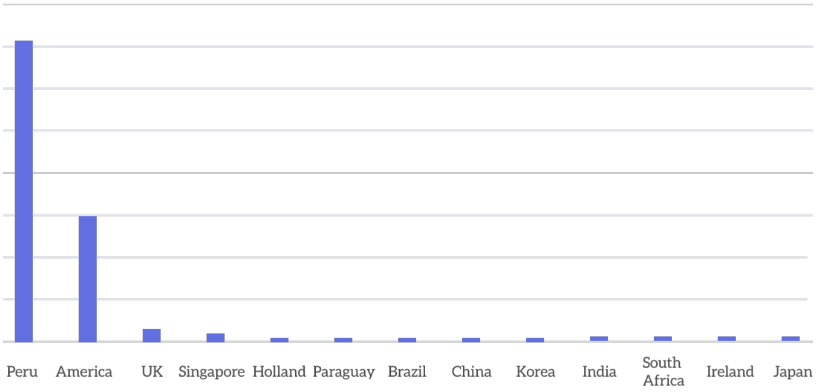


Distribution of attack sources for application-layer DDoS attacks

Different from network-layer DDoS attacks, application-layer DDoS attacks feature complete TCP connections and their attack source IPs cannot be forged. If huge numbers of application-layer attack source IPs have a high level of activity in a region, it indicates that botnets are active there. North America was the major source of application-layer DDoS attacks, with the United States contributing to 98.43%. It signals that the United States is an active botnet region at present.

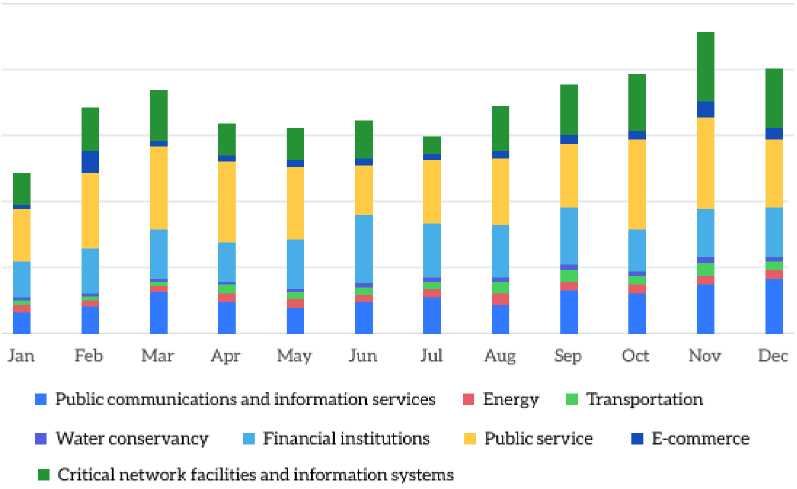
Peru Was Hit Hardest by Application-layer DDoS Attacks

In 2022, Peru was the most targeted country for application-layer DDoS attacks. As developed countries, the United States and the United Kingdom ranked second and third.



Target distribution of application-layer DDoS attacks by country

DDoS Attacks Increasingly Targeted Critical Infrastructure



Critical infrastructure targeted by DDoS attacks by month in 2022

In 2022, DDoS attacks against critical infrastructure increased, with the largest number registered in November.

The COVID-19 pandemic has caused the global economic downturn. Adversaries launching ransom DDoS attacks are turning to attack critical infrastructure, such as public communication and information services, finance, public services, e-government, and critical network facilities and information systems.

DDoS attackers attempt to exhaust the available resources of target networks, applications, or services, causing damage to critical infrastructure that plays a vital role in business continuity. Their high downtime costs mean that the ransom is more likely to be paid.

In recent years, DDoS botnets continue to exploit vulnerabilities to expand their reach. In 2022, the number of vulnerabilities exploited by botnets in the wild reached 135. New vulnerabilities are integrated within a few hours after disclosure. As a result, vulnerable hosts can be rapidly controlled and implanted with trojans before their vulnerabilities are fixed.

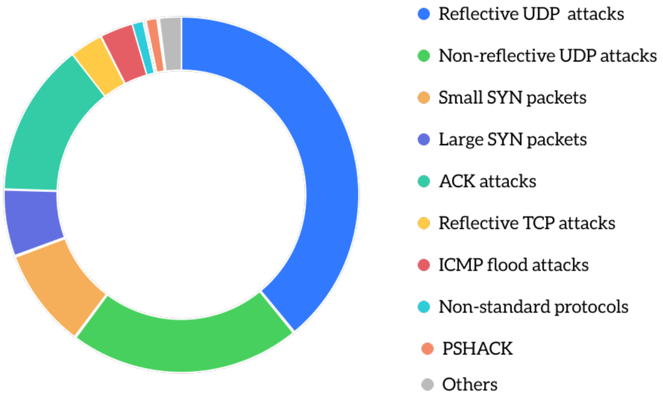
Mirai, as one of the most active botnets, was observed to carry 77 medium and high-risk vulnerabilities in 2022, such as Apache Log4j RCE vulnerability (CVE-2021-44228), F5 BIG-IP unauthorized RCE vulnerability (CVE-2022-1388), and Spring4Shell RCE vulnerability (CVE-2022-22965). Initially compromising devices by exploiting weak passwords, Mirai now evolves its tactics to exploit vulnerabilities for expanding its botnet. Mirai seeks every opportunity to infect more hosts to expand the control range.

We can conclude that hacking groups have the ability to employ critical vulnerabilities at any time to expand their botnet to large numbers of hosts for DDoS attacks, which poses a great threat to critical infrastructure.

2. Attack Vectors

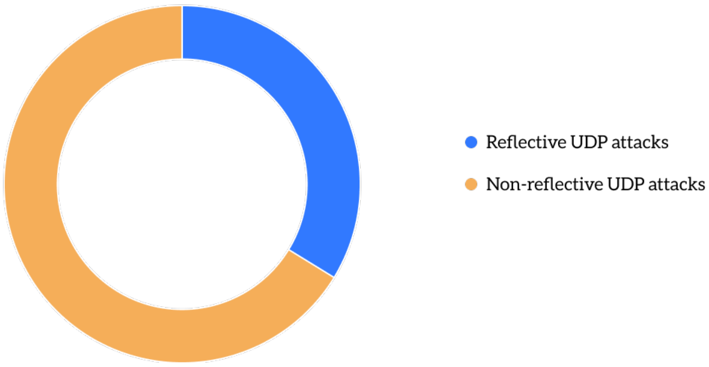
UDP-based Attacks Were Favored by Hackers

In terms of attack vectors, UDP-based attacks ranked first, accounting for about 60% of DDoS attacks. SYN flood attacks dropped to about 15%. As a popular attack method in the past two years, TCP reflection attacks represented 3%.



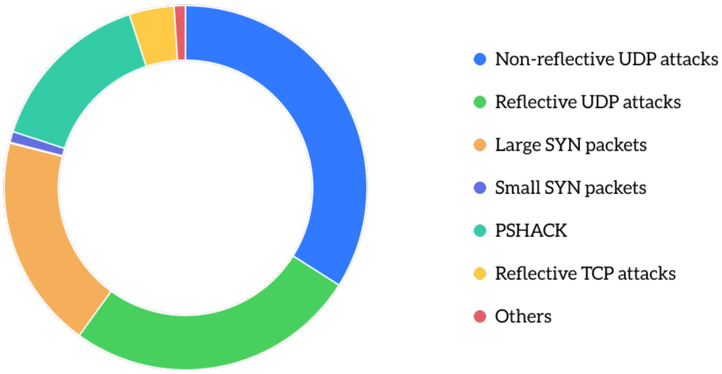
Distribution of DDoS attack vectors in 2022

All terabit attacks were UDP-based attacks. One third of them were reflective UDP attacks, and the remaining two thirds were non-reflective large UDP packet attacks. It signals that DDoS attackers have controlled extremely abundant attack resources and they can launch terabit-class attacks without needing UDP reflection to amplify traffic.



Distribution of vectors for terabit-class DDoS attacks in 2022

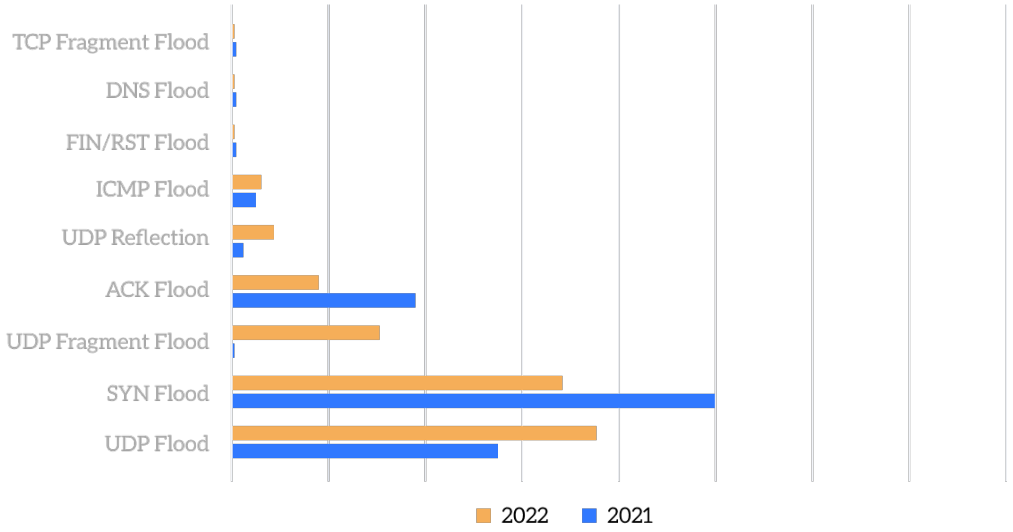
UDP attacks still made up the lion's share of attacks greater than 100 Gbps, representing nearly 60%. The percentage of large UDP packet attacks exceeded that of reflective UDP attacks. Large SYN packet attacks accounted for nearly 20%, ranking third. In addition, PSHACK attacks made up a considerable proportion.



Distribution of vectors for DDoS attacks larger than 100 Gbps in 2022

UDP Fragment Flood Stood Out

In 2022, UDP flood attacks, SYN flood attacks, and UDP fragment flood attacks were top 3 network-layer DDoS attacks. Compared to 2021, UDP flood attacks increased by 8.01%, and SYN flood attacks decreased by 15.08%. It is noteworthy that UDP fragment flood attacks increased significantly. During a UDP fragment DDoS attack, attackers transmit forged UDP packets which seem larger than the maximum transmission unit, but only part of which are sent actually. These fragments cannot be reassembled by the server. When large numbers of fragments hit the targeted server, server resources are sapped, ultimately making the server inaccessible.



Distribution of attack vectors for network-layer DDoS attacks in 2021 and 2022

Cloud9 Malicious Add-on, a New Attack Tool, Emerged for Remote Control

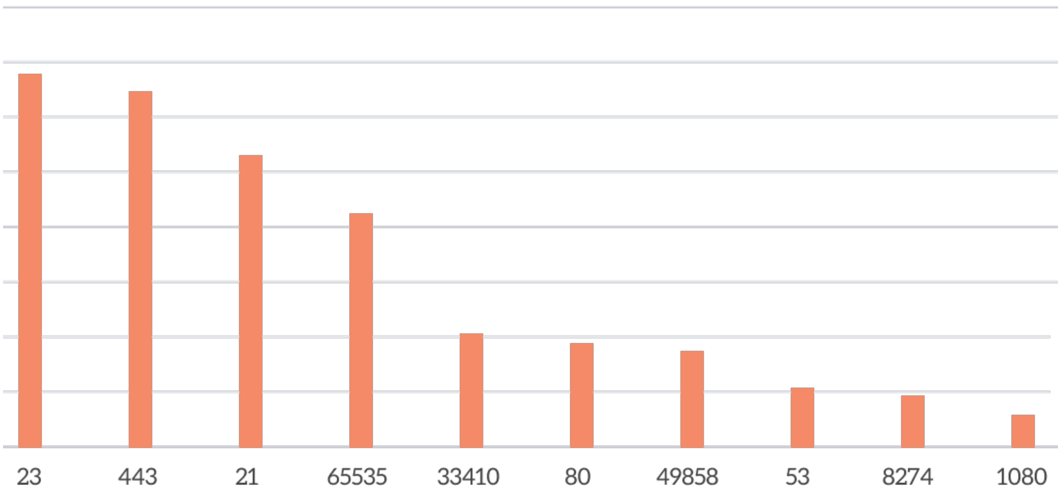
Security community researchers discovered a new browser botnet named Cloud9, which uses malicious extensions to steal online accounts, record keystrokes, inject ads and malicious JavaScript code, and enroll victim's browsers in DDoS attacks. Cloud9 is actually a browser's remote access trojan (RAT), which allows attackers to execute commands remotely. Cloud9 is not available in official browser web stores, but is spread through such channels as websites promoting fake player updates.

Cloud9 consists of three JavaScript files for collecting system information, mining cryptocurrencies, performing DDoS attacks, and injecting scripts that run browser exploits. The malware can use hosts to perform application-layer DDoS attacks via HTTP POST requests to the target region.

Attackers Focused on Remote Login and Web Application Services

Researchers examined victim ports and found that a majority of DDoS attacked services were telnet remote login service via TCP port 23 and HTTPS service via TCP port 443.

As the pandemic in 2022 made working from home a new normal, the remote login service via TCP port 23 and file transfer service via FTP port 21 became the most frequent targets of DDoS attacks. In addition, websites with high security requirements, like online banking, shopping, and finance websites, generally adopt the HTTPS service. If such websites come under DDoS attacks, huge economic loss will be incurred.

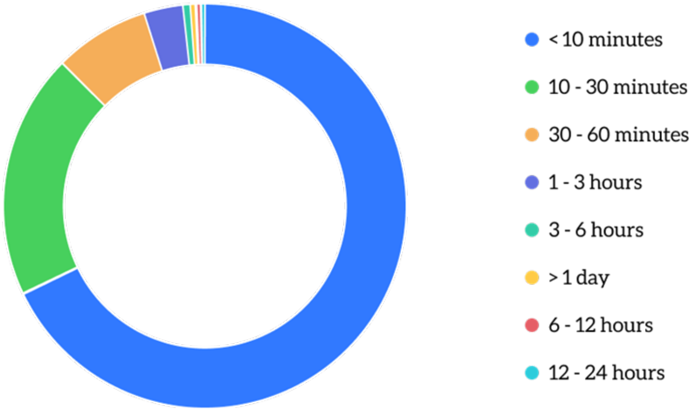


Number of attack events on affected ports in 2022

The "Quick Spike" Attack Tactic Continued to Take Dominance

Nearly 70% of global DDoS attacks were shorter than 10 minutes, about 20% lasted 10 to 30 minutes, and the rest exceeded 30 minutes. Currently, "quick spike" attacks prevail.

This type of DDoS attack sends a massive amount of attack traffic to bombard the target in a short time, which gives DDoS protection personnel relying on manual security analysis a hard time to defend against. When it happens, the DDoS protection personnel cannot deploy protection in time. As is often the case, they make an after-action review and deploy protection rules to filter these attack signatures for future alerting and mitigation. Once this type of short-duration DDoS attacks is successful, it may take hours or even days to restore application service, requiring much labor effort.

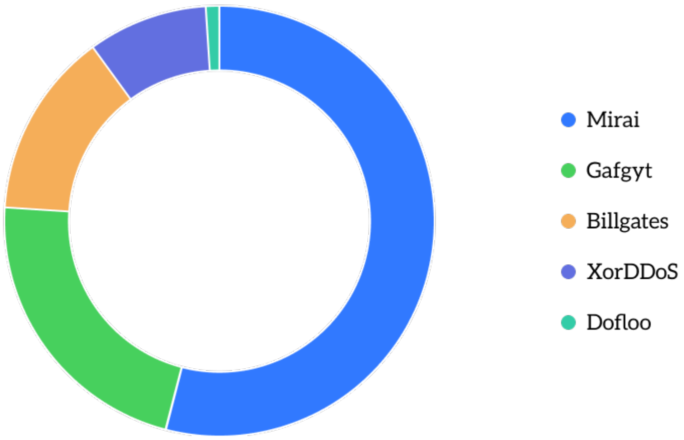


DDoS attack duration in 2022

3. Botnet Analysis

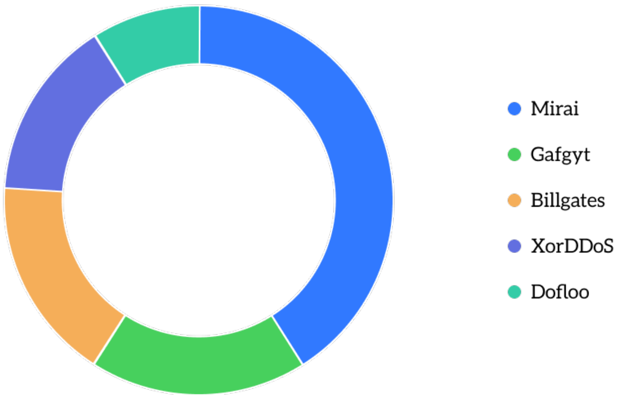
Distribution of Botnet Attack Activities

Mirai was the most active attack botnet in 2022, contributing to 54% of botnet activities. The Gafgyt and BillGates botnets ranked second and third respectively. However, the XorDDoS botnet that launched a large number of SYN packet attacks in the past two years kept a low profile, contributing to less than 10%.



Distribution of active botnets in 2022

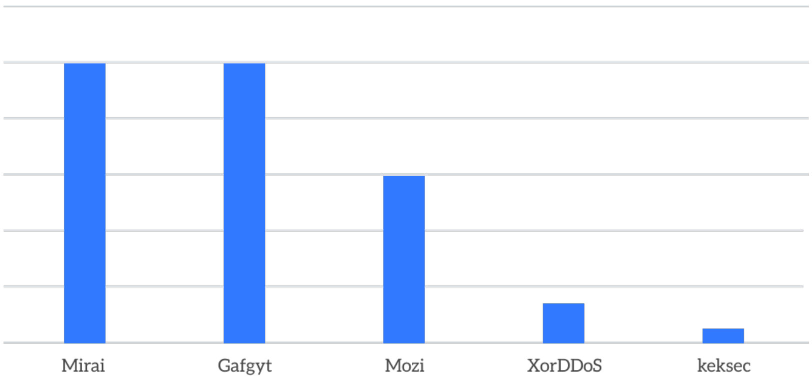
Bot Distribution



Number of bots in active botnets in 2022

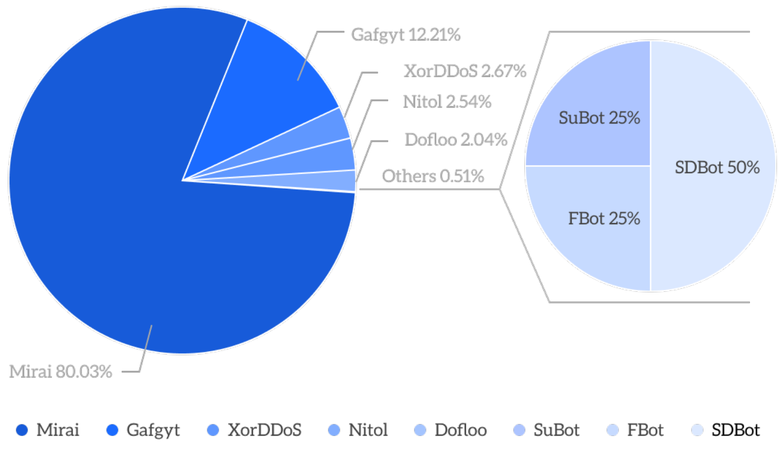
Mirai was still the king of botnets and had the largest number of bots, accounting for more than 40%. Gafgyt, BillGates, and XorDDoS had a relatively close number of bots, accounting for less than 20% respectively.

The statistics show that the rate of exploiting top 20 Linux/IoT critical vulnerabilities was positively related to the level of activity and the scale of botnets in 2022. Mirai and Gafgyt exploited nearly 100% of the top 20 vulnerabilities this year, and Mozi, a relatively new player, exploited close to 60%, whereas XorDDoS experienced a decline in these vulnerability exploits. Keksec, an emerging hacker group, exploited less than 3% of the top 20 vulnerabilities, and however, it was gradually expanding the attack range in its iterations.



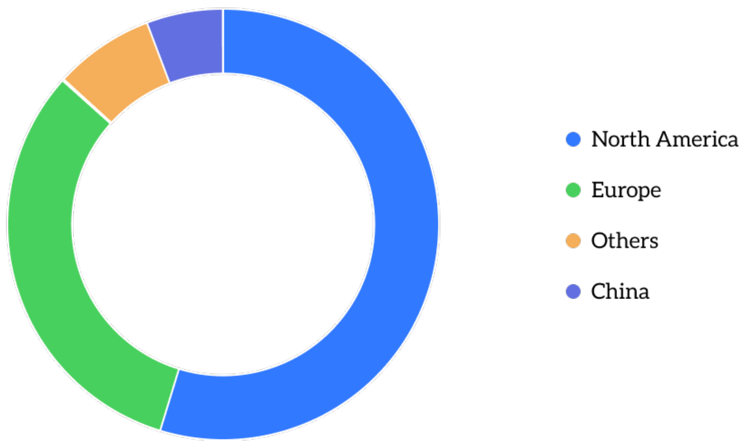
Exploitation of top 20 critical Linux/IoT vulnerabilities

Botnet Command-and-Control Server Analysis

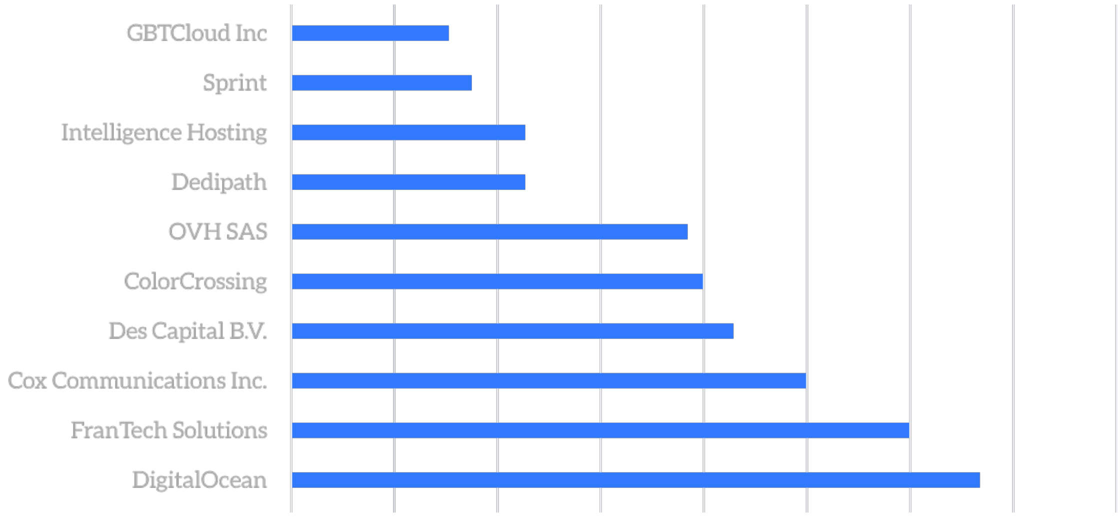


Percentage of C& C servers of active botnets

Mirai had the largest number of C&C server terminals, accounting for nearly 80%. The botnet's master C&C servers were mainly distributed in North America and Europe. DigitalOcean and FranTech Solution were the cloud service providers that hosted the most botnet C&C servers.



Distribution of C& C servers by country in 2022

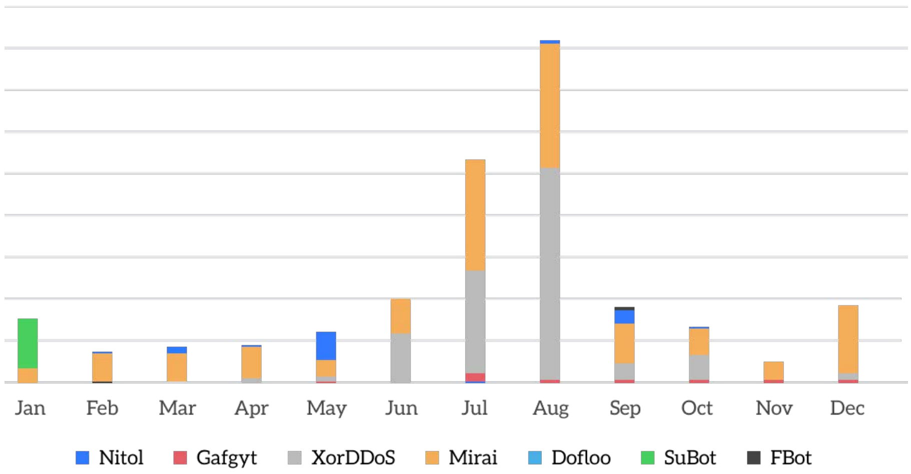


Cloud server vendors and Telcos affected with most C& C servers

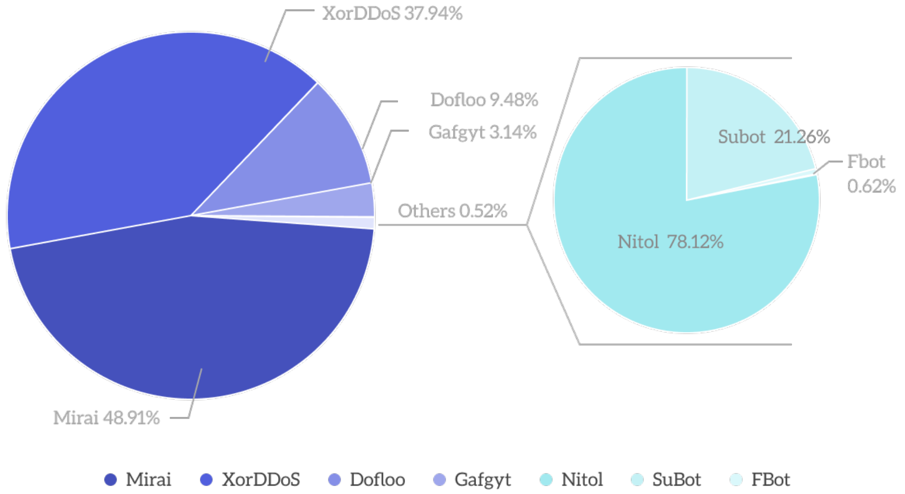
Analysis of Botnet Attack Instructions

Mirai launched nearly half of the DDoS attacks and reached the peak in July and August. The total number of attack instructions of XorDDoS exceeded that of the traditional family Gafgyt. XorDDoS contributed to nearly 40% attack activities in 2022.

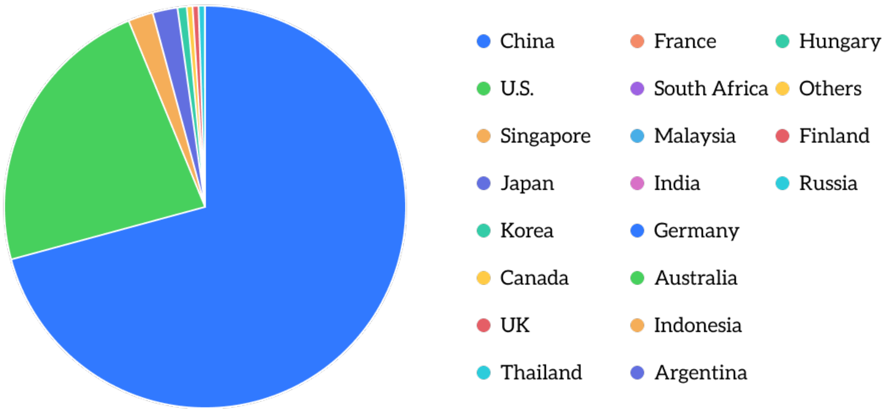
The XorDDoS botnet family was first observed at the end of September 2014 to establish a botnet capable of launching DDoS attacks. XorDDoS prefers brute-forcing the SSH weak password of the target host, then intrudes the target, and then executes the Shell script to install the XorDDoS malicious family and malicious RootKit for infecting hosts. XorDDoS mainly targeted China, the United States, and other countries and regions.



Distribution of DDoS attack instructions by month in 2022

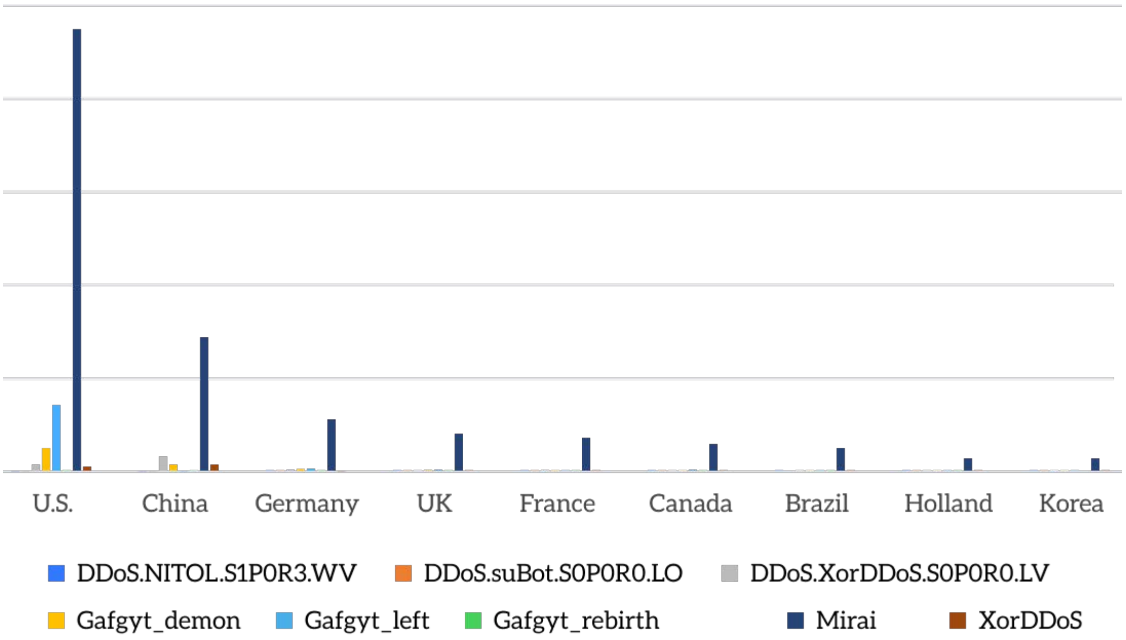


Percentage of DDoS attack instructions by active botnets



Distribution of Botnet targets by country in 2022

The United States Became the Top Target for Botnet DDoS Attacks

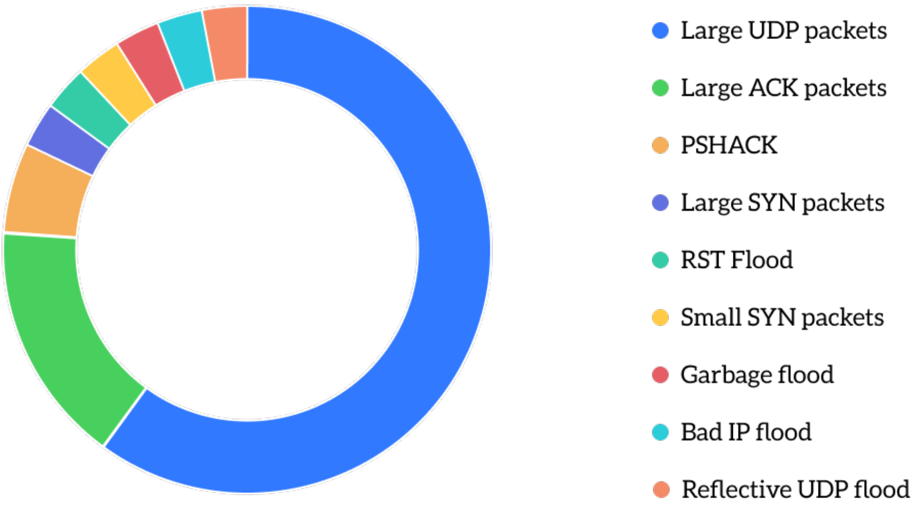


Botnet attacks generally aim for economic benefits, and the level of activity is closely related to the economic level in the region. As the world's largest economy, the United States becomes the most frequent target of botnet attacks. In 2022, the most active Mirai botnet and well-known botnets like Gafgyt and XorDDoS all targeted the United States most. China and Germany also suffered a large number of DDoS attacks launched by Mirai.

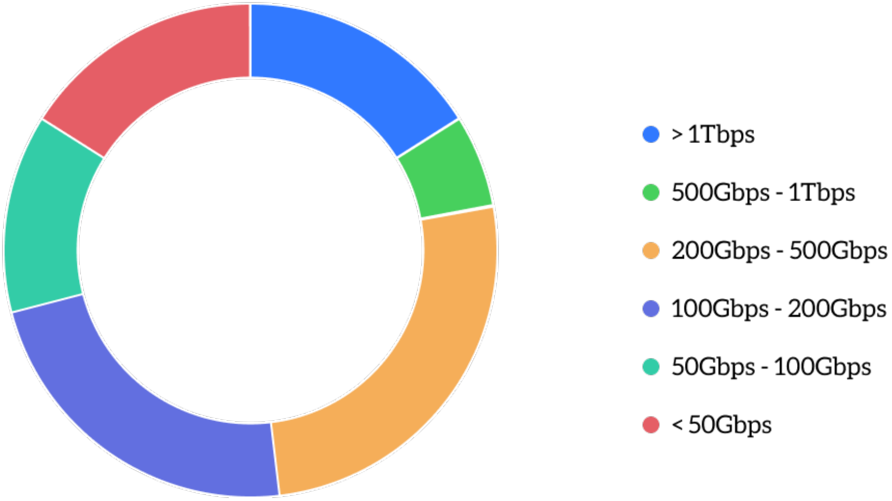
4. Defense and Protection Confrontation Cases

Case 1: Protecting a Customer Against a Multi-Vector Volumetric DDoS Attack

On December 2, 2022, a customer was under a high-volume DDoS attack, which was a UDP flood attack and whose attack peak reached 1.45 Tbps. In the following week, more than 9 attack methods were employed and more than 40 attacks were launched against the customer. A majority of attacks used large UDP packets, and the rest mainly used large ACK packets and PSHACK packets. 70% of attacks exceeded 100 Gbps, and nearly 50% of attacks were greater than 500 Gbps.



Distribution of attack vectors



Distribution of peak attack traffic

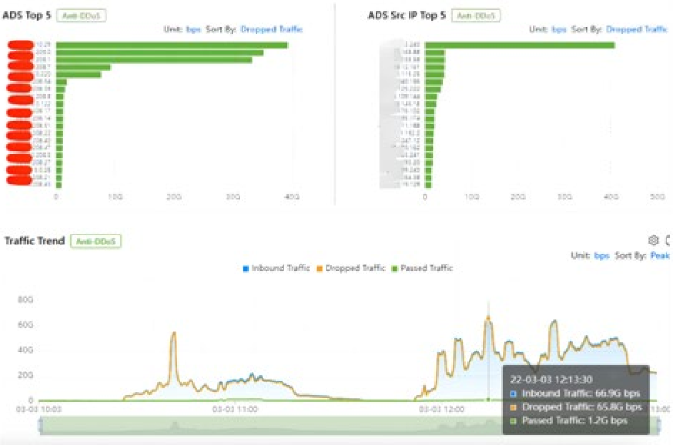
The analysis of the attack source shows that one variant of Mirai participated in the attack and the two C&C IP addresses captured were 157.XXX.102.XXX (located in Bangalore, India) and 138.XXX.65.XXX (located in Frankfurt, Germany) respectively. Attackers used more than 40,000 bots worldwide to launch the attack.

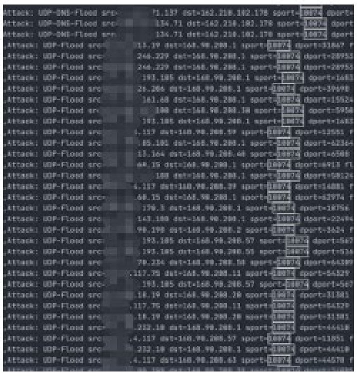
Case 2: Reflection/Amplification Attack Exploiting CVE-2022-26143

In early March 2022, a customer in Latin America experienced a UDP flood attack whose attack traffic peaked at 66.9 Gbps. The attack used a fixed source port 10074. The in-depth analysis shows that it was a reflection and amplification attack launched by hackers exploiting the TP-240 driver vulnerability
(CVE-2022-26143).

This vulnerability can lead to the abuse of a public command of the TP-240 driver service, which is designed to perform stress testing on its clients for debugging and performance testing. Attackers can use specially crafted commands to cause the TP-240 driver service to send larger informative status update packets, thus significantly improving the amplification ratio. In theory, the amplification factor can be 4,294,967,294.

After confirmation, NSFOCUS adjusted the UDP protection policy of the protection group on ADS, and limited the rate of UDP traffic on port 10074 to ensure the customer's business continuity.





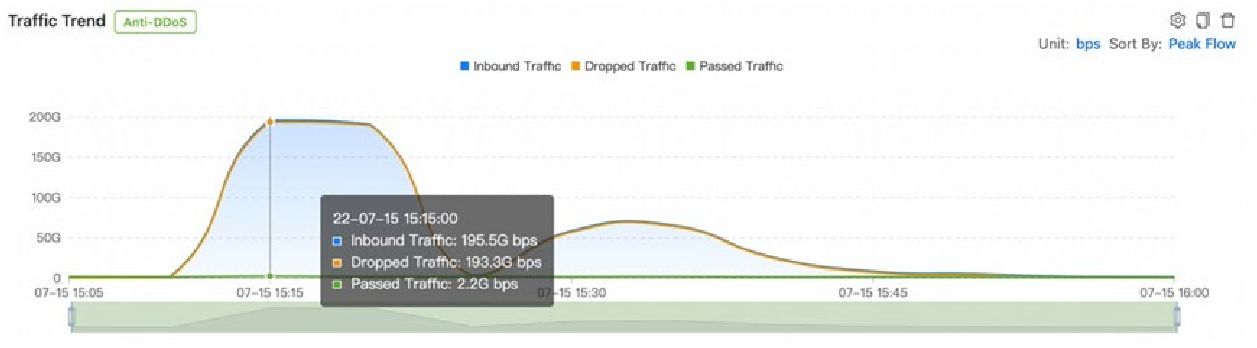
```
Attack: UDP-DNS-Flood src=[redacted]71.137 dst=162.218.102.178 sport=10074 dport=
Attack: UDP-DNS-Flood src=[redacted]134.71 dst=162.218.102.178 sport=10074 dport
Attack: UDP-DNS-Flood src=[redacted]134.71 dst=162.218.102.178 sport=10074 dport
,Attack: UDP-Flood src[redacted]13.19 dst=168.90.208.1 sport=10074 dport=31867 f
,Attack: UDP-Flood src[redacted]246.229 dst=168.90.208.1 sport=10074 dport=28953
,Attack: UDP-Flood src[redacted]246.229 dst=168.90.208.1 sport=10074 dport=28953
,Attack: UDP-Flood src[redacted]193.105 dst=168.90.208.1 sport=10074 dport=1683
,Attack: UDP-Flood src[redacted]26.206 dst=168.90.208.1 sport=10074 dport=39698
,Attack: UDP-Flood src[redacted]161.68 dst=168.90.208.1 sport=10074 dport=15524
,Attack: UDP-Flood src[redacted]100 dst=168.90.208.30 sport=10074 dport=5950
,Attack: UDP-Flood src[redacted]193.105 dst=168.90.208.1 sport=10074 dport=1683
,Attack: UDP-Flood src[redacted].117 dst=168.90.208.59 sport=10074 dport=12551 f
,Attack: UDP-Flood src[redacted].85.101 dst=168.90.208.1 sport=10074 dport=62364
,Attack: UDP-Flood src[redacted]13.164 dst=168.90.208.40 sport=10074 dport=6508
,Attack: UDP-Flood src[redacted]60.15 dst=168.90.208.1 sport=10074 dport=6913 fl
,Attack: UDP-Flood src[redacted]100 dst=168.90.208.1 sport=10074 dport=50124
,Attack: UDP-Flood src[redacted].117 dst=168.90.208.39 sport=10074 dport=14081 f
,Attack: UDP-Flood src=[redacted].60.15 dst=168.90.208.1 sport=10074 dport=62974 f
,Attack: UDP-Flood src[redacted]170.3 dst=168.90.208.1 sport=10074 dport=18756
,Attack: UDP-Flood src[redacted]143.180 dst=168.90.208.1 sport=10074 dport=22494
,Attack: UDP-Flood src[redacted]90.198 dst=168.90.208.2 sport=10074 dport=3624 f
,Attack: UDP-Flood src[redacted]193.105 dst=168.90.208.57 sport=10074 dport=567
,Attack: UDP-Flood src=[redacted]193.105 dst=168.90.208.55 sport=10074 dport=534
,Attack: UDP-Flood src[redacted]70.234 dst=168.90.208.50 sport=10074 dport=64389
,Attack: UDP-Flood src=[redacted].117.75 dst=168.90.208.11 sport=10074 dport=54329
,Attack: UDP-Flood src=[redacted]193.105 dst=168.90.208.57 sport=10074 dport=567
,Attack: UDP-Flood src[redacted].18.19 dst=168.90.208.20 sport=10074 dport=31381
,Attack: UDP-Flood src[redacted].117.75 dst=168.90.208.11 sport=10074 dport=54329
,Attack: UDP-Flood src[redacted].18.19 dst=168.90.208.20 sport=10074 dport=31381
,Attack: UDP-Flood src=[redacted].232.18 dst=168.90.208.1 sport=10074 dport=44410
,Attack: UDP-Flood src[redacted].4.117 dst=168.90.208.57 sport=10074 dport=11851 f
,Attack: UDP-Flood src[redacted].232.18 dst=168.90.208.1 sport=10074 dport=44410
,Attack: UDP-Flood src[redacted].4.117 dst=168.90.208.63 sport=10074 dport=44570 f
```

Case 3: Large-Scale UDP Flood DDoS Attacks

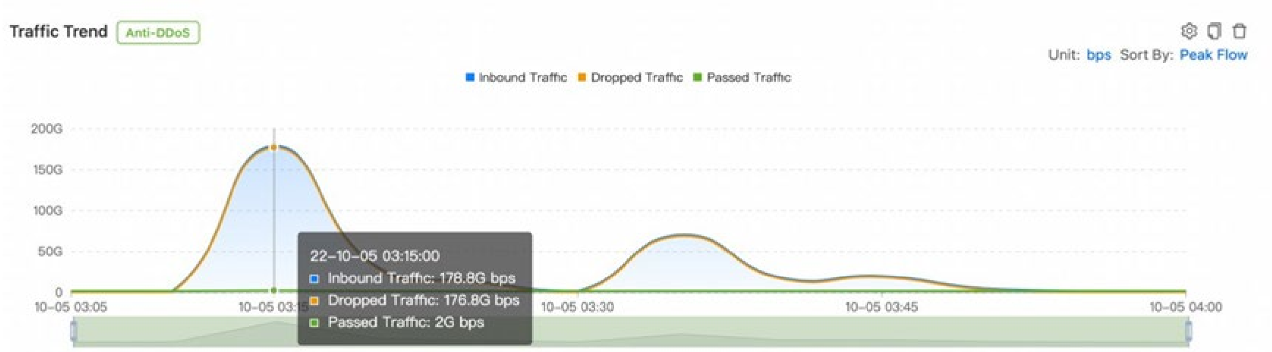
In late 2022, an international customer in Latin America was under three large-scale UDP flood DDoS attacks that peaked at 225.5 Gbps. After NSFOCUS cleaned the attack traffic, only 3.7-Gbps traffic was re-injected to the customer's network, indicating an attack mitigation efficiency of 98.8%.

When the customer was attacked, NSFOCUS's security team rapidly offered emergency response by communicating with the customer and conducting packet capture and analysis. The attacked IP address was found to provide an online gaming service via UDP ports 27030 and 27055. The attacker sent a single query request to the server from a random source with a complete protocol stack. The requests from these random sources had the same payload and the messages were normal.

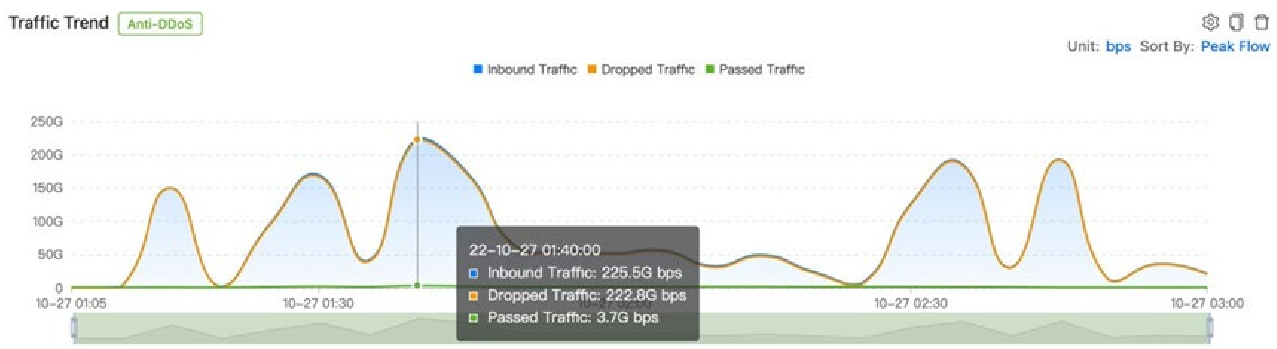
For the UDP flood attack on July 15, the mitigation efficiency was 98.87%.

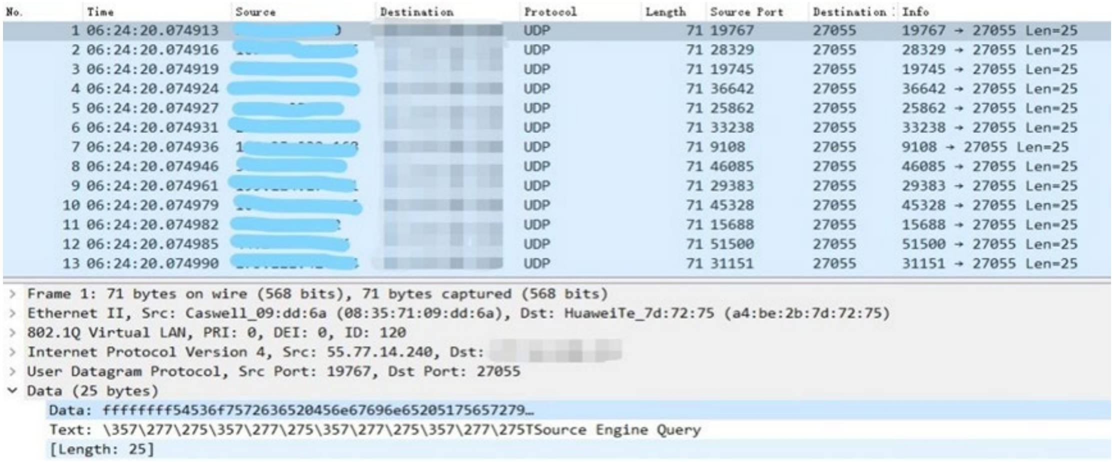


For the UDP flood attack on October 5, the mitigation efficiency was 98.88%.



For the UDP flood attack on October 27, the mitigation efficiency was 98.8%.

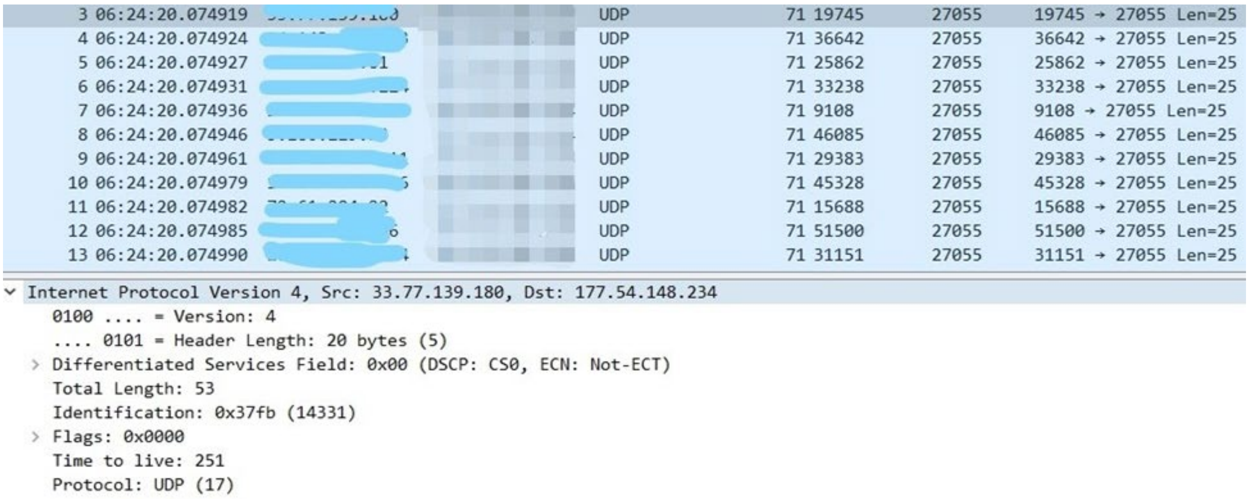




No.	Time	Source	Destination	Protocol	Length	Source Port	Destination	Info
1	06:24:20.074913	[redacted]	[redacted]	UDP	71	19767	27055	19767 → 27055 Len=25
2	06:24:20.074916	[redacted]	[redacted]	UDP	71	28329	27055	28329 → 27055 Len=25
3	06:24:20.074919	[redacted]	[redacted]	UDP	71	19745	27055	19745 → 27055 Len=25
4	06:24:20.074924	[redacted]	[redacted]	UDP	71	36642	27055	36642 → 27055 Len=25
5	06:24:20.074927	[redacted]	[redacted]	UDP	71	25862	27055	25862 → 27055 Len=25
6	06:24:20.074931	[redacted]	[redacted]	UDP	71	33238	27055	33238 → 27055 Len=25
7	06:24:20.074936	[redacted]	[redacted]	UDP	71	9108	27055	9108 → 27055 Len=25
8	06:24:20.074946	[redacted]	[redacted]	UDP	71	46085	27055	46085 → 27055 Len=25
9	06:24:20.074961	[redacted]	[redacted]	UDP	71	29383	27055	29383 → 27055 Len=25
10	06:24:20.074979	[redacted]	[redacted]	UDP	71	45328	27055	45328 → 27055 Len=25
11	06:24:20.074982	[redacted]	[redacted]	UDP	71	15688	27055	15688 → 27055 Len=25
12	06:24:20.074985	[redacted]	[redacted]	UDP	71	51500	27055	51500 → 27055 Len=25
13	06:24:20.074990	[redacted]	[redacted]	UDP	71	31151	27055	31151 → 27055 Len=25

```
> Frame 1: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)
> Ethernet II, Src: Caswell_09:dd:6a (08:35:71:09:dd:6a), Dst: HuaweiTe_7d:72:75 (a4:be:2b:7d:72:75)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 120
> Internet Protocol Version 4, Src: 55.77.14.240, Dst: [redacted]
> User Datagram Protocol, Src Port: 19767, Dst Port: 27055
v Data (25 bytes)
    Data: ffffffff54536f7572636520456e67696e65205175657279…
    Text: \357\277\275\357\277\275\357\277\275\357\277\275TSource Engine Query
    [Length: 25]
```

It was a small UDP packet attack in which the attacker used a random source. If the traditional rate limit was adopted, the customer's legitimate business traffic would be affected. After a closer look, NSFOCUS found more detailed attack signatures to block the attack source, without affecting the availability of customer business. A further analysis shows that the TTL of all UDP attack packets was 251, whereas the default TTL of Windows or MacOS operating systems is 128 or 64. NSFOCUS concluded that the attack packet was crafted by an attack tool. Based on these attack signatures, NSFOCUS immediately adjusted the protection policy for the customer, achieving a high filtering ratio across the attack lifecycle and effectively ensuring normal business operations.



```
 3 06:24:20.074919 [redacted] [redacted] UDP  71 19745  27055  19745 → 27055 Len=25
 4 06:24:20.074924 [redacted] [redacted] UDP  71 36642  27055  36642 → 27055 Len=25
 5 06:24:20.074927 [redacted] [redacted] UDP  71 25862  27055  25862 → 27055 Len=25
 6 06:24:20.074931 [redacted] [redacted] UDP  71 33238  27055  33238 → 27055 Len=25
 7 06:24:20.074936 [redacted] [redacted] UDP  71 9108   27055  9108 → 27055 Len=25
 8 06:24:20.074946 [redacted] [redacted] UDP  71 46085  27055  46085 → 27055 Len=25
 9 06:24:20.074961 [redacted] [redacted] UDP  71 29383  27055  29383 → 27055 Len=25
10 06:24:20.074979 [redacted] [redacted] UDP  71 45328  27055  45328 → 27055 Len=25
11 06:24:20.074982 [redacted] [redacted] UDP  71 15688  27055  15688 → 27055 Len=25
12 06:24:20.074985 [redacted] [redacted] UDP  71 51500  27055  51500 → 27055 Len=25
13 06:24:20.074990 [redacted] [redacted] UDP  71 31151  27055  31151 → 27055 Len=25

v Internet Protocol Version 4, Src: 33.77.139.180, Dst: 177.54.148.234
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 53
    Identification: 0x37fb (14331)
  > Flags: 0x0000
    Time to live: 251
    Protocol: UDP (17)
```

5. Mitigation Challenges and Recommendations

Challenge 1

The terabit-level DDoS attack has become a real threat. It impairs attacked services and congests networks of operators, further affecting other services of the equipment room.

Recommendation

As construction of an equipment room with super-large bandwidth will lead to a higher cost and lower bandwidth utilization for organizations, they should turn to cloud computing vendors with massive protection bandwidth to defend against terabit-level DDoS attacks, or leverage the cloud vendor's end-to-end integrated protection capabilities to protect against attacks.

Challenge 2

Hacking groups constantly evolve. Their attack capabilities are changing and improving every day, and attack methods are unpredictable. As ordinary organizations have limited security protection staff and resources, it is hard for them to learn about the latest attack situation and defend against attacks. They stay in a passive position when confronting with highly skilled hacker groups.

Recommendation

With professional security protection experts and massive attack and defense scenarios of customers, cloud computing vendors should invest more in security protection to track the latest attack and defense situation and constantly iterate protection strategies, offering comprehensive security capabilities to protect customers against threats.

6. About NSFOCUS Cloud DPS

NSFOCUS's Anti-DDoS devices have the largest market share in China and an industry-leading position in the international market.

These Anti-DDoS devices are augmented by NSFOCUS's unique threat intelligence from sources in China and outside. NSFOCUS has established eight global cloud scrubbing centers, covering regions that are targeted by most DDoS attacks, such as Asia Pacific, North America, Latin America, and Europe.

By using the Anycast technology, NSFOCUS is capable of combining near-source traffic scrubbing with service nodes across the globe. The terabit-class scrubbing capacity provides customers with unlimited protection. NSFOCUS also has a global backbone service network that provides support for customers through the nearest service node with the lowest latency and maximum stability.

NSFOCUS Cloud DPS Service provides 24/7 service in multiple languages to assist customers with security management and emergency response against attacks.

NSFOCUS

SECURITY MADE SMART & SIMPLE

www.nsfocusglobal.com