NSFOCUS Tencent

2021 Global DDoS Attack Landscape

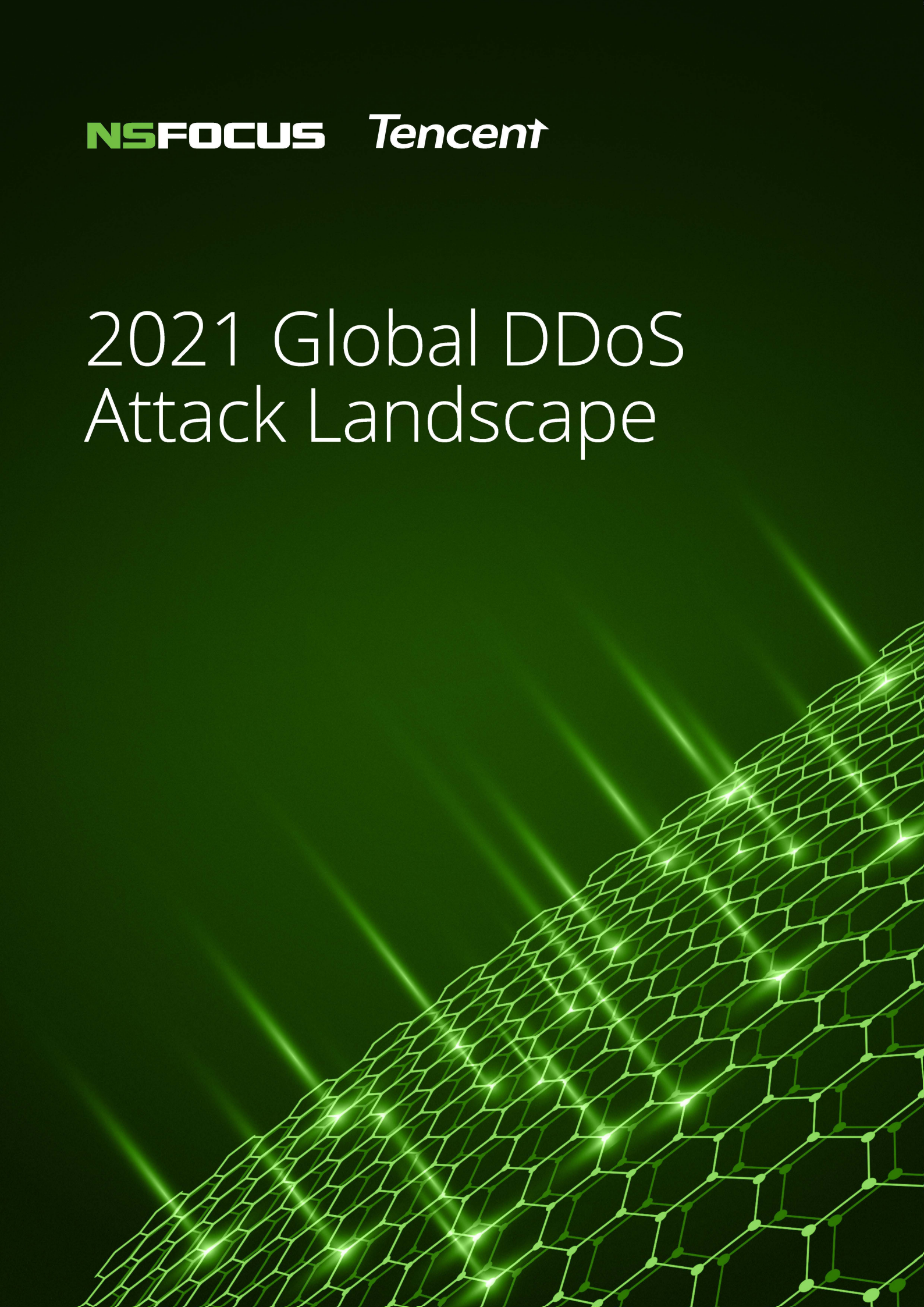


Table of Contents

Key Findings

01

DDoS attacks are gaining momentum in recent years, as outsized and diversified attacks are raging through the cyberworld.

02

DDoS attack gangs have been propagating DDoS botnets and expanding the range of reflection attacks.

03

Botnets have become a main tool for carpet-bombing DDoS attacks.

04

DDoS threats may become the preferred extortion method of cybercriminal gangs.

05

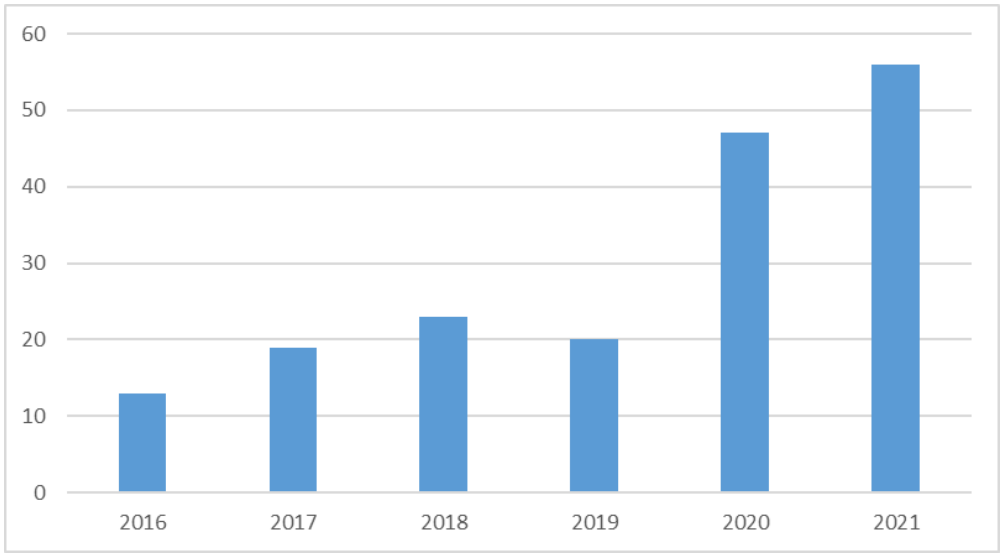
The main victim industries are beginning to diversify, but the gaming industry still tops the target list of attackers.

(* Unless otherwise specified, the data in this report is provided by NSFOCUS BotHunter and Tencent Cloud T-Sec DDoS Protection)

Global DDoS Attack Trends

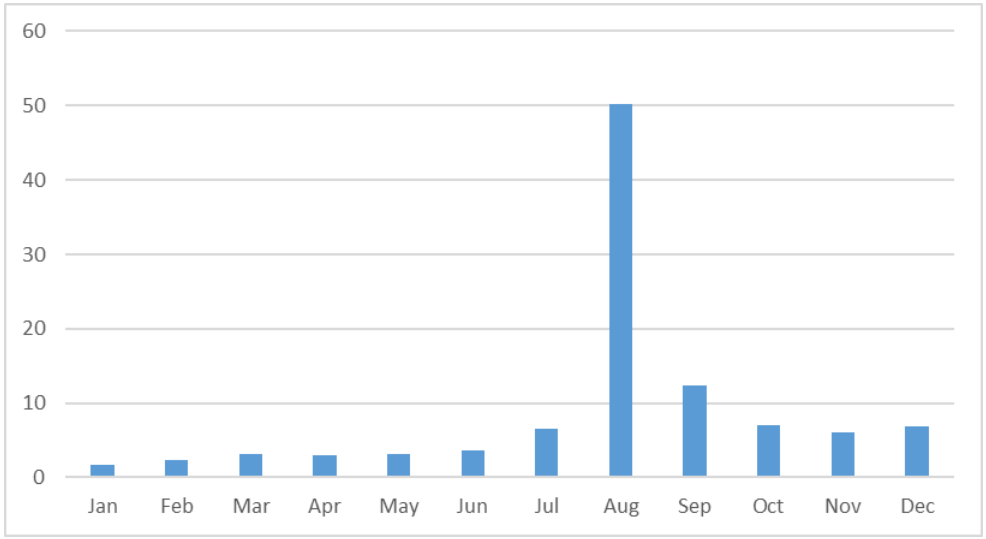
Since the first terabit-class attack hurled five years ago, the number of DDoS attacks has been surging for two consecutive years.

As the COVID-19 pandemic continues to wreak havoc on travel, social gathering, business trip, sports, retail, and other traditional offline activities, online business, such as live streaming, social media, gaming, video entertainment, and telecommuting takes up more hours of our lives. In the booming world of Internet-powered business, DDoS attackers have been adapting to the online mode of transactions to escalate their attacks to a more vicious level. Since the COVID-19 outbreak, DDoS attacks have been soaring. Following the surge of attacks in 2020, the number of attacks continued to grow in 2021.



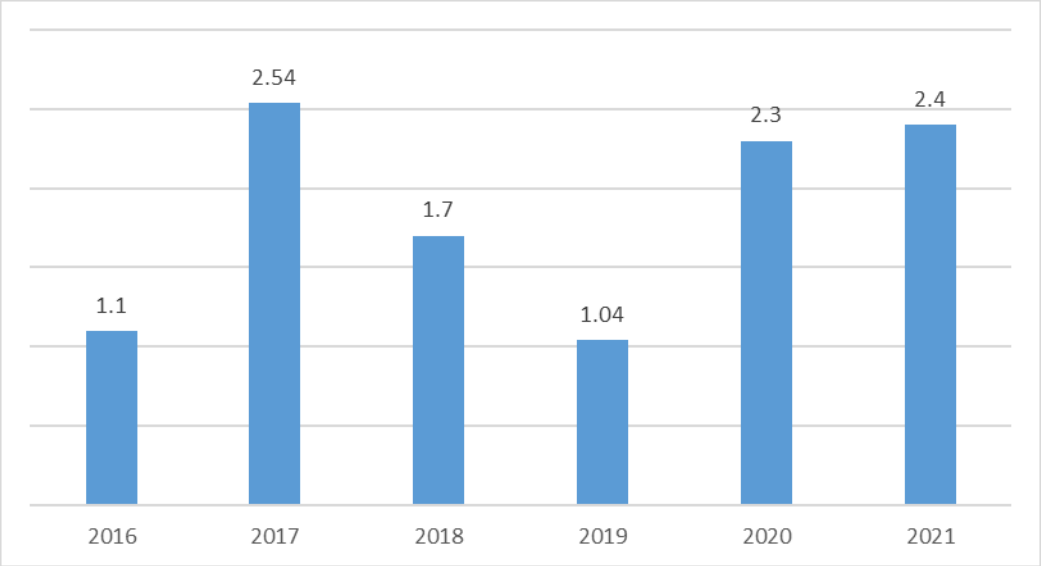
Number of DDoS attacks

In general, Internet enterprises suffer more DDoS attacks in the second half of a year, which is the period when people engage in more transactions and Internet business peaks. The threat of DDoS attack in the second half of 2021 was far greater than that in the first half. The carpet-bombing attack occurred in many countries was a contributing factor that makes August the month with the highest number of DDoS attacks, almost equal to the sum of DDoS attacks launched in all other months of the year In addition, the monthly numbers of attacks in the second half are all greater than those in the first half.



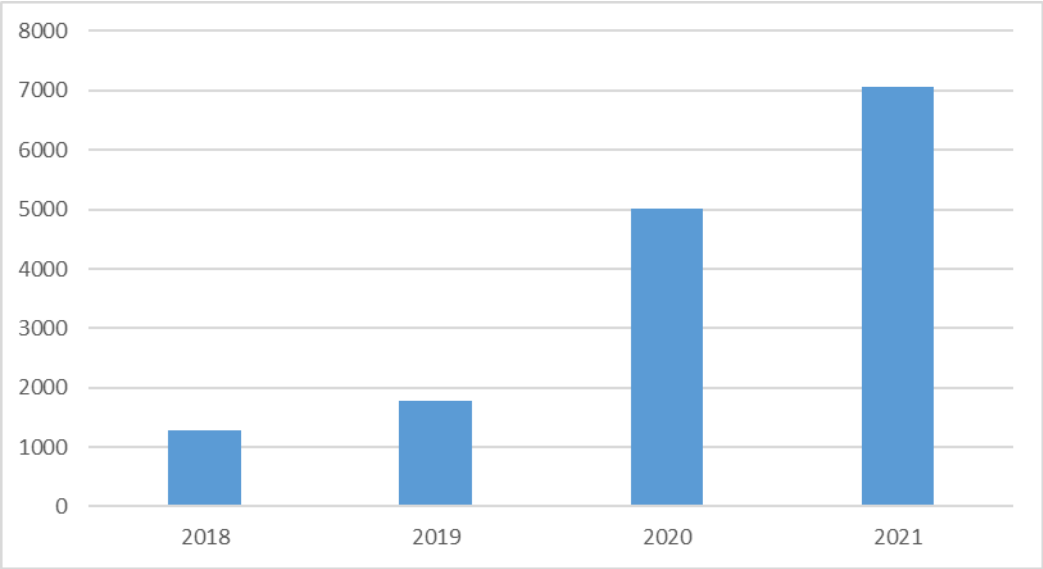
Overseas DDoS attack trends

In addition to the increasing number of attacks, the largest DDoS attack traffic peaked at 2.4 Tbps[1] this year, marking 2021 as the fifth year of terabit-class attacks after the first attack in 2016. This implies that terabit-class attacks have become a real threat to enterprises.



Peak traffic of DDoS attacks

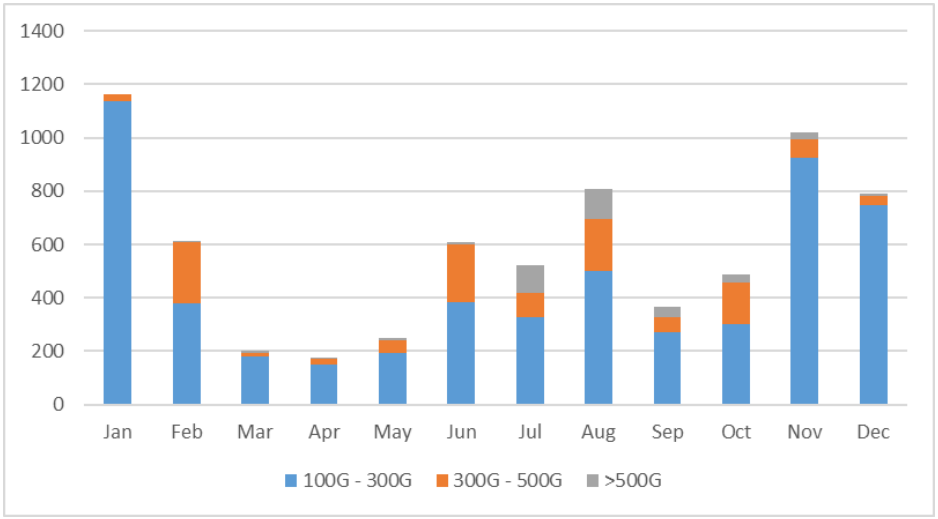
As the rapid popularity of 5G technology enables the significant increase in household bandwidth, the large number of networked devices is giving attackers more targets. This has not only elevated the number of DDoS attacks, but also spawned growing attacks larger than 100 Gbps, inflicting substantial harm on enterprises.



Annual trend of attacks larger than 100 Gbps

[1] Source from Microsoft: Business as usual for Azure customers despite 2.4 Tbps DDoS attack

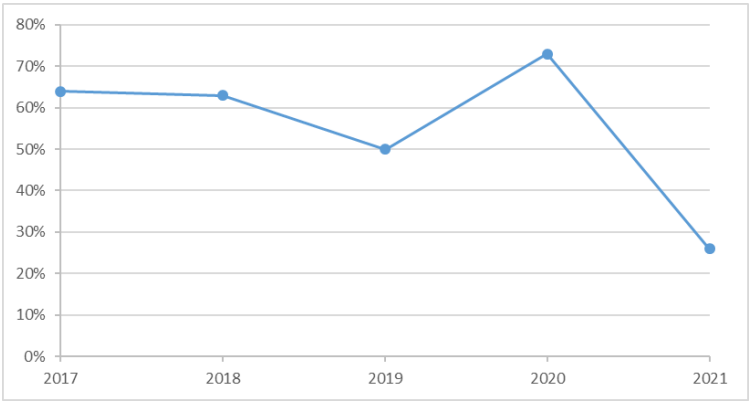
Under the influence of the above factors, the proportion of DDoS attacks larger than 300 Gbps significantly increased, accounting for more than 30% in February, June, July, August, and October in 2021.



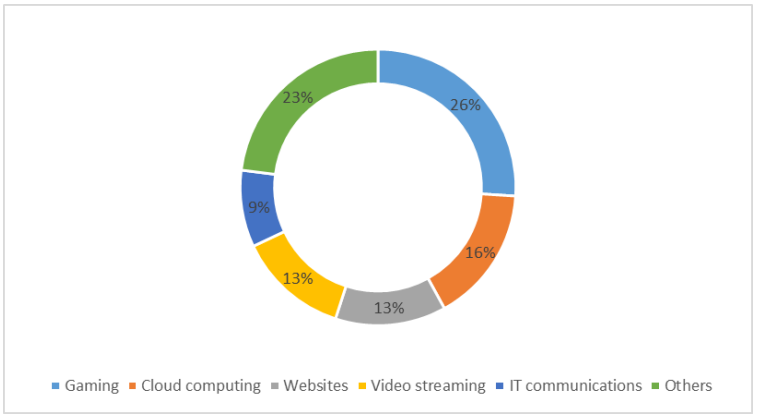
Monthly trend of attacks larger than 100 Gbps in 2021

The main victim industries are beginning to diversify, but the gaming industry still tops the target list of attackers

According to data, various industries across the world were under DDoS attacks in 2021. The gaming industry is still the main target of DDoS attacks, but the percentage of attacks directed to gaming market players decreased from the previous year. This can be attributed to the shift of the focus of attackers toward cloud computing, official websites, live streaming, and telecommunication in 2021.



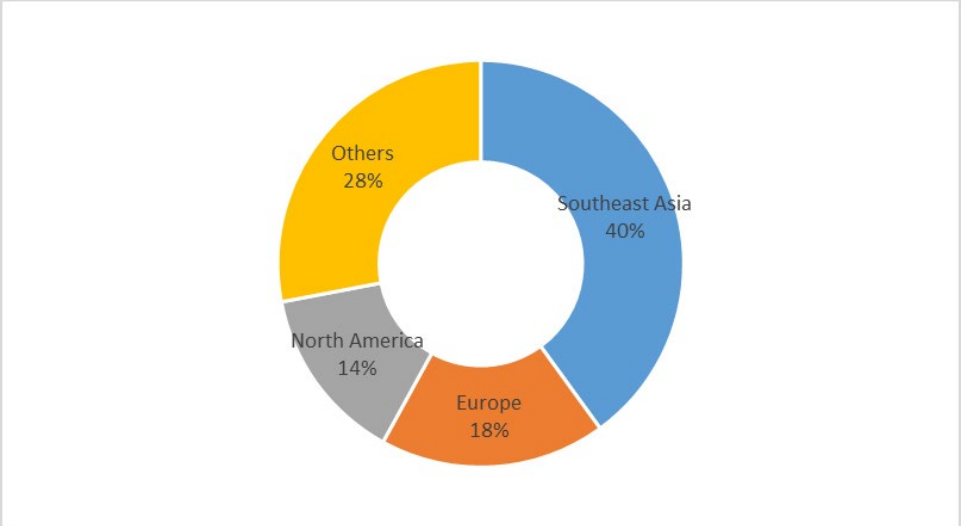
Percentage of DDoS attacks against the gaming industry



Industries under DDoS attacks

Southeast Asia becomes a hot target of attacks

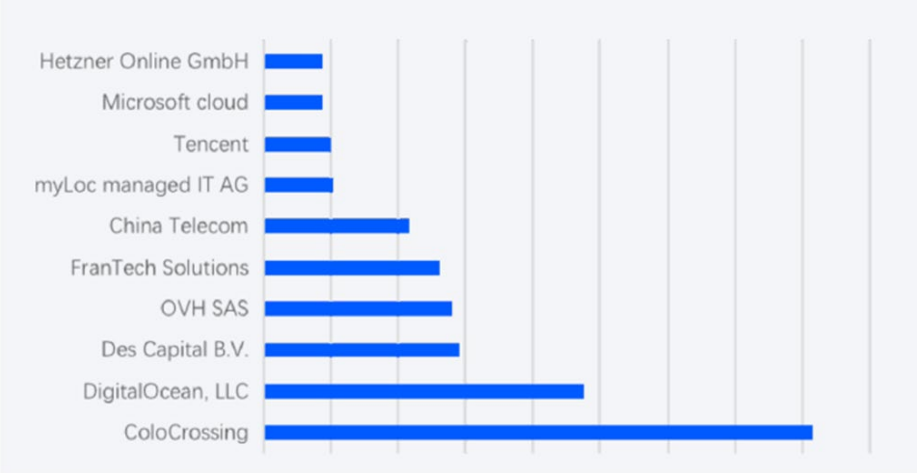
According to statistics, the geographical distribution of DDoS attacks is directly proportional to the development of the local economy and population. Southeast Asia, with the high economic level, large population, and a slew of Chinese enterprises, attracted attackers' attention and became the core of bullseye of DDoS attacks. The number of DDoS attacks in 2021 was evenly distributed across other regions of the world.



Regional DDoS attacks outside China

Botnet C&C servers are mainly distributed in North America and Europe

Data shows that North America and Europe are hosts of botnet C&C servers. Underground cybercriminal gangs focus on the C&C hosting service because each C&C server controls thousands of bots. If these bots are disconnected, all previous setups for the attacks are discarded. Underground cybercriminal gangs tend to select service providers who can provide guaranteed services with the high network quality.



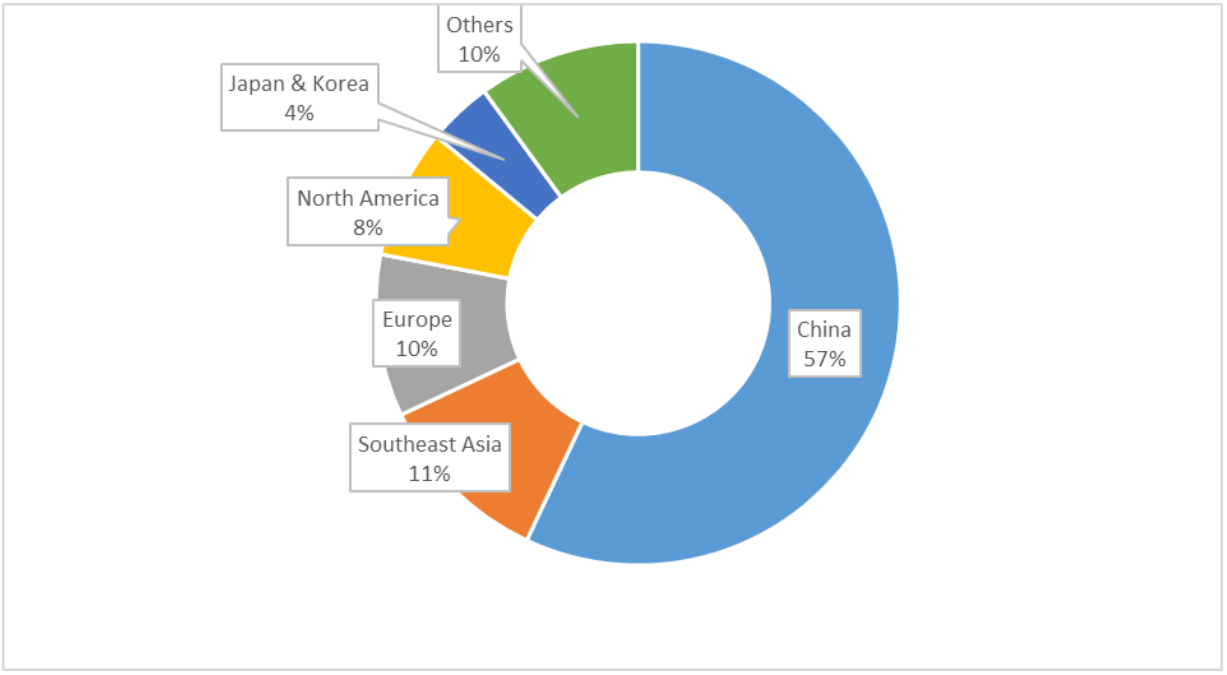
Top 10 C&C cloud vendors and telecom carriers

China is one of the main attack sources

With its huge economy, large population, and highly developed Internet industry, China remains as one of the top two sources of attacks, accounting for more than 50% of all attacks. Developed countries such as Japan, Germany, South Korea, and the UK, as well as developing countries such as Vietnam, Indonesia, Brazil, and India, are also among the main sources of attacks.

China, Southeast Asia, Europe, and North America have the largest number of bots

The geographical distribution of bots is highly correlated with the economic level and Internet penetration. Developed regions have a large number of bots. Specifically, China has more than 50% of the bots in the world, and Southeast Asia, Europe, and North America have approximately 10% each.



Geographical distribution of bots

DDoS threats may become the preferred extortion method of cybercriminal gangs

Ransomware attack was a big notorious event in 2021. Many victims were pestered by ransomware and DDoS attacks several times in 2021. Cybercriminal gangs weaponized ransomware for extortion. They threatened to disclose their prey's personal data in public if they refused to pay. If the prey calls to the police, DDoS attacks would come as retaliation. Although several ransomware DDoS attacks already occurred a couple of years ago, the huge value of ransom extorted in 2020 and 2021 made the predatory DDoS attackers greedier. Given that DDoS attacks are hard to trace and attackers can collect a large ransom at low costs, DDoS extortion remains a severe threat to enterprise security in the foreseeable future.

Attack Vectors

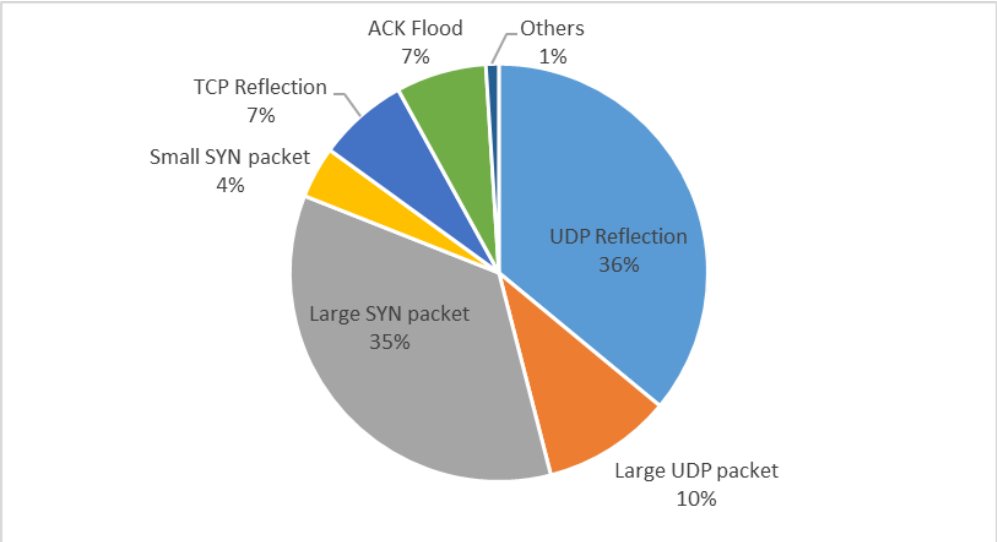
Botnets attack before vulnerabilities are repaired

DDoS attack is the first cyberattack with a clear way of profiteering by using botnets. Underground cybercriminal gangs usually exploit a vulnerability and rapidly plant botnet programs before the vulnerability is fixed while unceasingly looking for new types of reflection attack vectors.

For example, although GitLab issued the patch for CVE-2021-22205 in April 2021, Damian Menscher, a cloud security reliability engineer responsible for the DDoS defense of Google, disclosed in November that DDoS attack gangs have exploited this vulnerability to break down tens of thousands of servers and control them by using a botnet to launch large-scale DDoS attacks.

DDoS attacks larger than 100 Gbps become diversified

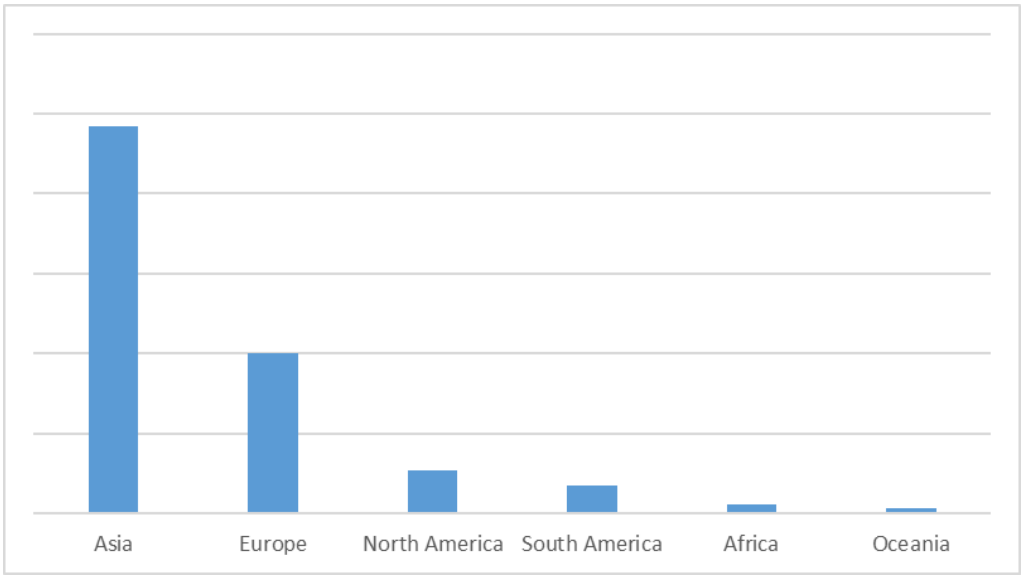
Although previous large traffic attacks were generally launched with large SYN packets and UDP reflection, statistics in 2021 shows that a considerable portion of DDoS attacks that are larger than 100 Gbps were launched through other means, such as TCP reflection, small SYN packets, and ACK flood. This indicates the means of such attacks have become diversified.



Means of larger-than-100 Gbps attacks

The sources of reflection DDoS attacks are correlated with the speed and scale of IoT development

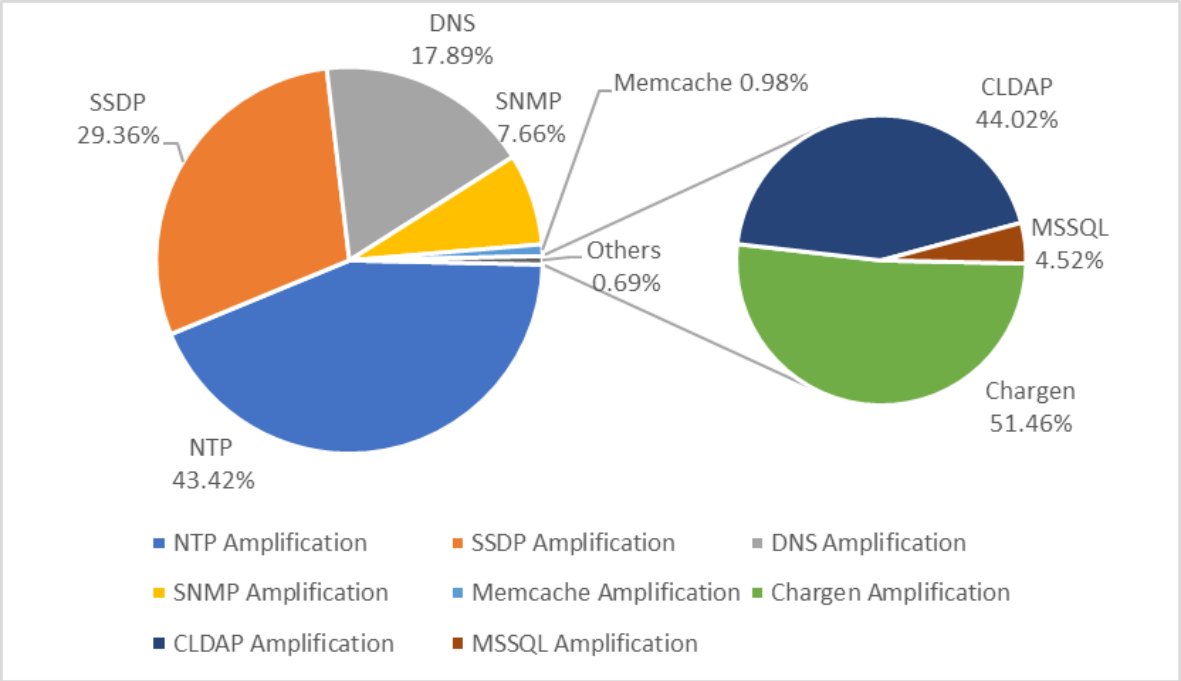
The global distribution of reflection DDoS attacks is strongly correlated with the development of regional Internet business. The budding IoT allows networked routers, cameras, access control systems, and other household devices to connect to the Internet. However, security measures are not quite in place. Even if vulnerabilities are identified in an IoT device, they can hardly be fixed in a short time. As a result, a large number of IoT devices can be exploited maliciously by underground cybercriminal gangs in no time.



Cross-regional distribution of reflection DDoS attacks

The preference of UDP reflection attacks is proportional to the amplification ratio

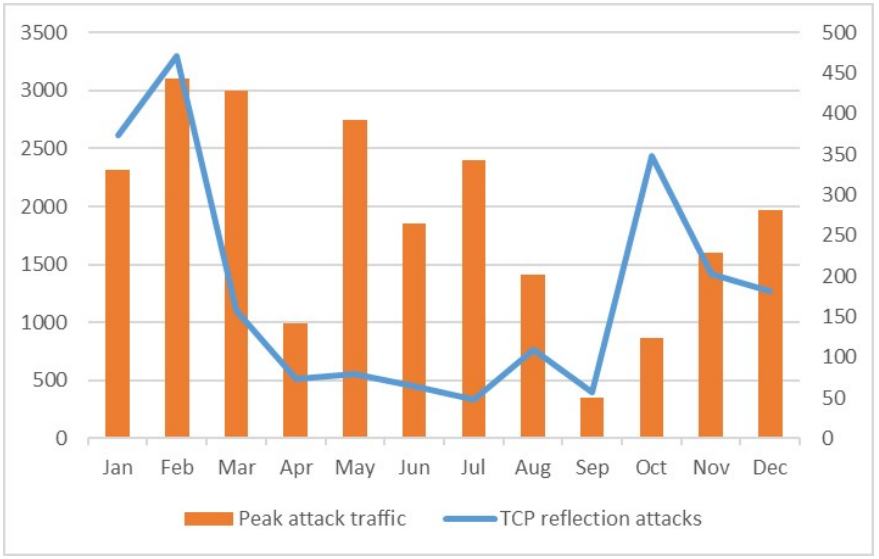
UDP reflection attacks are widely exploited by attackers due to their considerable amplification ratio and incognito nature. NTP reflection and SSDP reflection are the most common UDP reflection methods today. According to data, the amplification ratio for NTP, SSDP, DNS, and SNMP reflection attacks are 400-500:1, 30:1, 40-50:1, and 4-6:1, respectively. The figure below shows that the distribution of UDP reflection/amplification types is directly proportional to the amplification ratio of the protocol and correlated with their number on the Internet. Frequently leveraged in volumetric traffic attacks, the above-mentioned amplification types serve as main contributors to attacks over 100 Gbps.



Distribution of different types of reflection DDoS attacks

The TCP reflection attack in 2021 is U-shaped

As shown in the figure below, TCP reflection attacks peak in the first quarter and then decline significantly. After a hibernation period from April to September, the number of TCP reflection attacks rallied in October, resulting in a U-shaped trend throughout the year.

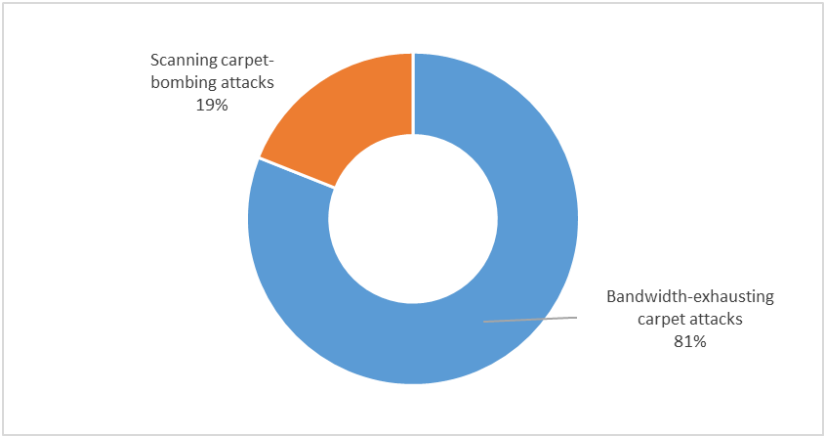


Trend of TCP reflection attacks

Carpet-bombing attacks and hit-and-run attacks are frequently used

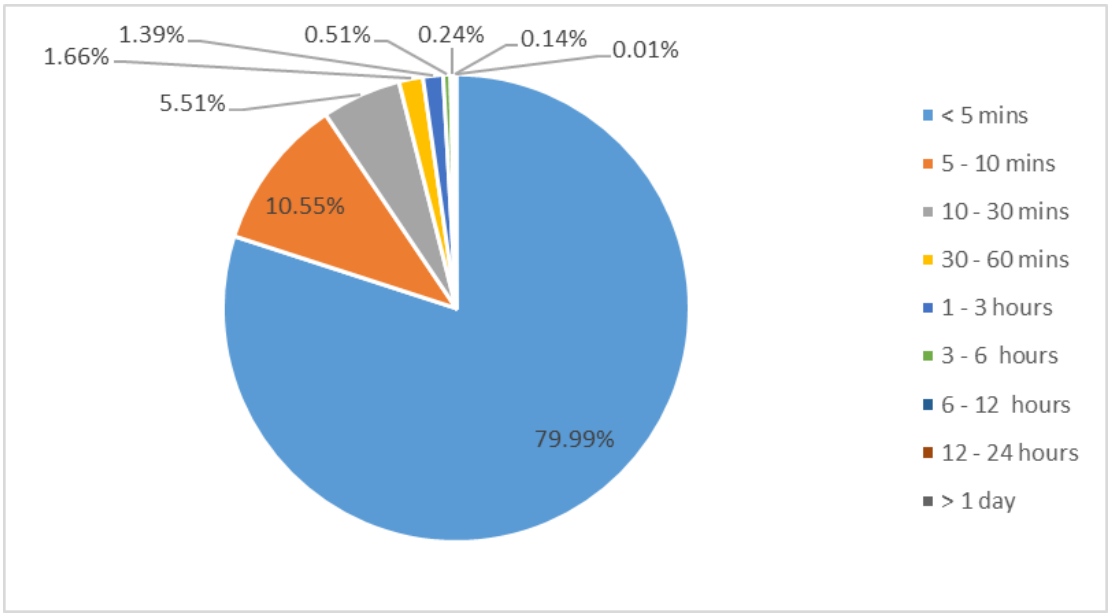
Carpet-bombing attack is a new form of DDoS attack that emerged in recent years. In a carpet-bombing attack, all IP addresses in a CIDR block are attacked at the same time or in sequence, with small and short-lived traffic against the same IP address lasting 3 to 30 seconds. In most cases, multiple DDoS attack types are launched in combination. When a large number of IP addresses are under attack at the same time, a small traffic pass-through is likely to happen. As a result, heavy attack flood and normal business traffic converge, which tends to bust down all servers of the victim due to the overwhelming load on the protection system.

According to data, carpet-bombing attacks have two major variants: bandwidth-exhausting carpet attacks and scanning carpet-bombing attacks. Bandwidth-exhausting attacks, which account for 81% of the overall carpet-bombing attacks, are mainly based on UDP reflection attacks and other mixed methods. This type of attack directs large traffic to a single IP address. In a typical bandwidth-exhausting attack, the attack flood against a single IP address can reach tens or hundreds of Gbps and last tens of seconds to a few minutes. By contrast, scanning attacks direct small traffic (tens or hundreds of Mbps) to a single IP address and last a few to dozens of seconds. The traffic distribution across different IP addresses is relatively uniform. However, the instantaneous attack traffic against multiple IP addresses can reach up to tens of Gbps, thereby causing considerable harm.

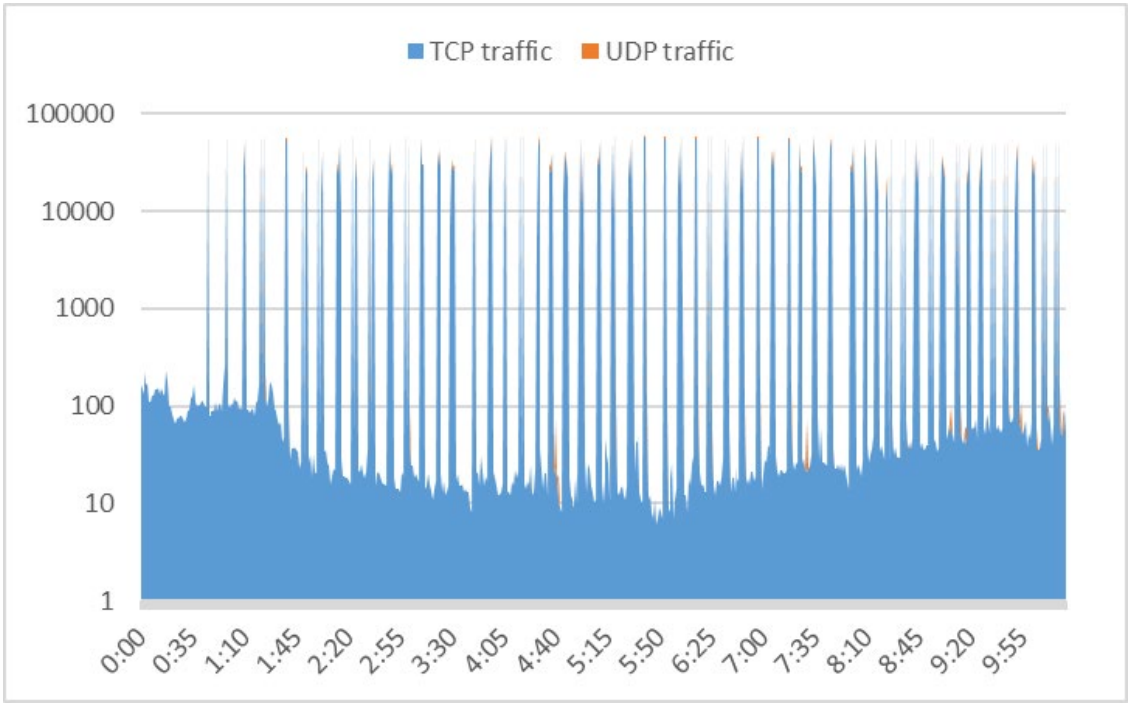


Types of carpet-bombing attacks

In addition to carpet-bombing attacks, the hit-and-run DDoS attack is also a popular choice of attackers. Data shows that 80% of DDoS attacks launched in 2021 ended in 5 minutes. The high percentage of hit-and-run DDoS attacks suggests that attackers focus on costs, efficiency, and technical countermeasures and use heavy attack traffic to cause the disconnection, delay, and jitter of the target in a short period of time. In the long run, instantaneous attacks can seriously downgrade the service quality of the target, sap the energy of DDoS defense service personnel, and effectively control the costs of attacks.



Duration of DDoS attacks

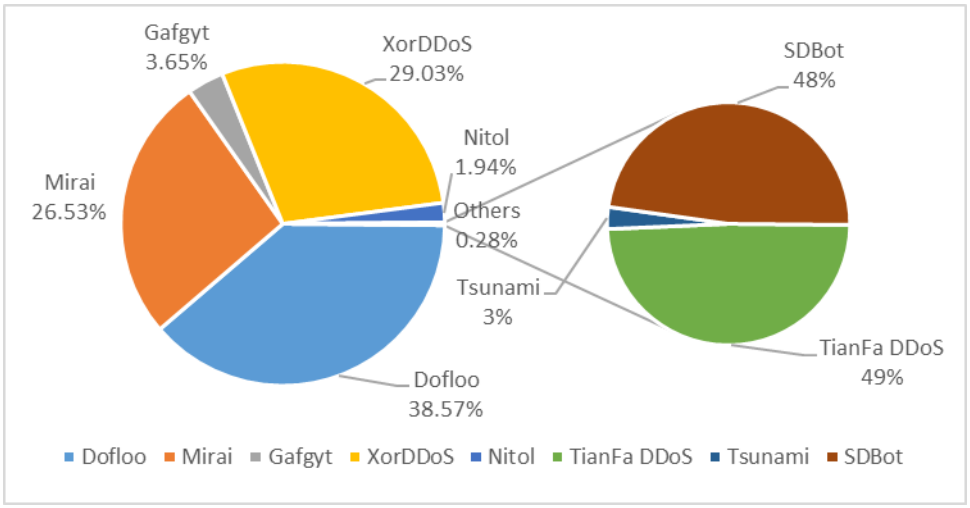


Hit-and-run DDoS attacks

Botnets

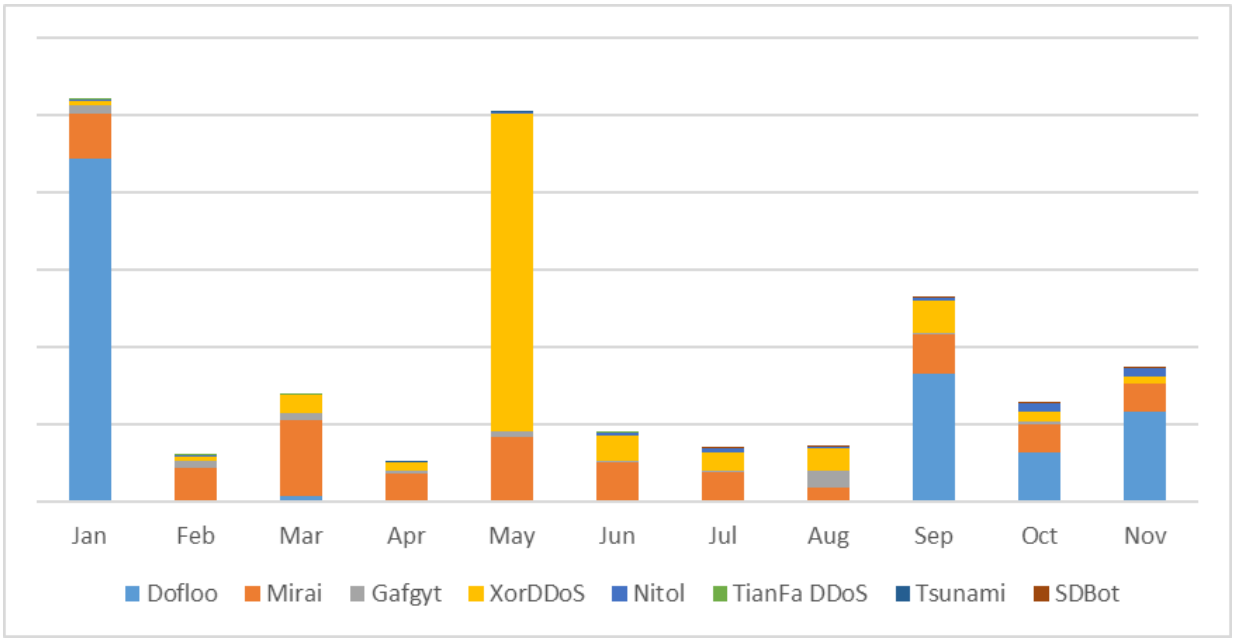
Major families of DDoS botnets

In 2021, NSFOCUS BotHunter tracked 15 DDoS botnet families and discovered the top four most active botnets: Dofloo, XOR DDoS, Mirai, and Gafgyt, whose attack instructions were mainly given from eight botnet families. By November 2021, more than a million DDoS attack instructions were tracked. The number of attack events was approximately one-sixth of the attack instructions. The percentage of attacks from the eight major botnet families is shown in the figure below.



Percentage of attacks from the eight major botnet families

With stable activity throughout the year, the Mirai family derived the most variants and had the fastest infection. Dofloo attacks peaked in January and became active again from September to November. XOR DDoS attacks peaked in May. Other attack families were less active than Mirai, Dofloo, and XOR DDoS, but also participated in the attacks, possibly because of their involvement in the Botnet as a Service (BaaS) network.



Distribution of DDoS attack instructions

Underground cybercriminal gangs strengthened DDoS attacks by propagating botnets

Data shows that attackers increasingly exploit vulnerabilities and weak passwords through DDoS botnets to expand their scope of control. Upon our analysis, botnets have exploited 72 types of vulnerabilities in the wild, and new vulnerabilities can be disclosed in one day.

Attackers infect and control devices before the vulnerabilities are fixed. The most exploited vulnerability is the command execution vulnerability at the Web end of the router. The vulnerabilities exploited by botnet families are shown in the figure below.

Top 20 Linux/IoT vulnerability exploitation and Botnet families	Gafgyt	hybridMQ	Mirai	Mozi	Persirai_shiina	tsunami	vbot	Zhtrap
CVE-2017-17215	Y	Y	Y	Y	Y	N	Y	N
CVE-2018-10561	Y	Y	Y	Y	Y	Y	N	N
CVE-2014-8361	Y	Y	Y	Y	Y	Y	N	Y
Netgear_DGN1000_1_1_00_48_Setup_cgi_Remote_Code_Execution	Y	Y	Y	Y	N	N	N	Y
Eir_D1000_Wireless_Router_WAN_Side_Remote_Command_Injection	Y	Y	Y	Y	N	N	N	N
JAWS_Webserver_unauthenticated_shell_command_execution	Y	Y	Y	Y	N	N	N	N
CVE-2015-2051	Y	Y	Y	Y	N	Y	N	N
CCTV-DVR Remote Code Execution	Y	Y	Y	Y	N	N	N	Y
ThinkPHP_5_X_Remote_Command_Execution	Y	Y	Y	N	Y	Y	N	N
ZyXEL_P660HN_T_v1_ViewLog_asp_privilege_escalation	Y	Y	Y	N	Y	N	N	N
D_Link_OS_Command_Injection_via_UPnP_Interface	Y	Y	Y	Y	N	N	N	N
CVE-2016-6277	Y	Y	Y	Y	N	N	N	N
Vacron_NVR_RCE	Y	Y	Y	Y	N	N	N	N
Seagate_BlackArmor_NAS_sg2000_2000_1331_Command_Injection	N	N	Y	N	N	N	N	N
CVE_2021_20090	N	N	Y	N	N	N	N	N
SAPIDO_RB_1732_Remote_Command_Execution	N	N	Y	N	N	N	N	N
CVE_2021_35395	N	N	Y	N	N	N	N	N
Linksys_E_series_Unauthenticated_Remote_Code_Execution	Y	Y	Y	N	Y	N	N	N
Common_Shell_Command_Abuse	Y	Y	Y	Y	Y	N	N	Y
D_Link_DSL_Devices_login_cgi_Remote_Command_Execution	Y	Y	Y	Y	Y	Y	N	N

Top 20 vulnerabilities exploited by DDoS botnet families

About NSFOCUS Cloud DPS

NSFOCUS boasts Anti-DDoS devices that have the largest market share in China and a leading industry position in the international market. These Anti-DDoS devices are augmented by NSFOCUS's unique threat intelligence from sources in and outside China. So far, 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.

About Tencent Cloud T-Sec DDoS Protection

By leveraging an extensive practice in business security for nearly 20 years, Tencent has independently developed T-Sec DDoS Protection, a global service that offers low-latency terabit-class cloud cleansing.

With the help of various algorithms, such as IP portrait, behavioral analysis, and cookie challenge, T-Sec DDoS Protection can effectively defend against all types of DDoS attacks from the IP layer to the application layer. The protection policies are continuously updated by AI-powered smart engines.

T-Sec DDoS Protection supports IPv4 and IPv6 dual-stack protection and provides enterprises with Anti-DDoS Pro, Anti-DDoS Advanced, and other all-in-one solutions to deal with all kinds of DDoS attacks.

The service offers effective support for diverse industries, covering gaming, online video streaming, financial, government, and other sectors.

NSFOCUS

SECURITY MADE SMART & SIMPLE

www.nsfocusglobal.com